الإمـــارات

برنامج محمد بن راشد للتعلم الذكي
Mohammed Bin Rashid Smart Learning Program

aqdar اقـدر
برنـامـج خليـفـة لتمكيـن الطـلاب
Khalifa Empowerment Program For Students

المواطنة الرقمية
وثقافة التواصل الإلكتروني

الصف الثاني عشر

1440-1441هـ/2020 - 2021م

الدراسات الاجتماعية والتربية الوطنية

المواطنة الرقمية وثقافة التواصل الإلكتروني

الصف الثاني عشر

1441 - 1442 هـ / 2020 - 2021 م

صاحب السّمو الشّيخ خليفة بن زايد آل نهيان
رئيس دولة الإمارات العربيّة المتّحدة، حفظه اللّه

"يجب التزوُّد بالعلوم الحديثة والمعارفِ الواسعة والإقبال عليها بروح عالية ورغبة صادقة، حتى تتمكّن دولة الإمارات خلال الألفيّة الثّالثة من تحقيق نقلة حضاريّة واسعة."

من أقوال صاحب السّمو الشّيخ خليفة بن زايد آل نهيان

قام بالنشر في دولة الإمارات العربية المتحدة شركة
Knowledge Point Educational Consultant, LLC UAE
تقاطع شارع 54 مع شارع 29
مدينة خليفة أ
أبوظبي، الإمارات العربية المتحدة

بموجب ترخيص من شركة Prestariang Systems Sdn Bhd, MALAYSIA
الطبعة الأولى، مارس 2012

حقوق الطبع والنّشر 2012 ©
Prestariang Systems Sdn Bhd (630804-K)
NeoCyber ,73-70
Lingkaran CyberPoint Barat
63000 ، سيبرجايا
سيلانغور ، ماليزيا
www.prestariang.com.my
الطبعة الأولى مارس 2012

حقوق الطبع والنشر

2012 © حقوق الطبع والنشر لأنظمة Prestariang
جميع الحقوق محفوظة. لا يجوز نسخ أي جزء من هذا المنشور أو نقله بأي شكل أو بأية وسيلة إلكترونية أو مادية، بِما في ذلك التصوير الضوئيّ أو التسجيل أو عن طريق أي نظام من أنظمة تخزين المعلومات واسترجاعها، دون الحصول على إذن مسبق من شركة Prestariang Systems Sdn Bhd و شركة Knowledge Point Educational Consultant, LLC UAE

CYBER C3

يُعد اسم وشعار Cyber C3 والمحتويات المترجمة من هذا المنهج التعليميّ ملكية خاصة وكاملة لشركة Knowledge Point Educational Consultant التعليميَّة المحدودة بالإمارات العربية المتحدة.

اعتراف

ساهمت شركة Knowledge Point Educational Consultant للاستشارات المحدودة في الإمارات العربية المتحدة في هذا المنهج التعليميّ في ترجمة المحتوى بما يتناسب مع ثقافة وتقاليد دولة الإمارات العربية المتحدة وأوضاعها. وشملت هذه المساهمات توفير دراسات الحالة المحلية والإحصاءات والمخططات والرسومات والصور بالإضافة إلى المراجع, فلولا ما تم تقديمه من نصح ومشورة ومساعدة مباشرة لما كان لهذا المنهج التعليميّ أن يظهر في صورته الحاليّة.
جميع الشعارات وأسماء المنتجات هي علامات تجاريَّة مسجّلة لمالكيها.
العناصر الخاصة ببرنامج أخلاقيَّات (الإنترنت) الخاص بكل مشروع هي ملكية كاملة وحصرية لشركة Knowledge Point Educational Consultant وهي تحتفظ بالحق في تغيير الاسم والشِّعار وحقوق الملكية الفكرية الأخرى.

إخلاء المسئولية

لا تُقَدِّم شركة Prestariang Systems Sdn Bhd أي ضمان أو توضيحات، سواء صريحة أو ضِمنية، فيما يتعلق بهذا الكتاب أو جودته أو أداء استخدامه أو الرواج التجاريّ أو الملاءمة لغرض معين. ولن تكون شركة Prestariang Systems Sdn Bhd مسئولة عن الأخطاء الواردة هنا أو عن أي أضرار عَرضيَّة ذات صِلة بتوفير هذه المواد أو الأداء المتعلق بها أو استخدامها. وجميع الروابط الموجودة في هذه الوحدة صالحة للاستخدام بتاريخ 6 مارس 2012 وجميع المعلومات الواردة صحيحة وقت طباعتها، وهي خاضعة للتغيير دون إشعار مسبق.

اعتراف

بفضل تكنولوجيا (الإنترنت)، أصبحت المعلومات في متناول يد كل منّا. وقد أعدّت معظم هذه الوحدات وجمعت من التقارير البيضاء والتقارير السابقة والمقالات التي المواد التي أدرجنا بيانها في الصفحة الأخيرة من كل وحدة للرجوع اليها.
فبدون الرجوع إلى هذه الوثائق المذكورة، لم تكن لتظهر هذه الوحدات في الشكل الذي هي عليه اليوم.
كل الشعارات وأسماء المنتجات هي علامات تجارية أو علامات تجارية مسجلة لمالكيها.

المقدمة

الانسان هو المورد الرئيس و العنصر الأهم في تحقيق التنمية الشاملة، فعلى إثر بنائه تبنى مجتمعاته وعلى مستوى ارتقاء قدراته وأفكاره تبنى حضارته، وتنمية هذا المورد تصدرت قائمة اهتمامات القيادة الرشيدة في دولة الإمارات العزبية المتحدة وخططها التطويرية واتسعت دوائر هذا الاهتمام لتشمل كل مسؤول في أرجاء مؤسساتها فالجميع أعلن مسؤولية المشاركة في رعاية اللبنات الناشئة واستكمال الدور التربوي الذي تقوم به وزارة التربية والتعليم وذلك عبر ما تبنته هذه المؤسسات من برامج توعوية وتدريبية وتنموية تجمعها غاية واحدة هو تحقيق البناء الرائد للمجتمع الإماراتي برعاية أبنائه وبناء ذواتهم وقدراتهم.

هذا المنهاج بين أيديكم يهدف إلى إعداد مواطنين مؤهلين رقميًا وقادرين على تحمل المسؤوليات أثناء تعاملهم مع الفضاء الإلكتروني.

يهدف هذا البرنامج إلى إرساء قواعد صلبة في كافة المجالات التي تتخاطب بلغة (السايبر) ولكن على وجه الخصوص ليضع القواعد وأفضل الممارسات في (آداب التعامل المقبول على الشبكات الإلكترونية أو ما يعرف بالإيتيكيت) الذي ينبغي تطبيقه عند استخدام أدوات رقمية، أو عند استخدام الوسائط الرقمية والتواصل مع الآخرين على الشبكة العنكبوتية.

المحتويات

يتم تعريف المحتوى على تطبيق التعلم الذكي

مُقدمة

01 الوصول الإلكتروني

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المحتويات

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المحتويات

05 التفاعل والتعاون الإلكتروني

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

06 المشروعات الإلكترونيّة

07 الرعاية الإلكترونية

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المحتويات

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

مُقدمة

مرحبًا بِكم

هل تستخدِم النُّظمَ والأدوات الرقميَّة استخدامًا أخلاقيًا عند تبادل المعلومات ومشاركتها؟ هل تتبعُ آداب حاسوبيَّة سليمة عند استخدام التكنولوجيا؟ هل أنت قادر على تمييز الفرق بين الاستخدام المناسب من الاستخدام الغير مناسب للتكنولوجيا؟ هل تتمتع بالحماية من برامج التجسس والقراصنة والاحتيال وسَرقة بيانات الهُوية والمطاردة عند استخدام (الإنترنت)؟

قد تكون على قدرٍ من الذكاء في استخدام تكنولوجيا المعلومات والاتصالات ولكن هل أنت على درايةٍ بكل ما يلزم لتصبحَ مستخدماً محترفًا لشبكة المعلومات المترامية الأطراف؟ لمعرفة ذلك، يمكُنك إجراء تقييمٍ (CYBER C3) المعروف عالميًا، وهو بَرنامج عالميّ خاص بأخلاقيَّات (الإنترنت) فيما يتعلقُ بآداب استخدام الحاسوب، للتأكُّد والتحقُّق مِن فَهمك للقواعد الأساسيَّة الخاصَّة بالاستخدام المقبول للتكنولوجيا في العالم الرقميّ المعاصر.

ويُعَدُّ إختبار (CYBER C3) هو الأول من نوعه في العالم الذي تم تطويره وتصميمه خصيصًا لدولة الإمارات العربية المتحدة، وذلك للارتقاء بمستوى المواطنين إلى درجة المعرفة والمسئولية الرقميَّة، بحيث يمتلك المواطِنُ الوعي الكافي حول أمن (الإنترنت) وثقافة الاتصال الإلكترونيّ، وبذلك ينمو لدى مستخدمي (الإنترنت) الشعور بالمسئوليَّة المدَنيَّة تجاه مجتمعهِم على (الإنترنت) كمثل شعورهم تجاه مجتمعهم الفعليّ.

كما يُعد بَرنامج (CYBER C3) مُؤيدًا لفكرة (Netizen) (مستخدمو (الإنترنت))، وهو مصطلح أطلقه مايكل هاوبين في عام 1992م. "(Netizen مستخدمو (الإنترنت)) هو مُستخدِم (الإنترنت) الذي يمتلك حسَّ الشعور بالمسئوليَّة المدَنيَّة تجاه مجتمعِه على (الإنترنت) على نحوٍ مماثلٍ لما يشعر به المواطنونَ تجاه مجتمعهم الفعليّ "

مايكل هاوبين؛
مؤلف كتاب" مستخدمو (الإنترنت): حول تاريخ شبكات المستخدمين و(الإنترنت) وآثارهم (1992م) "

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

01 الوصول الإلِكترونِيّ

حول هذه الوحدة

سنكشف في هذه الوحدة عن الفجوة الموجودة بين من يتمتعون بالوصول الفعَّال إلى التكنولوجيا الرقمية وتكنولوجيا المعلومات، وبين هؤلاء من ذوي الوصول المحدود جدًا أو المنعدم. وهذا يشمل استكشاف التكنولوجيات المستخدمة، وعدم التوازن، على حد سواء، في الوصول الفعليّ إلى التكنولوجيا وفي الموارد اللازمة للمشاركة الفعَّالة في الحصول على التكنولوجيا. كما تُوفر فهمًا لامتياز استخدام المعلومات الإلكترونيّة في المجتمع، فض عن الحقوق في الوصول المتساوي والآمن والموثوق به. كما سيكون هناك نقاشًا، بالإضافة إلى ذلك، حول كيفية تَصَفُّح أصحاب الهمم (للإنترنت).

كما سنركز على بعضِ دراسات الحالة، ونكشف عن الكيفية التي ساعدت بها بعض الحكومات في تعزيز تطوير عمليات الوصول الإلكترونيّة ورأب الصدع الرقميّ في بلدانهم.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أهداف التعلُّم

أهداف هذه الوحدة هي:

- توضيح المقصود بالوصول الإلكتروني.
- ترسيخ التقدير لبعض المبادرات الرقمية الحكومية.
- مشاركة معلومات حول كيفية ومكان الوصول إلى شبكة (الإنترنت).
- مشاركة معلومات حول كيفية استخدام أصحاب الهمم للتقنيات.

نواتج التعلُّم

في نهاية هذه الوحدة، سوف تكون قادرًا على:

- إدراك ماهية الوصول الإلكتروني.
- تقدير مدى مساعدة بعض الحكومات لدفع عجلة الوصول الإلكتروني.
- معرفة كيفية ومكان الوصول إلى شبكة (الإنترنت).
- معرفة كيف يمكن لأصحاب الهمم الوصول إلى شبكة (الإنترنت).

قائمة المراجعة

البنود	التحصيل العلمي	قبل	بعد
1	أنا أدرك ما المقصود بالوصول الإلكتروني.		
2	أدرك ما قامت به حكومة دولتي لدفع عجلة الوصول الإلكتروني في الدولة.		
3	أدرك كيفية ومكان الوصول إلى شبكة (الإنترنت).		
4	أدرك كيف يمكن لأصحاب الهمم الوصول إلى شبكة (الإنترنت).		
5	أنا أعرف كيفية استخدام التكنولوجيا بطريقة إيجابيَّة		

التعليمات:

بعد الانتهاء من قراءة هذه الوحدة، يُرجى إكمال الاستبيان باستخدام المقياس التالي:

المقياس:

1. ليس لدي أدنى معرفة.
2. لدي معرفة محدودة.
3. على دراية وقادر على التوضيح الجيّد.
4. ذو كفاءة وإمكانية على الممارسة الكاملة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الوصول الإلكتروني ـ ميزة تهدف إلى استخدام المعلومات الإلكترونية في المجتمع

مع التطورات الحادثة في المعلوماتية المجتمعية، يصبح استخدام تقنيات المعلومات والاتصالات كوسيلة لنشر المعلومات أكثر شهرة في عصرنا الحالي. وتتيح تقنيات المعلومات والاتصالات نشر المعلومات بشكل متزامن أو غير متزامن، كما توفر الفرص للأشخاص للحصول على المعلومات في أي وقت، وفي أي مكان، وحول أي شيء يمكنهم استخدامه لتطوير أنفسهم على الصعيد الاجتماعي والثقافي والاقتصادي.

وتعني كلمة الوصول «القدرة على الدخول»، أو «الانتقال من أو إلى مكانٍ ما»، أو «التواصل مع أي شخصٍ أو أي شيءٍ».

بسبب وجود (الإنترنت) أصبحت المعلومات متوفرة للجميع ويمكن الوصول اليها بسهولة. وقد احدث ثورة في عالم الاتصال وشبكات التواصل الاجتماعي واوجد منطقة كانت عالمية. يتواصل الناس ويتشاركون المعلومات بواسطة (الإنترنت). يلعب (الإنترنت) دور في ازالة الحدود بين الامم.

لقد جلب القرن الجديد الكثير من التحديات الحديثة أمام البشرية، بما في ذلك التطورات والإنجازات التقنية الناجمة عن العولمة. ومع ذلك، يجب ألا نرزح تحت نير هذه التطورات. فيجب ألا نسمح لأنفسنا بأن نكون عبيدًا للتقنيات الحديثة.

التعرُّف على الفجوة الرقميَّة: ماهيتها

ما هي الفجوة الرقميَّة؟

الفجوة الرقميَّة تشير إلى الفرق بين البلدان في قدرة الوصول إلى البنية التحتيَّة العالميَّة للمعلومات، والفرق بين أولئك الذين لديهم إمكانيَّة الوصول إلى أجهزة (الكمبيوتر) و(الإنترنت)، وأولئك الذين لا يملكون ذلك.

مُؤشِّر الوصول الرقميّ (Digital Access Index - DAI)، هو مصطلح أطلقه الاتحاد الدولي للاتصالات (International Telecommunication Union - ITU) ويُساعد مُؤشِّر الوصول الرقميّ على قياس الامكانات الكُليَّة للناس في بلدٍ معين في الوصول إلى تكنولوجيا المعلومات والاتصالات واستخدامها.

وتوضح الفئات الخمس الواردة في مُؤشِّر الوصول الرقميّ (DAI) على النحو التالي:

فئات مُؤشِّرالوصول الرقميّ DAI	التعريف
البنية التحتيَّة	يشير إلى عدد المشتركين في الهاتف الثابت والهاتف الجوَّال
القدرة على تحمُّل التكاليف	تُؤخذ أسعار الوصول إلى (الإنترنت) من حيث النسبة المئوية لإجمالي دخل الفرد
المعرفة	مستوى محو الأميَّة لدى الكبار ومستوى الالتحاق بالمدرسة
الجوْدة	النطاق الترددي العريض الدولي للفرد الواحد والمشتركين في النطاق العريض (سرعة (الإنترنت))
الاستخدام	عدد مستخدمي (الإنترنت)

الجدول 1: مؤشِّر الوصول الرقميّ الفئة التعريف

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

العدد الإجمالي لمستخدمي شبكة (الإنترنت) في دولة الإمارات حتى عام 2020 هو 99 لكل 100 شخص.

العدد الاجمالي لمستخدمي (الإنترنت) في العالم حتى عام 2020 هو 59لكل 100 شخص

مستخدمو (الإنترنت)/ 100شخص = مستخدمي (الإنترنت) x100

مجموع عدد السكان

يُمكن أن يشير مستخدمو (الإنترنت) إلى مستخدمين فوق سن معينة فقط

تكنولوجيا المعلومات والاتصالات في الوطن العربيّ

أعلى 5 في تصنيف مُؤشّر الوصول الرقميّ

في مُؤشّر الوصول الرقميّ العالميّ الأخير، كانت دولة الإمارات العربية المتحدة هي الأعلى من بين البلاد العربية في المرتبة 34 بتصنيف وصول 0.64 ، تليها البحرين في المرتبة 38 بوصول 0.64

أعلى (5) في تصنيف مُؤشّر الوصول الرقميّ

قام الاتحاد الدوليّ للاتصالات أيضًا بتطوير مُؤشّر تطوّر تكنولوجيا المعلومات والاتصالات (IDI) الذي احتلت فيه دولة الإمارات العربية المتحدة المرتبةَ الثانية بعد البحرين في منطقة الدول العربية (انظر الجدول) والمرتبة 32 على مستوى العالم.

ويُعَدُّ مؤشر تطور تكنولوجيا المعلومات والاتصالات (IDI)، على النحو الوارد في تقرير "قياسات مجتمع المعلومات 2017 « الذي قام بإعداده الاتحادُ الدوليّ للاتصالات، مؤشرًا مُركَّبًا يجمع بين ١١ مؤشر آخر مرتبطة جميعها بالوصول إلى تكنولوجيا المعلومات والاتصالات واستخدامها ومهارات التعامل معها. ونظرًا لأن مؤشر تطور تكنولوجيا المعلومات والاتصالات (IDI) يضم (175) بلدًا، فهذا سيسمح بإجراء عمليات القياس على المستوي العالميّ والإقليميّ. وتُصنَّف كل واحدة من هذه البلدان ضمن واحدة من المجموعات الأربع (الأعلى والعليا والمتوسطة والمنخفضة) والتي تصف مستوى تكنولوجيا المعلومات والاتصالات في الاقتصاد.

المرتبة العالمية	البلد	المرتبة في مؤشر تطور تكنولوجيا المعلومات والاتصالات (IDI) (عالميًا)
الأولى	دولة الإمارات لعربية المتحدة	15
الثانية	المملكة العربية السعودية	32
الثالثة	مملكة البحرين	34

الجدول 2: 2019م، وفق مؤسسة محمد بن راشد آل مكتوم للمعرفة

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تحقيق الوصول المتساوي للمعلومات والتغلُّب على الفجوة الرقميَّة

كيف يمكننا الوصول إلى (الإنترنت)؟

لقد أصبحنا أكثر اعتمادًا على الشكل المتطور غير المسبوق لوسائل الإعلام، وشبكة (الإنترنت)، وذلك على النقيض لِما كان عليه الوضع فيما مضى من اعتماد الناس على الصُّحف والمجلات والكتب وغيرها من المواد المطبوعة كمصدر وحيد للحصول على المعلومات. الأمر الجيِّد في ذلك هو توفُّر العديد من الطرق المختلفة للوصول إلى (الإنترنت) بين أيدينا. ومع ذلك، يمكن أن تكون المجموعة الواسعة من الخيارات سببًا مُربِكًا للغاية.

تعتبر دولة الإمارات رائدة على مستوى الاقليم في التغلب على الفجوة الرقمية من خلال مشاريع خلاقة مثل:

- مدينة دبي الذكية.
- مشروع الحكومة المتنقلة والخدمات المتنقلة في أبو ظبي الذي يهدف إلى توفير منصة خدمات يمكن الدخول إليها في أي وقت ومن أي مكان من قبل المواطنين.

أَلق نظرة على المعلومات الواردة أدناه. سوف نناقش هنا الخيارات المتاحة للوصول إلى (الإنترنت)، بالإضافة إلى الأمور ذات الصلة بهذه الخيارات. وهذا سوف يساعدك على تحقيق فَهم أفضل للخيارات المتاحة، وكيف يمكنك اختيار أفضل الخيارات التي تناسب احتياجاتك.

هناك طرقٌ عديدة ومختلفة للوصول إلى (الإنترنت). ولكل منها نِقاط قوة ونِقاط ضعف. ولاختيار أفضل الطرق التي تناسب احتياجاتك الشخصيَّة، يجب تقييم كل خَيار.

المودم

استخدام المودم هو الطريقة الأساسيَّة والأقدم للوصول إلى (الإنترنت). وقد أنتجت الشركات المصنِّعة للكمبيوتر في الوقت الراهن أجهزة مودم مدمجة في أجهزة (الكمبيوتر) المحمولة.

وقد قامت العديد من الفنادق بمبادرة توفير منافذ بيانات في الغرف الفدقيَّة للدخول الى (الإنترنت)، وإن لم يكن هذا فإنها على الأقل توفِّر قوابس للاتصال في هواتف الغرف. مما يَسمح لنزلاء الفندق بربط المودم في أجهزة (الكمبيوتر) المحمول الخاصة بهم بخط الهاتف ومن ثم البدء في إجراء اتصال الطلب الهاتفيّ والاتصال ب(الإنترنت).

خدمات (الإنترنت) العامَّة

يمكنك في الوقت الراهن الاتصال بسهولة بشبكة (الإنترنت) السلكية ، نظرًا لأن العديد من المؤسسات قد بدأت في توفير شبكات النطاق العريض، وهي شبكات سريعة وسهلة الاستخدام. ومع ذلك، قد يلزم دفع رسوم رمزيَّة للحصول على هذه الخدمة، وهذا يتوقف على عرض النطاق الترددي. فالمكتبات العامة والمرافق الحكوميَّة هي أمثلة لتلك الأماكن التي يُمكنك فيها الوصول مجانًا إلى (الإنترنت).

وبالإضافة إلى ذلك، يُمكنك في الغالب الوصول إلى (الإنترنت) في الأماكن التالية:

- الكليَّات والجامعات.
- المحلات التجارية مثل المراكز التجاريَّة الفندقيَّة ومراكز المؤتمرات والمطارات.
- مقاهي (الإنترنت).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الوصول إلى (الإنترنت) بنظام Wi-Fi اللاسلكيّ المجانيّ منه والمدفوع

بَدأت العديد من الدول بناء مناطق حيويَّة يتوفر فيها (الإنترنت) بنظام Wi-Fi ، وتوفرها مجانًا أو برسوم مخفَّضة. فالمطارات والمكتبات، مراكز التسوق ، والاماكن المشهورة والمقاهي من بين الأماكن التي تقدم خدمات حيويَّة في الإمارات. ومع ذلك، قد يلزم الاشتراك في خِدمة (الإنترنت) بنظام Wi-Fi لتتمتع بالوصول إلى مواقع مختلفة.

الاتصال بـ (الإنترنت) عبر الهاتف النقال

يشير مصطلح "(الإنترنت) عبر الهاتف النقال" قدرة المستخدم إلى الوصول إلى (الإنترنت) عبر مزود خدمة الهاتف الخلوي ، فعند اشتراك المستخدم بالخدمة من خلال مزود خدمة (الإنترنت) ISP التابع لدولته سواء ذلك بعقد أو من خلال الدفع المقدم يتم تحديد كمية البيانات المتاحة للمستخدم وتقاس عادة بالميغابايت وتسمح للمستخدم الوصول إلى (الإنترنت) والانتفاع به. تجدر الإشارة بتوفر سرعات مختلفة يتم تقديمها للمستخدم مثل شبكة الجيل الرابع 4G ومؤخرا شبكة الجيل الخامس 5G والتي تعتبر الأسرع وقد تغير العالم من خلال تأثيرها الكبير والواسع في عدة مجالات حيوية .

المختبرات العملية – الدخول إلى (الإنترنت)

سوف تتعلم في هذه المختبرات كيفيفة الدخول إلى (الإنترنت).

الخطوات العملية موضحة في نهاية هذا الفصل.

الهواتف المحمولة وأجهزة المساعد الرقميّ الشخصيّ.

من المعروف أن الهواتف المحمولة وأجهزة المساعد الرقميّ الشخصيّ تقدّم خدمات (الإنترنت) لبعض الوقت. ويتميز استخدام الهواتف المحمولة في الاتصال بشبكة (الإنترنت) في أنها سَهلة الاستخدام ومريحة. فشراء هاتف أصبح أرخص بكثير من شراء جهاز كمبيوتر محمول، كما أنه من الأسهل حمل الهاتف المحمول والتجوُّل به مقارنةً بحمل (الكمبيوتر) المحمول معك طوال الوقت.

لماذا أصبحَ الحصول على المعلومات قضيَّة عالميَّة

لم يعد الوصول إلى (الإنترنت) مقتصرًا على أجهزة (الكمبيوتر) الشخصية وأجهزة (الكمبيوتر) المحمولة. ففي كثير من البلدان النامية، يتصل المستخدمون ب(الإنترنت) من خلال هواتفهم المحمولة.ومع ذلك، فالوصول إلى (الإنترنت) باستخدام الهواتف المحمولة مكلّف نوعًا ما، كما أن تكلفة إعداد البنية التحتيَّة مرتفعة أيضًا.

معظم الدول الغربيَّة لا تستثمر في النطاق العريض، والوضع أكثر سوءًا في البلدان الفقيرة. وحتى في البلدان المتقدمة، هناك فجوة ظاهرة بين أولئك الذين لديهم اتصال عالي السرعة ب (الإنترنت)، وأولئك الذين لا يملكون السرعات العالية.

ما هي الأسباب التي تُكوّن هذه الفجوة الرقميَّة؟ بعض الأسباب هي:

1. نقص البنية التحتيَّة لتكنولوجيا المعلومات والاتصالات.
2. الافتقار إلى المهارات والقدرات العاملة في المؤسسات.
3. القيود الماليَّة.
4. المشاركة الضعيفة في برنامج التنمية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

نظرة ثاقبة: كيف تتعاملُ دولة الإمارات العربية المتحدة مع قضايا الفجوة الرقميَّة

قبل أن ننظر في كيفية تعامل دولة الإمارات العربية المتحدة مع قضاياها الخاصَّة بالفجوة الرقميَّة، دعونا نلقي نظرةً عامةً على أسواق تكنولوجيا المعلومات في الشرق الأوسط وأفريقيا.

عندما يتعلقُ الأمر بتطوير مجتمع المعلومات في الشرق الأوسط، فإن الوصول إلى شبكة (الإنترنت) يكون ذا نسبة عالية في الدول الأكثر ثراء ولكن لا يكون الوضع كذلك مع الدول الوليدة في السوق.

تُعَدُّ دولة الإمارات العربية المتحدة واحدةً من الدول الأكثر استعدادًا من الناحية الإلكترونيَّة في المنطقة، والتي وصل انتشار (الإنترنت) فيها إلى 99 % في عام 2020م.

انتشار (الإنترنت) 2020م (لكل 100 من السكان)

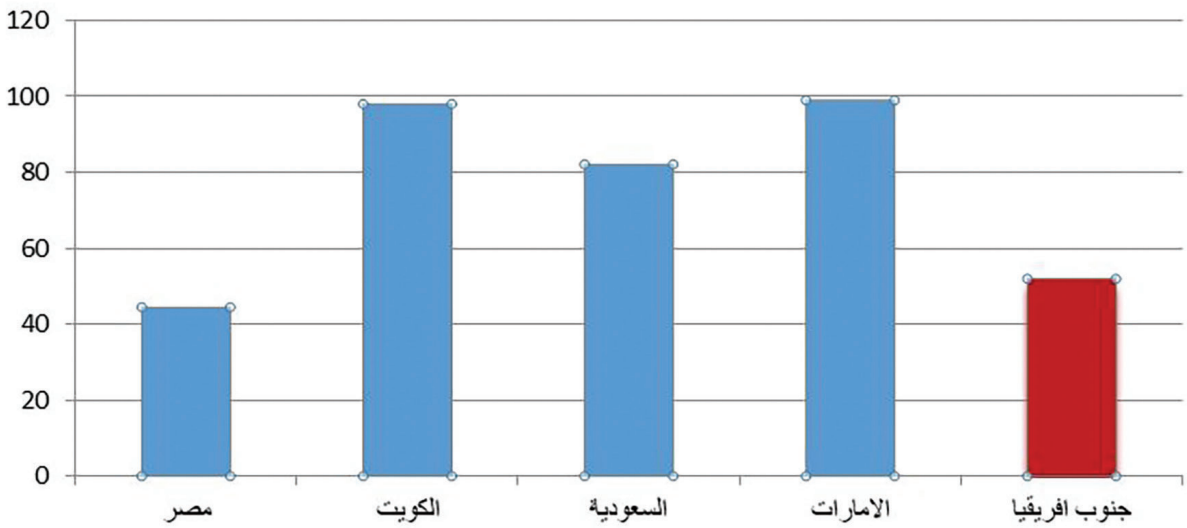


Figure 2: Internet penetration per 100 populations in 2020 (forecast) Source: Internet Word Stats: https://www.internet-worldstats.com/top20.htm

يمكن ملاحظة تناقضات مماثلة من حيث انتشار النطاق العريض حيث أن النطاق العريض المحمول حاليا هو القوة الدافعة لكل عمليات النفاذ عمومًا، ويرجع ذلك إلى الحث على استخدام الجيل الرابع 5G في الهاتف المحمول في جميع أنحاء المنطقة.

وتُعتبر دولة الإمارات العربية المتحدة من بين الدول الأكثر ثراءً وأكثر تقدمًا من الناحية التكنولوجيَّة في منطقة الشرق الأوسط، حيث يرتفع معدل انتشار (الإنترنت) والوصول إلى خدمات النطاق العريض لكثيرٍ من المنازل.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المبادرات الحكوميَّة المختلفة لتسهيل الوصول الرقميّ من قِبَل الجمهور

أمثلة على المبادرات الحكوميَّة

تَعرضُ المعلومات أدناه ستة من أفضل الأمثلة على كيفيَّة قيام الحكومات في مختلف البلدان بتسهيل الوصول الرقميّ إلى الناس في دولهم.

الإمارات

نَفَّذت شركة اتصالات – والتي تُعَدُّ أكبر شركة اتصالات في منطقة الخليج – نظامَ الألياف البصرية الذي يسَّر لمشتركي شركة اتصالات في البلاد مشاهدة قنوات التلفاز على أجهزة (الكمبيوتر) في أي مكان في البلاد ومن تحويل استقبال المكالمات من الهاتف المحمول إلى الهاتف الأرضيّ في المنزل.

كما أطلقت شركة اتصالات برنامج e-Life ، وهو مزيج من الخدمات تُستخدم عبر شبكة الألياف البصريَّة. فهو يُوفر خدمة (الإنترنت) بنظام النطاق العريض، وخدمة الهاتف الثابت وكابل للتلفاز في حزمة خدميَّة واحدة. وكان التحدي الذي تواجهه شركة اتصالات هو إمكانية دمج كل هذه الخدمات في شبكة واحدة في نفس الوقت مع تقديمها بجَوْدة عالية.

كما نفذت شركة اتصالات حاليًا نظام الجيل الرابع (5G) لسرعة نقل البيانات، والصوت و(الفيديو) عبر هواتف المحمول، وتهدف إلى توفير تغطية بنسبة (100%) في المناطق مرتفعة الكثافة السكانيَّة في الإمارات، بما في ذلك الشواطيء والجُزُر.

وتسعى شركة اتصالات حاليًا إلى توسيع شبكتها الخاصَّة بنظام الألياف البصريَّة لتجعل أبوظبي، عاصمة الإمارات، مُتصِلة جميعها عبر كابل الألياف البصريّة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تقرير: تصنيف دولة الإمارات العربيَّة المتحدة في العديد من الدراسات الدوليَّة

لقد ثبتت إيجابية أداء تكنولوجيا المعلومات والاتصالات في دولة الإمارات من وجهة النظر الدوليَّة من خلال العديد من الدراسات الدوليَّة المنشورة حديثًا من مجموعة متنوعة من مؤشّرات تكنولوجيا المعلومات والاتصالات.

كما أكد مؤشر «التنمية الاقتصادية المستدامة 2018م» الصادر عن مؤسسة «بوسطن كونسلتنج جروب» الاستشارية العالمية، حصول دولة الإمارات على المرتبة الأولى عالميًا في جودة البنى التحتية، وهو أحد العناصر الرئيسية للتقرير، فيما احتلت المركز الـ (28) في الترتيب العام على مستوى العالم، متقدمة على كوريا الجنوبية وإيطاليا وتركيا والبرازيل وماليزيا. وفي فبراير الماضي، كشفت دراسة صادرة عن الأمم المتحدة بشأن الحكومة الإلكترونية 2018م، حصول دولة الإمارات على المرتبة الثانية عالميًا على مؤشر جودة البنية التحتية للاتصالات، والسادسة عالميًا على صعيد جودة الخدمات عبر شبكة (الإنترنت)، كما حققت أعلى مرتبة على مؤشر تنمية الحكومة الإلكترونية بين دول مجلس التعاون لدول الخليج العربية.وقد صنفت مؤشرات تكنولوجيا المعلومات والاتصالات الإمارات العربيَّة المتحدة في المرتبة الأولى من بين جميع الدول العربيَّة في ما يلي:

- عرض نطاق (الإنترنت) لكل مستخدم.
- مؤشر المشاركة الإلكترونية.
- تواصل الشركات مع المستهلك عبر (الإنترنت).
- إجمالي خوادم (الإنترنت) الآمن.
- انخفاض معدلات قرصنة البرمجيات، كنسبة من إجمالي البرامج المحملة.
- قوة المنافسة المحلية.

وعالميًا، احتلت دولة الإمارات العربية المتحدة المرتبة:

- الأولى عربيًا والتاسع عالميًا في محور "الجاهزية للمستقبل الأولى في تغطية شبكة الهاتف المحمول – النسبة المئوية للسكان المشمولة بالتغطية - (مشترك مع عدة دول).
- (12) و تصعد من المركز (17) إلى (12) عالميًا في التصنيف العام لتقرير 2019م.
- الأولى عربيًا في كل المحاور الثلاثة الرئيسة وهي "المعرفة" و"التكنولوجيا" و"الجاهزية للمستقبل".
- الأولى عالميًا في مؤشرات "توفر الخبرات الدولية" و"مرونة الشركات" و"استخدام البيانات الضخمة والأدوات التحليلية" و"الشراكة بين القطاع الحكومي والخاص".
- الأولى في استخدام تقنية المعلومات والاتصالات والفعاليَّة الحكوميَّة.
- الأولى في تغطية شبكة الهاتف المحمول - النسبة المئوية للسكان المشمولة بالتغطية (مشترك مع عدة دول).
- الاولى في نجاح الحكومة في تعزيز تكنولوجيا الإتصالات والمعلومات.
- الثانية في المشتريات الحكومية لمنتجات التكنولوجيا المتقدمة.
- الرابع في معدل انتشار الهاتف المتحرك.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

- الرابع في أثر تكنولوجيا الإتصالات والمعلومات في الوصول للخدمات الأساسية،
- الرابع في استخدام تكنولوجيا الإتصالات والمعلومات في المعالمات بين الشركات.

هيئة تنظيم الاتصالات (http://www.tra.gov.ae/UAE_rankings.php).

تكافؤ الفرص الإلكترونيَّة التي يشارك فيها ذوو الاحتياجات الخاصّة

يجد الأشخاص من ذوي أصحاب الهمم صعوبة أكبر في الوصول إلى المعلومات من (الإنترنت). غير أن وزارة التنمية الاجتماعية في الإمارات تعمل على وضع خطط استراتيجية وسياسات محددة تسمح للاشخاص من ذوي أصحاب الهمم بالدخول الى المعرفة بل واستخدام مواقع (الإنترنت) وتطبيقاتها بواسطة هواتفهم الذكية.

وتهدف هذه البادرة الى تمكين ذوي أصحاب الهمم من الحصول على المعلومات بصرف النظر عن مصادرها. ومع التركيز على مفهوم وممارسة الحكومة الذكية سوف يتمكن ذوي أصحاب الهمم من الحصول على المواد المكتوبة والسماعية والمرئية المناسبة للمحتوى الرقمي. وتعتبر هيئة الطيران المدني في دبي من أوائل المؤسسات التي عملت على هذا المفهوم حيث سعت إلى تصميم مواقع خاصة لخدمة المكفوفين على وجه الخصوص وبيان كيفية التواصل معهم.

يعتبر ادخال التعليم الذكي في المدارس الحكومية احد الجوانب التي تعود بالفائدة على ذوي أصحاب الهمم ، حيث ساهمت تقنيات التعليم بما نسبته (80%) من العملية التعليمية الكلية لهذه الفئة، وساعدتهم في التغلب على العقبات التي تقف في طريق استقلاليتهم وذلك بتسهيل عملية التواصل الاجتماعي وزيادة قدرتهم على استيعاب المهارات الحياتية اليومية وتطبيقها، مما كان له اثر ايجابي على تحصيليهم الاكاديمي والنفسي، ومنظورهم الاجتماعي والاقتصادي. كذلك يعتبر التعليم الذكي خطوة مهمة في تمكين هذه الفئة من متابعة الادوات الإلكترونية التي تساعدهم في التغلب على اعاقاتهم والتعامل مع التعليم بشكل اكثر انتاجية. إن عولمة التعليم تعني توفير ما يلزم لربط الطلبة بمصادر المعرفة على مستوى العالم لفتح آفاق جديدة لهم باستخدام انواع متعددة من المحفزات، إلا ان ذلك لا يجب ان يتعارض مع ضرورة الانتباه إلى ان المواد والبرامج المختلفة التي يتم تنزيلها من (الإنترنت) يجب ان تكون ذات محتوى مفيد وتواكب تطورات العملية التعليمية.

إن برنامج التحديث للحكومة الإلكترونية في أبوظبي يساعد الهيئات المحلية في توفير خدماتها من خلال عدة قنوات تقنية مثل: صفحة الحكومة الإلكترونية، ومركز الاتصال الخاص بحكومة أبوظبي (800555)، صفحة وظائف حكومية في أبوظبي. كما يوفر مركز أبوظبي للانظمة الإلكترونية والمعلومات (ADSIC) خيارات متعددة للاشخاص ذوي أصحاب الهمم لجعلهم اعضاء فاعلين في التنمية المحلية من خلال مبادرات ومعايير تضمن الالتزام الدائم من قبل مزودي الخدمة بتقديم اقصى فائدة ممكنة. وقد اطلق مركز أبوظبي للانظمة الإلكترونية والمعلومات خدمة جديدة للتوظيف (على صفحة وظائف حكومية) تساعد ذوي أصحاب الهمم على ايجاد الوظائف واستخدام الخدمات الإلكترونية المتقدمة التي توفرها حكومة أبوظبي.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

يمكنك ايجاد كافة الاعدادات التي تختص بذوي أصحاب الهمم على كمبيوترك، اذهب إلى لوحة التحكم ثم إلى مركز الدخول السهل.

يمكن تقسيم المصابين بهذه الإعاقات إلى أربعة أنواع رئيسية هي:

1. الإعاقة الحركيَّة.
2. الإعاقة البصريَّة أو العمى.
3. الإعاقة اللُّغويَّة والإدراكيَّة.
4. إعاقة السمع والصمم.

المعلومات الواردة أدناه تُفصّل المشاكل التي يواجهها أصحاب الهمم ، وكذلك ما يمكن القيام به أو أنه قد تم القيام به من أجل مساعدتهم على الوصول واستخدام (الإنترنت).

الإعاقة الحركيَّة

يمكن أن تؤدي الإعاقات الحركية إلى خلق الصعوبات أمام المستخدمين خاصة عند الرغبة في استخدام الماوس. والسبب في ذلك يكمن في أن معظم الأزرار يكون حجمها صغيرًا، ويمكن أن يكون من الصعوبة بمكان النقر على تلك الأزرار. ومع ذلك، يمكن أن يتم التغلب على هذه المشكلة من خلال استخدام أوامر لوحة المفاتيح بدلاً من الماوس. على سبيل المثال، يمكنك استخدام مفتاح علامة الجدولة (Tab) للتنقل، أو يمكنك استخدام مفاتيح الاختصار مثل Ctrl+C للنسخ. ومن المشاكل التي يمكن أن تظهر أنه قد لا يمكن الوصول إلى بعض صفحات (الويب) من خلال استخدام أزرار لوحة المفاتيح. ومع ذلك، فطالما كان بإمكان أصحاب الهمم حركيًا التعامل مع واجهة المستخدم واستخدامها، فسيكون بإمكانهم استخدام شبكة (الإنترنت) بشكل أسهل من خلال الاعتماد بشكل تام على الماوس .

الإعاقة البصريَّة أو العمى

إحدى الطرق الشائعة التي يعتمد عليها المعاقون بصريًا للوصول إلى المعلومات المعروضة على الشاشة تتمثل في تكبير أو تحسين وضعية المنطقة المرغوب التركيز عليها. فمن خلال تعديل الخطوط، والمؤشرات، والألوان، يمكن للمستخدمين عرض واستخدام البرامج بشكل أسهل حيث يمكنهم رؤية ما يتم عرضه على الشاشة بشكل أفضل. وبالتالي، فإن الأشخاص المصابين بضعف البصر يمكن أن يحتاجوا إلى تكبير الشاشة للتمكن من الرؤية بشكل أفضل. وبالتالي، فإنهم قد يرغبون في الإبقاء على بساطة التفاصيل الموجودة في الصفحة، مع توافر التباين الكافي. أما العيب فيكمن في أنهم لن يتمكنوا من رؤية الصفحة كاملة مرة واحدة.

تتوافر للأشخاص المصابين بعمى الألوان فرصة أفضل للوصول إلى البرامج عندما تكون الرموز اللونية مكررة مع الوسائل الأخرى لتوصيل المعلومات. كما يجب أن تكون البرامج قادرة أيضًا على العمل في الوضع أحادي اللون، بينما يتم استخدام الألوان التي تختلف في درجة القتامة. كما يمكن لبرامج قراءة الشاشة مساعدة المستخدم على قراءة صفحات (الإنترنت) من خلال تحويل النص المعروض إلى صوت.

الإعاقة اللغوية والإدراكيَّة

يحتاج الأشخاص المصابون بهذا النوع من الإعاقة أن تكون التصميمات بسيطة ومتسقة. وهذا يعني أنه يجب أن يتم تصميم التصميمات بالطريقة الأكثر بساطة ومباشرةً. كما أنه يمكن مساعدتهم أيضًا من خلال توفير برنامج قراءة للشاشة لهم أثناء استخدام شبكة (الإنترنت).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

إعاقة السمع والصَّمم

قد يعاني بعض الأشخاص من عدم القدرة على الاستماع إلى الصوت بسبب أشكال مختلفة من الإعاقات السمعية. وبسبب هذه المشكلة، ينصح بأن تحتوي كل المعلومات السمعية على نماذج مرئية أيضًا.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تمرين

1. **تحتاج إلى تسليم مهمة على (الإنترنت) بشكل عاجل، إلا أن مقهى (الإنترنت) المحلي مغلق. ولاحظت أنه توجد نقطة وصول غير مؤمنة لدى أحد الجيران. ما الذي يجب عليك فعله؟**

   أ. تقوم باستخدامها، فهي وسيلة وصول متاحة للجميع.

   ب. تقوم باستخدامها وطلب الموافقة على هذا الاستخدام في وقت لاحق.

   ج. طلب الموافقه من الجار قبل إستخدام نقطة الوصول.

   د. تقوم باستخدامها وتعويض الجار في وقت لاحق.

2. **يمكن أن يكون توافر شبكة (الإنترنت) في المدرسة مفيدًا للغاية لتحسين العملية التعليمية، إلا أنه يجب على الطلبة استخدام شبكة (الإنترنت) بشكل يتسم بالحكمة. أي خيار يناسب العبارة "استخدام شبكة (الإنترنت) بشكل يتسم بالحكمة " بأفضل طريقة ممكنة فيما يتعلق ببيئة المدرسة؟**

   أ. يمكن للطلاب رفع ونشر مقاطع فيديو.

   ب. يمكن للطلاب استخدام (الإنترنت) من أجل اللعب مباشرة على (الإنترنت).

   ج. يمكن للطلاب التفاعل مع بعضهم البعض وتبادل المذكرات.

   د. يمكن للطلاب تحميل وتثبيت برمجيات النظير للنظير.

3. **أي خدمة من الخدمات المتوفرة على (الإنترنت) قانونية ومقبولة اجتماعيًا؟**

   أ. تحميل الأفلام من أحد مواقع الاستضافة غير القانونية.

   ب. التواصل مع الآخرين باحترام عبر مواقع التواصل الاجتماعي.

   ج. شراء وبيع المنتجات المقرصنة من السوق على (الإنترنت).

   د. مشاركة الملفات عبر نظام النظير للنظير للمواد غير المحفوظة بحقوق طبع ونشر.

4. **قم بتحديد أفضل طريقتين لمساعدة المجتمع المحلي الخاص بك على التمكن من الوصول إلى شبكة (الإنترنت). (اختر طريقتين)**

   أ. إنشاء نادي إلكتروني في المجتمع.

   ب. تشجيع الحملة المجتمعية التي تنادي "بجهاز كمبيوتر لكل منزل".

   ج. توفير التدريب المجتمعي على استخدام أجهزة (الكمبيوتر) و(الإنترنت).

   د. توفير الاتصال عريض النطاق الخاص بك إلى شبكة (الإنترنت) مقابل رسوم ضئيلة للغاية.

   هـ. دفع شركات توفير خدمات (الإنترنت) نحو الانخراط في رعاية اتصالات (الإنترنت) المجتمعية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

5. **أعلنت أم أصيبت بالقلق الشديد عن فقد ابنها. وتم العثور على هذا المراهق فيما بعد في مقهى (للإنترنت) حيث كان يمارس الألعاب المتاحة عبر (الإنترنت) على مدار 48 ساعة".**
ما هو السلوك الذي ينطبق على هذا المراهق بأفضل شكل ممكن؟

أ. تظهر عليه علامات التصفح القهري

ب. بإدمان ممارسة الألعاب متعددة الأطراف على (الإنترنت).

ج. جضرورة فرض قيود قانونية على الألعاب.

د. ضرورة قضاء المزيد من الوقت لكي تصبح لاعبًا أفضل.

الإجابة : 1.ج 2.ج 3.ب 4.أ ه 5.ب

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

02 محْو الأميَّة الإلكترونيَّة

حول هذه الوحدة توفر وحدة محْو الأميَّة الإلكترونيَّة مقدمة إلى التقنيات الرقمية العالمية في القرن الحادي والعشرين. وهي توضح القدرات اللازمة لاستخدام التقنيات الرقمية ومعرفة متى يتم استخدامها ومتى لا يتم استخدامها وكيفية استخدامها. فهي تركز على الأخلاقيات وعملية التعليم فيما يتعلق بالتقنيات واستخدامات التقنيات.

وقد تم تصميم هذه الوحدة لتوفير التعليم التفاعلي للمستخدم النهائي فيما يتعلق بالتقنيات الرقمية. ومن خلال تعليم المستخدمين النهائيين العادات الملائمة والمسئولة أثناء التواجد على (الإنترنت)، والتي يتم توضيحها من خلال دراسات الحالات الفعلية، سيتمكن المتعلمون من تطوير إحساس بالمسئولية والمحاسبة حيال الممارسات التي يقومون بها على (الإنترنت).

ففي هذا العصر، أصبح التعليم المقترن بالتقنيات أمرًا شائعًا في حياتنا اليومية. ولسوء الحظ، ما زال إدراك كيفية استخدام التقنيات بشكل إبداعي وأخلاقي في مراحله الأولى. وفيما بعد في هذه الوحدة، سوف نطلع سويًا على كيفية استخدام التقنيات للبحث عن الموارد والمواد التي يمكن الاعتماد عليه أو تجميعها باستخدام أجهزة مختلفة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أهداف التعلُّم

أهداف هذه الوحدة هي:

- توفير المعلومات للمشاركين حول الطرق الملائمة أو غير الملائمة للكشف عن المعلومات من خلال شبكة (الإنترنت).
- مساعدة المشاركين للحصول على إدراك أفضل لكيفية التمييز بين الموارد التي يمكن الاعتماد عليها وتلك التي لا يمكن الاعتماد عليها من شبكة (الإنترنت).
- جعل المشاركين يدركون كيفية تحديد التداعيات الإيجابية والسلبية لامتلاك مقر رقمي.
- توفير إرشادات حول كيفية التمييز بين الموارد الرقمية محل الثقة وتلك التي لا تحظى بالثقة.
- توفير إدراك أفضل للإجراءات/الأنشطة التي يمكن تصنيفها على أنها تَنَمُّر إلكتروني وتبعاته تجاه المجتمع.

نواتج التعلُّم

في نهاية هذه الوحدة، سوف تكون قادرًا على:

- وصف أدوات وتطبيقات محو الأمية الإلكترونية وقضايا التقنية الرقمية التي قد يحتاجها المستخدم.
- التعرف على الطرق المناسبة عند إجراء الاتصال الرقميّ.
- التفرقة ما بين المصادر الموثوقة وغير الموثوقة على (الإنترنت).
- وصف الآثار السلبية للبصمة الرقميّة.
- وصف عمليات التنمر الإلكتروني وتأثيرها على الضحايا.

قائمة المراجعة

التعليمات:

بعد الانتهاء من قراءة هذه الوحدة، يُرجى إكمال الاستبيان باستخدام المقياس التالي:

المقياس:

1. ليس لدي أدنى معرفة.
2. لدي معرفة محدودة.
3. على دراية وقادر على التوضيح الجيّد.
4. ذو كفاءة وإمكانية على الممارسة الكاملة.

البنود	التحصيل العلمي	قبل	بعد
1	لدي القدرة على تحديد أشكال التقنيات الرقمية وكيف يمكن أن تساعد على تسهيل حياتي اليومية.		
2	أنا أدرك الطرق الملائمة لكشف المعلومات الشخصية الخاصة بي للآخرين على شبكة (الإنترنت).		
3	أنا أدرك كيف يمكن العثور على أفضل الموارد من ناحية المصداقية على الوسائط الرقمية سواء للاستخدام الرقمي أو للاستخدام الأكاديمي.		
4	أنا أعرف ما هي البصمة الرقميّة وتأثيرها علىّ وعلى الآخرين.		
5	أنا أدرك ما هو التنمر الإلكتروني وكيف يمكن تجنب التعرض له.		
6	أنا أدرك القضايا الحالية فيما يتعلق بالتقنيات الرقمية من مختلف أرجاء العالم.		

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

محـوَ الأميَّـة الإلكترونيَّـة هـي القـدرة علـى اسـتخدام التكنولوجيـا ومعرفـة متـى وكيفيَّـة اسـتخدامها بشـكلٍ مناسـبٍ.

"يمكـن تعريـف ثقافـة تقنيـات المعلومـات والاتصـالات علـى أنهـا الاهتمـام والاتجـاه والقـدرة الخاصـة بالفـرد علـى اسـتخدام أدوات الاتصـالات والتقنيـات الرقميـة بالشـكل المناسـب للوصـول إلـى المعلومـات وإدارتهـا ودمجهـا وتقييمهـا، وإنشـاء المعلومـات الحديثـة، والتواصـل مـع الآخريـن بهـدف المشـاركة بشـكل فعـال فـي المجتمـع "

فان فولينجين

لقـد عرفـت منظمـة التعليـم والعلـوم والثقافـة فـي الأمـم المتحـدة اليونسـكو (UNESCO I) لثقافـة الإلكترونيـة بشـكل أكثـر عمقًـا:

"القـدرة علـى التعريـف والإدراك والتفسـير والإنشـاء والتواصـل والحسـاب، باسـتخدام المـواد المطبوعـة والمكتوبـة فيمـا يتعلـق بالسـياقات المتنوعـة. وتشـتمل الثقافـة علـى تواصـل التعليـم فيمـا يتعلـق بتمكيـن الأفـراد مـن تحقيـق الأهـداف الخاصـة بهـم، وتطويـر معارفهـم، وقدراتهـم، والمشـاركة بشـكل كامـل فـي المجتمـع المحيـط بهـم وفـي المجتمـع الأوسـع".

اليونسكو

تطور التقنية الرقمية

هنـاك العديـد مـن الأجهـزة الرقميـة المتنوعـة المتاحـة فـي الأسـواق الآن. لقـد تطـورت التقنيـات مـن الأجهـزة التقليديـة وصـولاً إلـى الأجهـزة الرقميـة متعـددة الأغـراض. علـى سـبيل المثـال: تطـورت الهواتـف مـن الهواتـف السـلكية إلـى الهواتـف المحمولـة، وتطـور البريـد إلـى البريـد الإلكترونـي، وتطـورت الكتـب/ الصحـف المرجعيـة إلـى محـركات البحـث علـى (الويـب). ويتـم توضيـح التطـور المتنـوع للتقنيـات فـي الشـكل التوضيحـي أدنـاه:

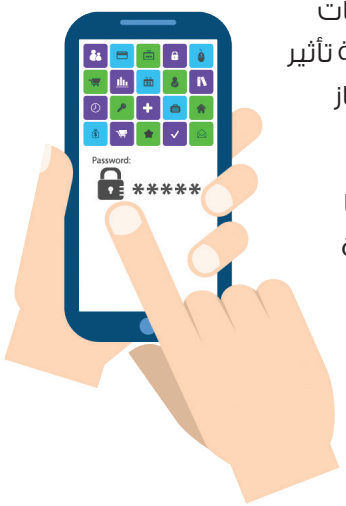
وتسـهل هـذه الأجهـزة الرقميـة متعـددة الأغـراض أنشـطتنا اليوميـة وتتيـح لنـا القـدرة علـى الوصـول إلـى شـبكة (الإنترنـت) فـي أي وقـت، وفـي أي مـكان. ومـع ذلـك، وبـدون الحصـول علـى الإرشـادات الملائمـة، يمكـن أن تتـم إسـاءة اسـتخدام هـذه الأجهـزة مـن قِبَـل مسـتخدميها.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أدوات محو الأمية الرقميّة

إليك أدناه مجموعة متنوعة من التقنيات الرقمية المعاصرة التي يتم استخدامها حاليًا على الصعيد العالمي. كم من هذه التقنيات تمثل جزءًا من حياتك بشكل فعلي؟

الهواتف المحمولة



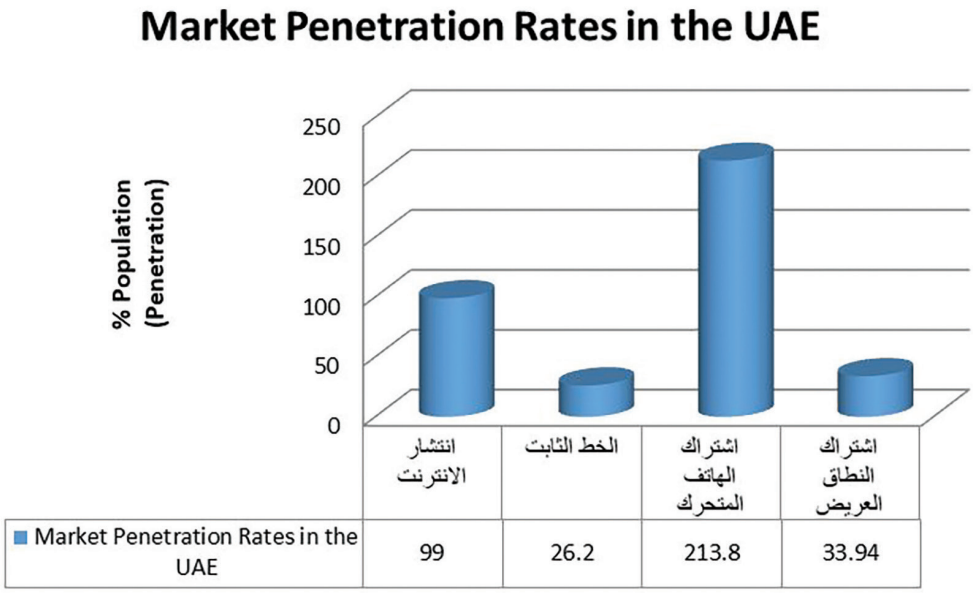
من الهاتف التقليدي القديم، سمح لنا تطور التقنيات بالاستفادة من التقنيات الرقمية على الهواتف المحمولة استفادة تامة. فقد أصبح للهواتف الذكية تأثير أساسي في كيفية إدخالنا واستخدامنا للمعلومات الرقمية وأصبحت جهاز التحكم الشخصي الذي نستخدمه في حياتنا.

فيمكننا القيام بالكثير من الأمور باستخدام الهواتف المحمولة الخاصة بنا مثل: التقاط الصور/مقاطع (الفيديو) عالية الدقة، وإرسال الرسائل المصورة إلى الأصدقاء، وإجراء مؤتمرات (الفيديو) من خلال تطبيقات الجيل الثالث، ووصولاً إلى العثور على الطريق للوصول إلى منازل الأصدقاء والأقارب من خلال استخدام أنظمة تحديد المواقع العالمية (GPS) البسيطة المتاحة في الهواتف الخاصة بنا وبالإضافة إلى ذلك، يتم تزويد الهواتف المحمولة الخاصة بنا بالقدرة على الوصول إلى شبكة (الإنترنت).

فيمكننا استعراض شبكة (الإنترنت)، أو فتح البريد الإلكتروني، أو مراقبة البورصة أثناء التنقل.

وطبقًا لما أوردته هيئة تنظيم الاتصالات، فإن إجمالي المشتركين في خدمات المحمول في الإمارات قد وصل إلى (18.38) مليون مشترك في 2020م، مما يعني أن كل شخص في أكثر الاحتمالات لديه هاتفين نقالين مختلفين. ويمثل ذلك معدل انتشار للنقال لم يسبق له مثيل بما يتجاوز(187%). ونتيجة لذلك، فإن الإمارات ليست فقط الأعلى في الدول العربية بأنها كذلك واحدة من أعلى أسواق الانتشار في العالم! وقد بدأ انخفاض معدل الارتفاع، بالرغم من أنه مازال مرتفع جدًا، في 2020م. أما عن انتشار (الإنترنت) في الإمارات فهو كالتالي:

معدل الإنتشار في السوق الإماراتية



Source http://www. internetworldstats. com/list2. htm#help
Source: http://www. tra. gov. ae/latest_statistics. php

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المكونات الذكيَّة

تتيح لنا التقنيات القدرة على تطوير تطبيقات رقمية صغيرة تعتمد على أجهزة (الكمبيوتر) تعرف باسم "المكونات الذكية".

وتشتمل التطبيقات الحالية "المكونات الذكية " على بطاقات الهوية، وبطاقات الائتمان، والبطاقات البنكية، وجوازات السفر، وغير ذلك الكثير. وتسمح تقنية المكونات الذكية بتخزين الكود / البيانات الخاصة بالمستخدم على كائن.

وتشتمل التطبيقات الحالية "المكونات الذكية" على بطاقات الهوية، وبطاقات الائتمان، والبطاقات البنكية، وجوازات السفر، وغير ذلك الكثير. وتسمح تقنية المكونات الذكية بتخزين الكود/البيانات الخاصة بالمستخدم على كائن.

بطاقة هُوية الإمارات

بطاقة هُوية الإمارات بطاقة بلاستيكيَّة تُستَخدَم كوثيقة سفر ما بين دول مجلس التعاون الخليجيّ بدلاً من جواز السفر.

تحتوي واجهة البطاقة على اسم حاملها وجنسيته وصورته ورقم التعريف الشخصيّ المكوَّن من (15) رقم. كما توجد في واجهة البطاقة رقاقة إلكترونيَّة تحمل بيانات عن حامل البطاقة مثل: صورة الوجه، والشهادات الرقميَّة والبصمات.

أما ظهر البطاقة فيحمل تاريخ الميلاد والجنس وتوقيع حامل البطاقة بالإضافة إلى رقم وتاريخ انتهاء البطاقة.

Figure 1: UAE ID Card
Source: http://www. itp. net/580761-national-id-card-to-allow-e-payments-in-future

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الفوائد

تعتبر بطاقة الهُوية وسيلة آمنة ودقيقة للتأكد من هُوية الشخص. فهي تمكن حامل البطاقة من الاستفادة من التعامل مع جميع المنظمات الحكومية وبعض المنظمات غير الحكومية والتي تتطلب إثبات شخصية.

وليس ذلك فحسب، وإنما تعزز بطاقة الهُوية الشعور بالانتماء، وحماية الهُوية بالإضافة إلى السهولة واليسر عند تشغيل قاعدة بيانات متكاملة.

تلفاز الأقمار الصناعية

سمح التلفاز التقليدي للمستخدمين بعرض مجموعة محددة فقط من القنوات التلفازية. اليوم، يمكن أن نشاهد برامج التلفاز من مجموعة متنوعة من قنوات التلفاز التي يمكن اختيارها. فمن خلال بث إشارات التلفاز الرقمية من خلال الأقمار الصناعية، يمكن لأي شخص يمتلك جهاز تلفاز مزود بجهاز تشفير لإشارات الأقمار الصناعية الاستمتاع بهذه الخدمات بغض النظر عن موقع هذا الشخص. ويتم توفير هذه الخدمات بشكل طبيعي من قبل شركات توفير برامج التلفاز المحلية مقابل الحد الأدنى من الرسوم.

وحدة الألعاب الطرفية

سمح تطور مشغل الألعاب بحلول الألعاب ثلاثية الأبعاد (3D) محل الألعاب ثنائية الأبعاد (2D). مما سمح لوحدة الألعاب الطرفية بأن تطغى الألعاب ثلاثية الأبعاد على الألعاب ثنائية الأبعاد. وتتيح آليات الصور الأكثر وضوحًا والأكثر واقعية والصوت المحسن للمستخدمين الاستمتاع بالألعاب بأفضل شكل ممكن. فمعظم الوحدات الطرفية عبارة عن ألعاب (DVD) تسمح للمستخدم بالاستمتاع بصور أكثر واقعية، ناهيك عن كونها أكثر تفاعلية.

تطبيقات محو الأمية الرقمية

يتواصل الأشخاص في مختلف أرجاء العالم من خلال شبكة (الإنترنت) باستخدام رسائل البريد الإلكتروني، والرسائل الفورية، ومواقع الشبكات الاجتماعية، وغير ذلك. وبناءً على الإحصاءات العالمية لشبكة (الإنترنت) لعام 2020م، فإن العدد الأكبر لمستخدمي (الإنترنت) في العالم يأتون من قارة آسيا (50.3%)، ثم تأتي قارة أوروبا بعدها (15.9%). ويتم تلخيص التوزيع الإجمالي حسب المناطق العالمية حسب الشكل الذي امامك:

مستخدمو (الإنترنت) في التوزيع العالمي حسب المناطق العالمية – 2020م

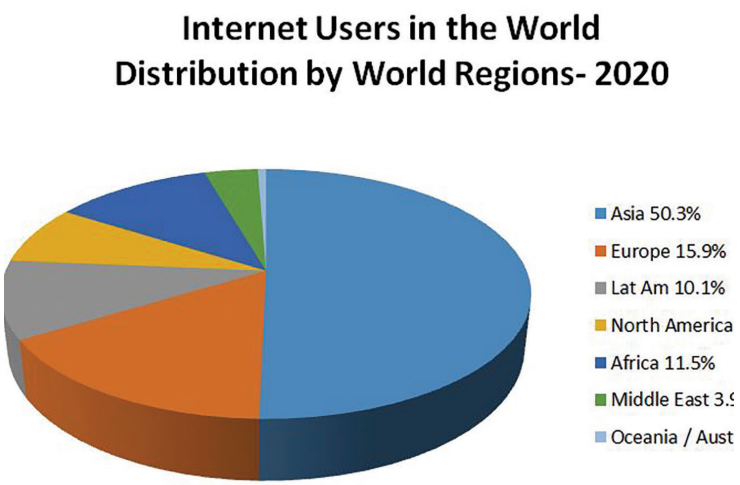


Figure 2: Internet Users in the World
Source: http://www. internetworldstats. com/stats. htm

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

نظام (ويب 2)

نظام (Web 2.0) هو الجيل الثاني من (الإنترنت). كانت بدايته بالصفحات الثابتة، أصبح الآن أكثر ديناميكية بمحتويات المشاركة والتواصل الاجتماعيّ. فأصبح المستخدمون هم معدّي المحتوى وليس فقط مجرد متصفحين أو مستخدمين له. كما أنه يمكن كل شخص من إنشاء موقعه الخاص به، لتحميل ملفات الصوت و(الفيديو)، والصور، وآخر المعلومات وإتمام العديد من المهام الأخرى.

التراسل الفوري

تعد الرسائل الفورية، أو التي تشتهر بين الناس بالاختصار (IM)، أحد أنواع خدمات الاتصالات التي تتيح لك القدرة على إنشاء نوع من أنواع غرف المحادثة الخاصة مع شخص آخر لكي تتمكن من التواصل معه في الوقت الفعلي عبر شبكة (الإنترنت).

وبشكل نموذجي، ينبهك نظام الرسائل الفورية عندما يتواجد أحد الأشخاص الموجودين في قائمتك الخاصة على (الإنترنت) في حالة اتصال. ثم يمكنك بدء جلسة محادثة مع هذا الشخص بعينه.

كما تسمح معظم برامج الرسائل الفورية أيضًا للمستخدمين بالتواصل شفويًا ومن خلال المؤتمرات الهاتفية المصورة. ومن خلال كل هذه الميزات، يمكن أن يتواصل المستخدمون في مختلف أرجاء العالم مع بعضهم البعض عبر الوسائط الإلكترونية.

مواقع الشبكات الاجتماعية

موقع الشبكات الاجتماعية هو موقع يوفر مجتمع افتراضيّ لأشخاص ذوي اهتمامات مشتركة للتواصل وتبادل الآراء والمعارف. كما يمكن اعتبارها خدمة تركز على بناء الشبكات أو العلاقات الاجتماعية بين الناس. التسجيل غالبًا ما يكون مجانًا. أمثلة على بعض مواقع الشبكات الاجتماعيّة مثل: (ال(فيس بوك)) و(تويتر) بالإضافة إلى العديد من المواقع.

تلعب الشبكات الاجتماعيَّة دورًا واضحاً في تشكيل مشهد الإعلام الاجتماعيّ في الإمارات. حيث يشارك حوالي (99%) من السكان مواقع التواصل الاجتماعي ويعد موقع (youtube) هو الأكثر استخدامًا بنسبة (88%) يليه (فيسبوك) و(واتس آب) بنسبة (79%) (طبقًا لإحصائيات العام 2020م). وبصرف النظر عن الاستخدامات الواضحة كوسيلة من وسائل التواصل الدائم بزملاء الدراسة والبقاء على اتصال مع الأصدقاء، فقد استُخدمت مواقع الشبكات الاجتماعيَّة كوسيلة لنشر المعلومات عن مختلف القضايا والأحداث الدوليَّة.

بعض التطبيقات الشهيرة في الإمارات ، على سبيل المثال:

- (يوتيوب): يشكل استخدام (يوتيوب) في الإمارات العربية المتحدة نسبة (99%) من مستخدمي (الإنترنت) حاليًا.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

- (فيس بوك) و(واتس آب): تظهر النتائج أن حوالي (78%) يستخدمون خدمات (فيس بوك) أو (واتس آب).
- التطبيقات الأخرى :تلي التطبيقات السابقة تطبيقات (انستجرام) بنسبة (68%) و(فيس بوك ماسنجر) بنسبة (62%) و(تويتر) بنسبة (53%) و(لينكد إن) بنسبة (45%)، إضافة لتطبيقات وسائل التواصل الاجتماعي الأخرى المستخدمة داخل الإمارات ولكن بنسبٍ أقل.

مواقع (الفيديو) الاجتماعية

توفر مواقع (الفيديو) الاجتماعية الوصول إلى ملفات (الفيديو) التي يقوم المستخدمون بتحميلها إلى المواقع في جميع أنحاء العالم.

https://vimeo.com

http://www.youtube.com

هناك وفرة كبيرة من مواقع مشاركة (الفيديو) في الإمارات، ولكن العديد منهم لديه عدد كبير من الجماهير الذين يتابعونه. ويُعد موقع الـ (يوتيوب) هو الأكثر شيوعًا بين القنوات الرئيسية. فهو ثاني أكثر موقع يتم الدخول عليه في الإمارات بعد جوجل، وهو يستخدم للبحث بشكل أساسي عن الموسيقى و(الفيديو) والاشتراك في القنوات الشرق أوسطية الشهيرة. ومن ضمن المواقع الأخرى الشهيرة التي يتم الدخول عليها بشكل متكرر (سيديريل) و(فيدوب).

التطبيقات عبر (الإنترنت)

الأعمال التجارية الإلكترونية

لقد قام معظم التجار بنشر المنتجات التي يقومون بإنتاجها على شبكة (الإنترنت) لخلق سوق أكثر اتساعًا، ولعمل إستراتيجية اتصالات أفضل، أو حتى لتسهيل التعاملات. ويمكن أن يشاهد المشترون السلع التي يرغبون في شرائها ويدفعون للبائع من خلال بطاقات الائتمان و(e-Dirham) لدفع الرسوم الحكومية وغير الحكومية مثل: (souq.com and dubizzle.com amazon.ae and dubizzle.com).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الحكومة الإلكترونية

الحكومة الإلكترونية، والتي يشار إليها اختصارًا باللغة الإنجليزية باسم (e-Government)، هي عبارة عن مصطلح يصف استخدام التقنيات لتسهيل تشغيل الأعمال الحكومية ونشر المعلومات والخدمات الحكومية.

وتستخدم الحكومات في مختلف أرجاء العالم حاليًا منصات تتاح عبر (الإنترنت) لتسهيل وصول العملاء إلى البرامج والأنشطة الحكومية. ويساعد ذلك المسئولين الحكوميين على الاقتراب بشكل أكبر من الشعوب، وبالتالي يتم خلق المزيد من التفاهم تجاه تخطيط ومبادرات الحكومة للمجتمع.

الإضافة إلى ذلك، يمكن للمستخدمين أيضًا عرض الأنشطة والأخبار التي يتم تحديثها للوكالات والمؤسسات الحكومية. ويمكن للمستخدمين تنزيل النماذج، والتقدم بالطلبات، وتقديم الشكاوي، وحتى دفع الضرائب عبر (الإنترنت). وفيما يلي بعض الأمثلة لبوابات الحكومة على (الإنترنت):

- (https://u.ae) البوابة الرسمية لحكومة الامارات.
- (www.tamm.abudhabi) حكومة أبوظبي.
- (https://secureportal.dubai.gov.ae) حكومة دبي.

التعليم الإلكتروني

التعليم الإلكتروني، والذي يشار إليه اختصارًا باللغة الإنجليزية بالاسم (e-Learning)، عبارة عن طريقة جديدة للحصول على المعرفة والمعلومات من خلال الاستفادة من تقنيات المعلومات والاتصالات. فهو بمثابة إعادة اختراع للتعليم والتعلم في عالم رقمي.

واختصارًا، فهو يعني التعليم المعتمد على شبكة (الإنترنت) أو الشبكات. ويساعد التعليم الإلكتروني على تحويل غرفة الدراسة التقليدية إلى عملية تعليمية تتسم بالإثارة وتتيح للمعلمين والمتعلمين على السواء استخدام المهارات والأدوات الجديدة لتحقيق النجاح في مجتمع معلوماتي.

وقد أطلقت معظم المؤسسات التعليمية في مختلف أرجاء العالم أنظمة تعليم عبر (الإنترنت) مثل: (Blackboard)، (moodle) و(edmodo) حيث يتفاعل الطلبة مع مدرسيهم/محاضريهم من خلال منصات على (الإنترنت). وفيما يلي بعض الأمثلة عن بوابات التعلم على (الإنترنت):

- (Hamdan Bin Mohammed University) - (https://www.hbmsu.ac.ae).
- (Khalifa emporment programs for students) – (Aqdar.cyberc3.ae).
- (Khalifa University) –(https://www.ku.ac.ae).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الوظائف الإلكترونية/المستقبل المهني الإلكتروني

بشكل تقليدي، للبحث عن وظيفة، يجب على الشخص البحث في الصحف، أو في إعلانات التوظيف، أو في مجلات التوظيف. وللتقدم للوظائف، قد يتوجب عليك ملء النماذج، وكتابة وطباعة خطابات التقدم لشغل الوظيفة، وتقديم تلك النماذج من خلال شركة نقل أو باليد إلى شركات التي يحتمل العمل بها.

أما اليوم، وبسبب تقنيات المعلومات والاتصالات، يمكن للأشخاص البحث بكل سهولة عن الوظائف في مختلف أرجاء العالم عبر شبكة (الويب). ويوجد المئات من المواقع المدخلية الدولية المخصصة للبحث عن الوظائف المنتشرة عبر (الإنترنت) والتي يمكن أن يسجل المستخدمين أسماؤهم بها. فبكل بساطة، ومن خلال ملء التفاصيل الشخصية، والتعليمية، وتفاصيل العمل للشخص، تقوم البرامج الموجودة على هذه المواقع بالبحث عن الوظيفة التي تناسبك. إن الأمر بمنتهى البساطة!

- (http://www.bayt.com).
- (https://recruitgulf.ae).
- (https://www.vacancies.ae/jobs/jobs-in-abudhabi).
- (http://www.manpower.com).

قضايا التكنولوجيا الرقميّة

علاوة على الفوائد العديدة للتكنولوجيا الرقمية الجديدة، برزت العديد من القضايا الجديدة المتعلقة بالأخلاق والصحة والملكية (لتسمية بعضها). تم وصفها كالتالي:

1. التعدي على حق الطبع والنّشر.
2. سرقة الهوية وتزوير بطاقات الائتمان.
3. القواعد والأحكام المتعلقة ب(الإنترنت) والوسائط المتعددة القديمة.
4. الثقة في المصادر الموجودة على (الإنترنت).
5. قضايا السلامة والصحة.
6. الوصول غير المصرح به.
7. التهديد الإلكترونيّ.
8. اضطرابات إدمان (الإنترنت).

التعدي على حق الطبع والنّشر

إن مسائل حقوق الطباعة والنشر هي المشاكل الأكثر شيوعًا فيما يخص موارد (الإنترنت). يقوم العديد من المستخدمين بتحميل واستخدام المواد المنشورة على (الإنترنت) دون معرفة أنه ينبغي عليهم احترام مالك هذه المواد المحمية بحقوق الطبع والنشر.

سرقة الهوية وتزوير بطاقات الائتمان

سرقة الهوية وتزوير بطاقات الائتمان يتسبب فيها المفترسين ممن يقومون بسرقة هوية الآخرين واستخدامها في الإساءة للغير وتدمير سمعتهم.

فيما يلي بعض الأمثلة عن كيفية قيام المفترسين بتزوير البطاقات:

- سرقة البطاقات.
- التقاط بيانات حساب البطاقة المخزنة على الشريط المغناطيسيّ باستخدام أجهزة التلصص.
- إنتاج بطاقات مزيفة باستخدام بيانات حساب البطاقة.
- إجراء انطباعات زائفة.
- استخدام رقم البطاقة بطرق غير مصرح بها.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

بعض الحالات في الإمارات تستهدف كذلك اجهزة الصراف الآلي و رقم تعريف الهُوية الشخصي لحامل البطاقة باستخدام كاميرات صغيرة خفية. المصارف في البلد تشدد على عملائها بشأن حماية البطاقة وتعطيهم النصائح لتجنب المحتالين وتعرفهم بالحيل الاحتيالية.

قانون جرائم تقنية المعلومات في الإمارات

وفقًا للمادة رقم (12)، أي شخص يُدان بالحصول على بيانات بطاقة ائتمان أو بيانات من أي بطاقات إلكترونية أخرى باستخدام (الإنترنت) أو أي وسيلة عالية التقنية، يُعاقب بالسجن أو التغريم. إذا وقع الأمر بنية استخدام البطاقات الائتمانية أو الإلكترونية لأخذ أموال شخص آخر أو استغلال الخدمات المتاحة له، يُسجن من يُدان بذلك مدة لا تقل عن(6) أشهر، ويُغرم غرامة لا تقل عن (100.000) درهم ولا تتجاوز (300.000) ألف درهم أو إحدى العقوبتين.

هل يمكن أن تكون الموارد المتاحة على (الإنترنت) محل ثقة؟

تُعتبر سلامة موارد (الإنترنت) أمرًا هامًا جدًا. على سبيل المثال، قد تجد الآلاف من الموارد على شبكة (الإنترنت) من عملية بحث واحدة فقط على (الإنترنت). ولكن هل يُمكن الوثوق في هذه الموارد وهل تتمتع بالمصداقيَّة لاستخدامها كمراجع أم لا؟

والسبب في ذلك هو أن المعلومات المتاحة عبر (الإنترنت) يمكن أن تكون غير دقيقة ويمكن أن تحتوي على دعاية تتعلق بالأنشطة الإجرامية. وتساعد القدرة على تقييم نزاهة الموارد المتاحة على (الإنترنت) على تجنب المعلومات الخاطئة، والدعاية، والحيل التي تنتشر بشدة على شبكة (الإنترنت).

إذا كنت متيقنًا من مصداقية مصدر المعلومات أو مؤلفيها حينها تعتبر المعلومات موثوقة.

متى يمكن أن تضع ثقتك في موقع ويب؟

كيف يمكن أن تدرك أن مواقع (الويب) التي تستعرضها توفر معلومات محل ثقة بالفعل؟ إذا كنت تشك في موقع (الويب)، وكنت تحتاج إلى إرشادات، ففكر في إجابات تلك الأسئلة:

- هل موقع (الويب) مملوك لشركة أو منظمة شهيرة؟
- هل هناك طريقة للاتصال بشخص ما عبر الهاتف أو البريد الإلكتروني؟
- إذا لم تكن تعرف الموقع، فهل لديك معلومات أخرى يمكن أن تساعدك على التقرير؟

كيف تَعرِف إذا ما كانت صفحة (الويب) آمنة أم لا؟

نظرًا لوجود الملايين من المواقع التي تنتشر على (الإنترنت)، فإنك تحتاج إلى أن تكون حذرًا من مرسلي الرسائل العشوائيَّة والمخادعين. هؤلاء هم المفترسون ممن يستغلون فرصة جَهلك لمكاسب شخصيَّة خاصة بهم. ولذلك، فأنت تحتاج إلى معرفة كيف تبحث عن مواقع آمنة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

نصائح: كيفية معرفة ما إذا كان الموقع غير جدير بالثقة

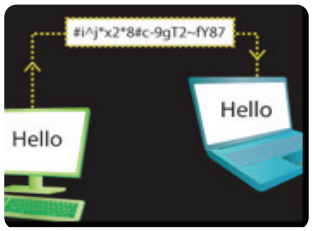
- إذا تم إعلامك بموقع (الويب) من خلال رسالة بريد إلكتروني من شخص لا تعرفه.
- إذا كان الموقع يعرض محتويات مسيئة، مثل: المواد الإباحية أو المواد غيرالقانونية.
- إذا كان يقدم عروضًا تبدو خيالية للغاية لدرجة يصعب معها تحقيقها، مما يشير إلى احتمالية وجود حيل أو إذا كان يبيع منتجات غير مشروعة أو تعرضت للقرصنة.
- إذا تم إغراؤك للدخول إلى الموقع، ووجدت المنتجات أو الخدمات ليست كما كنت تتوقع.
- إذا طلب منك إدخال رقم بطاقة الائتمان الخاصة بك كوسيلة للتحقق من هويتك، أو إذا طلب منك إدخال معلومات شخصية يبدو أنها غير ضرورية.

يوجد مؤشران تعرف منهما إذا ما كانت صفحة الإنترنت آمنه:

- مواقع (الويب) التي تبدأ بـ (https).
- أيقونة القفل (Lock).

مواقع الويب التي تبدأ بالبادئة (https)

معظم مواقع (الويب) تبدأ بالحروف (http)، ومن المستحيل تحديد هل مواقع الويب هذه آمنة أم لا. أما إذا كان عنوان (URL) موقع (الويب) يبدأ بالبادئة (https)، فهذا يعني أن موقع (الويب) يوفر اتصالاً آمنًا للمستخدمين.

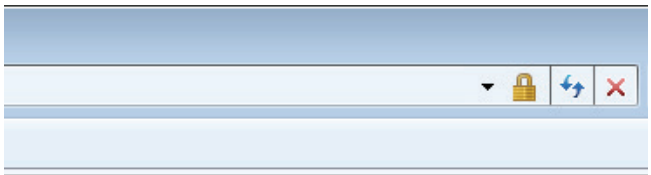


والبادئة (https) هي اختصار للكلمات Hypertext Transfer Protocol (Secure) أي البروتوكول الآمن لنقل النص التشعبي. والهدف الرئيسي لبروتوكول (https) هو توفير التشفير. والتشفير هو عبارة عن طريقة لتحسين أمان رسالة أو ملف من خلال خلط محتوياته بحيث لا يمكن قراءته إلا من قبل شخص لديه مفتاح التشفير الصحيح للتخلص من هذا الخلط.

المفهوم الذي يقوم عليه بروتوكول (https) هو ضمان إنشاء قناة آمنة عبر شبكة غير آمنة.

تعرض الصورة موقع ظهور البادئة (https).

أيقونة «Lock»



كل مواقع (الويب) الآمنة تحتوي على أيقونة "قفل" في مكان ما في الصفحة. والهدف من ذلك هو ضمان أن تكون المعاملات والبيانات التي يتم توفيرها آمنة وسالمة. تعرض الصورة التالية أيقونة القفل (Lock).

يمكن أن تتواجد أيقونة "القفل" في الركن العلوي الأيمن أو الركن السفلي الأيمن من نافذة المستعرض. ويمكن أن تنقر (أو أن تنقر نقرًا مزدوجًا) على أيقونة "القفل" لعرض تفاصيل أمان الموقع.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

التعرف على حالات الاستخدام غير الأخلاقية وغير الملائمة للتقنيات

هل قمت بالكشف عن المعلومات الشخصية الخاصة بك على شبكة (الإنترنت) من قبل، وإذا كنت قد قمت بفعل ذلك، فإلى أي مدى؟ هل تعلم أن أي شخص في أي مكان في العالم يمكن أن يتتبعك فقط وبكل سهولة من خلال فحص عنوان البريد الإلكتروني الخاص بك؟ بسبب انتشار مواقع (الويب) الاحتيالية، وسرقات عناوين البريد الإلكتروني والهُويات، يجب أن تكون أكثر دراية بأن خصوصيتك معرضة للخطر. يمكن أن تصبح المعلومات الشخصية الخاصة بك هشة للغاية بمجرد نشرها على شبكة (الإنترنت)، حيث إنها يمكن أن تجذب لصوص (الإنترنت) للتلاعب بهذه المعلومات.

نصائح: كيف يمكنك تجنب التعرض لأن تكون ضحية لسرقة الهُوية

- لا ترد مطلقًا على أية رسالة أو رسائل بريد إلكتروني تثير الشك.
- احذر من أي شخص يتظاهر بأنه شخص آخر، وخذ حذرك منه. يمكن أن تظاهر المستغلين بأنهم أشخاص آخرون ولهم أعمار وخلفيات مختلفة، ويحاولون إقناعك بإضافتهم كأصدقاء.
- لا تقم بإعطاء معلوماتك الشخصية لأي شخص على (الإنترنت). يمكن أن تكون المعلومات مثل: أرقام الهواتف المحمولة، أو عناوين البريد الإلكتروني، وعناوين السكن نقطة بداية لهؤلاء المستغلين لمطاردتك.
- قم بالاستفادة من ميزات إعداد الخصوصية على مواقع الشبكات الاجتماعية.
- فمن شأن ذلك المساعدة في تأمين المعلومات الخاصة بك. فقد ترغب في أن تطلع مجموعة محددة فقط من الأصدقاء على البيانات الشخصية الخاصة بك، وليس الجميع.
- تذكر أن ما تنشره على (الإنترنت) ليس شيئًا يتسم بالخصوصية. فيمكن أن يبحث والديك وأصدقائك وأصحاب العمل المحتملين عنك على (الإنترنت) ويمكنهم التوصل إلى معلومات عنك بتلك الطريقة.
- لا تقم أبدًا بملء أية ملفات تعريف على (الإنترنت). يجب أن تحد من معلومات ملفات التعريف التي تنشرها على (الإنترنت).
- هل قمت بإجراء بحث على (الويب) عن نفسك؟ جرب ذلك!! سوف تشعر بالمفاجأة اذا قام شخص ما بنشر معلوماتك الشخصية على شبكة (الإنترنت).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

التعرف على التَّنَمُّر الإلكتروني

يحدث التنمر الإلكتروني عندما يقوم شخص ما، وبشكل متكرر، بالتحرش بالآخرين أو إساءة التعامل معهم أو السخرية منهم عبر رسائل البريد الإلكتروني أو مواقع (الويب) أو الرسائل النصية أو الهواتف الخلوية أو مقاطع (الفيديو) أو المدونات أو أي شكل آخر من أشكال التواصل الإلكتروني.

يشتمل التنمر الإلكتروني أيضًا على صور، رسائل أو صفحات لا يمكن إلغاؤها حتى لو تم طلب ذلك من الشخص المعني. بمعنى آخر، هو أي شئ يتم نشره الكترونيًا بهدف أيذاء، مضايقة أو إزعاج الآخرين.

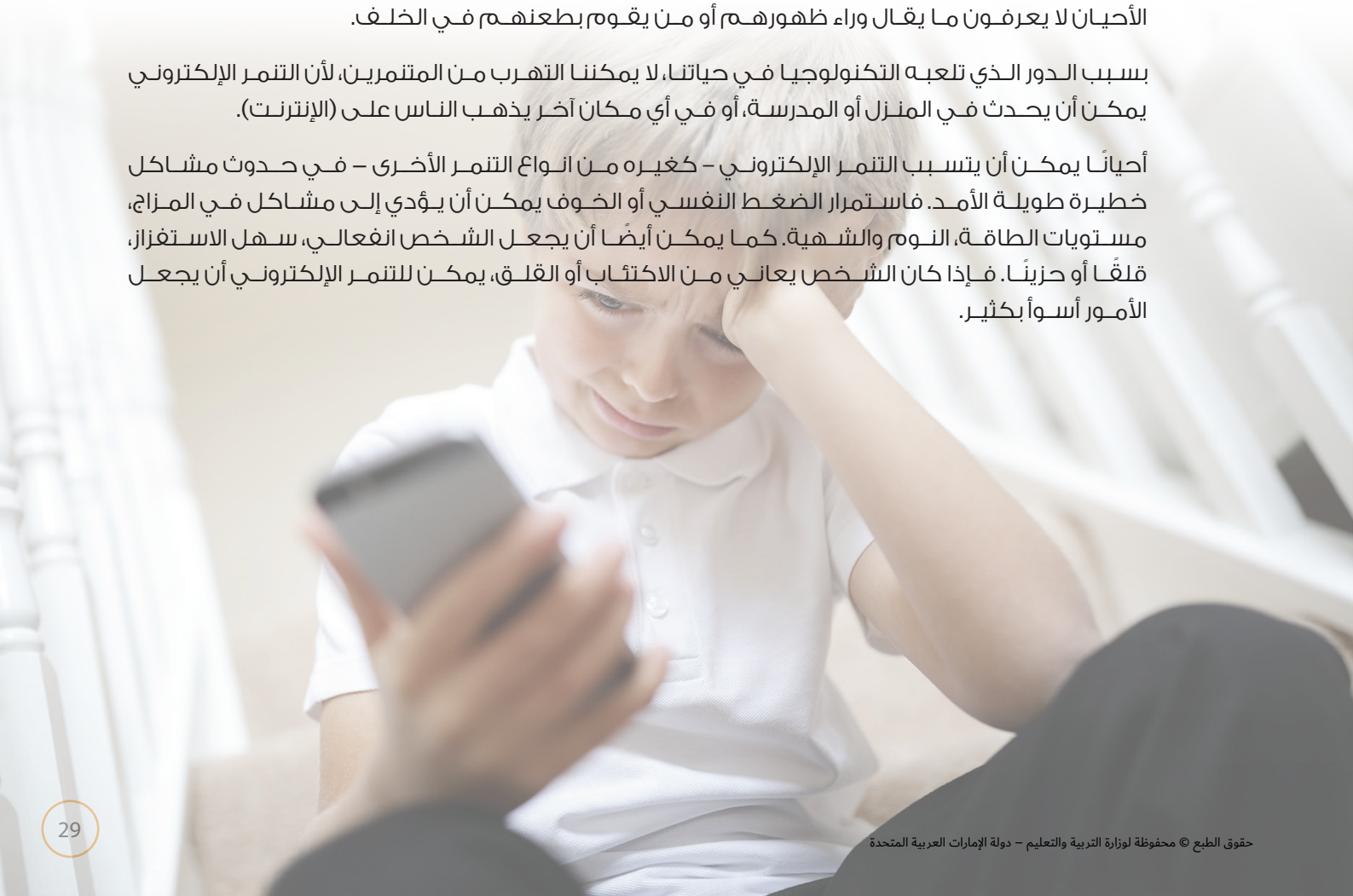
يمكن أن يشتمل التنمر الإلكترونيّ على الأنشطة التالية:

- نشر رسائل افتراء على مواقع الشبكات الاجتماعية.
- نشر الشائعات على (الإنترنت).
- استبعاد الشخص من مجموعة ما على (الإنترنت).
- إرسال رسائل غير مرغوب فيها عبر الرسائل النصية أو الفورية أو عبر البريد الإلكترونيّ.

لأن هذا النوع من التهديد يمكن أن يحدث في أي مكان، ويمكن أن يفقد الضحايا الشعور بالأمان في منازلهم. وهذا بدورة يتسبب في مصيبة كبيرة وتأثير سلبي على تقدير الذات وثقة الضحية من الممكن أن يكون تأثير التنمر الإلكترونيّ على الضحية مزعجًا ويلحق ضررًا بالغًا بالضحية لأنه عادة ما كون مجهول المصدر أو من الصعب تتبعه. كما أنها من الصعب السيطرة عليه، وليس هناك فكرة لدى الضحية عن عدد الأشخاص الذين شاهدوا الرسائل أو المشاركات. يمكن أن تتعذب الضحية باستمرار في كل مرة يتفقد فيها هاتفه المحمول أو جهاز (الكمبيوتر) الخاص به. في بعض الأحيان لا يعرفون ما يقال وراء ظهورهم أو من يقوم بطعنهم في الخلف.

بسبب الدور الذي تلعبه التكنولوجيا في حياتنا، لا يمكننا التهرب من المتنمرين، لأن التنمر الإلكتروني يمكن أن يحدث في المنزل أو المدرسة، أو في أي مكان آخر يذهب الناس على (الإنترنت).

أحيانًا يمكن أن يتسبب التنمر الإلكتروني – كغيره من انواع التنمر الأخرى – في حدوث مشاكل خطيرة طويلة الأمد. فاستمرار الضغط النفسي أو الخوف يمكن أن يؤدي إلى مشاكل في المزاج، مستويات الطاقة، النوم والشهية. كما يمكن أيضًا أن يجعل الشخص انفعالي، سهل الاستفزاز، قلقًا أو حزينًا. فإذا كان الشخص يعاني من الاكتئاب أو القلق، يمكن للتنمر الإلكتروني أن يجعل الأمور أسوأ بكثير.



حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

آثار التنمر الإلكتروني

لم يعد التنمر الإلكتروني يقتصر على ساحات المدارس أو زوايا الشوارع، بل يمكن أن يحدث في المنزل والمدرسة طوال اليوم. يمكن أن يشعر الأطفال الذين يقعون ضحايا التنمر بانزعاج مستمر وأنه ليس هناك مفر. طالما أن لديهم إمكانية الوصول إلى هاتف أو كمبيوتر أو جهاز آخر (بما في ذلك الحواسيب اللوحية)، فهم معرضون للخطر.

يمكن للتنمر الشديد، على المدى الطويل أو المتكرر أن يجعل كل من الضحايا والمتنمرين أكثر عرضة للقلق والاكتئاب، والاضطرابات المرتبطة بالتوتر أخرى. في بعض الحالات النادرة التي حظيت بتغطية إعلامية كبيرة، تحول بعض الأطفال إلى الانتحار. يقول خبراء ان الاطفال الضحايا والمتنمرين أنفسهم عرضة للأفكار الانتحارية، محاولات الانتحار، وربما الانتحار فعليًا.

عقوبة التنمر الإلكتروني يمكن أن تشمل الفصل المؤقت من المدرسة أو الطرد من الفرق الرياضية. أنواع معينة من التنمر الإلكتروني يمكن أن تصل لمستوى جريمة.

كيف أتعامل مع المتنمر الإلكتروني؟

في بعض الأحيان، لا يعرف الضحايا أو لا يكونوا متأكدين مما إذا أنهم يتعرضون للتنمر أو لا، فلا يفعلون شيء حيال ذلك، ولكن يشعرون أسوأ وأسوأ في داخلهم. إذا كنت تعرف عن تعرض أحدهم للمعاملة القاسية أو المضايقة أو تعرف شخص يتعرض لذلك، فلا يوجد سبب للمعاناة في صمت. في الواقع يجب الإبلاغ عن أي رسائل فورية، نصية أو رسائل بريد إلكتروني مزعجة.

أخبر شخص ما. أول شيء يجب أن تفعله هو أن تخبر شخصًا راشدًا تثق به. غالبًا ما يكون القول أسهل من الفعل. غالبًا ما يشعر الضحايا بالحرج أو التردد في الإبلاغ عن حالة التنمر. البعض يتردد لأنهم غير متأكدين (100%) من الذي يقوم بالتنمر عليهم. ولكن التنمر يمكن أن يتفاقم، لذلك استمر في الكلام حتى تجد شخص ما يساعدك. في بعض الأحيان تستطيع الشرطة تعقب المتنمر المجهول الهوية، لذلك فقد يكون من المفيد أن نخبر عنهم.

اترك الموضوع وابتعد. ما سمعته عن الابتعاد عن المتنمر في الحياة الواقعية يعمل في العالم الافتراضي أيضًا. تجاهل المتنمرين هو أفضل وسيلة لانتزاع سلطتهم، ولكن ليس من السهل دائمًا القيام بذلك في العالم الحقيقي أو الإلكتروني.

إذا رأيت شيئًا مزعجًا، حاول الابتعاد عن جهاز (الكمبيوتر) أو إيقاف الهاتف لفترة من الوقت. لا تستجيب، ولا تمرر الرسالة إلى شخص آخر. جد شيئًا لصرف انتباهك عن ما يجري. إفعل شيئًا تحبه ولا يعطيك الوقت للتفكير في ما يحدث.

مقاومة الرغبة في الانتقام أو الرد. إن الابتعاد عن الجهاز أو أخذ استراحة عند تعرضك لتنمر الإلكتروني يوفر لك بعض الوقت لمقاومة إغراء قيامك برد عنيف أو الاشتباك بغضب مع المتنمر. ردود الفعل ساعة الغضب يمكن أن تجعل الأمور أسوأ. (الوقوف في وجه المتنمر يمكن أن يكون فعالاً في بعض الأحيان، إلا أنه في أغلب الأوقات يصعد الموقف ويجعله يبدو أسوأ)، لذا أخذ استراحة يجعل زمام الأمور في يديك!

على الرغم من أنها الرد على المتنمر ليست فكرة جيدة، إلا أن الاحتفاظ بأدلة على عملية التنمر تعتبر فكرة جيدة، فذلك يساعدك على إثبات قضيتك إذا لزم الأمر. لا يشترط بك الاحتفاظ برسائل البريد الإلكتروني، الرسائل النصية المسيئة أو غيرها من الاتصالات في المكان الذي تصلك إليه طوال الوقت، بل يمكنك أن تسأل أحد الوالدين لعمل نسخة، أو حفظها إلى محرك أقراص أو فلاش ميموري.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

رفع تقرير التنمر إلى مزود الخدمة الخاص بك. مواقع مثل: الـ (فيسبوك)، إنستغرام، و(يوتيوب) تأخذ الأمر على محمل الجد عندما يستخدم الناس مواقعهم لنشر مواد مسيئة أو إنشاء حسابات وهمية. إذا تقدم المستخدمون بتقرير سوء استخدام، فقد يقوم المسؤول عن الموقع بمنع المتنمر من استخدام الموقع في المستقبل. إذا كنت تتعرض لمضايقات من قبل شخص يرسل لك رسائل نصية أو بريد إلكتروني، يمكنك الإبلاغ عن ذلك لخدمة الهاتف أو مزودي خدمات البريد الإلكتروني (مثل: (كومكاست)، (جوجل)، (فيريزون)، و(ياهو).

حجب المتنمر ووضعه على قائمة المنع (block). معظم الأجهزة لديها إعدادات تسمح لك إلكترونيا بمنع المتنمر من إرسال الملاحظات/الرسائل. إذا كنت لا تعرف كيفية القيام بذلك، اطلب من صديق أو أحد البالغين القيام بذلك.

استخدم (الإنترنت) بشكل آمن. قم بحماية هاتفك المحمول ومواقع (الإنترنت) الخاصة بك باستخدام كلمة المرور، وقم بتغيرها بشكل دوري. تأكد من مشاركة كلمات المرور الخاصة بك فقط مع والديك أو ولي الأمر. كما أنه من الحكمة أن تفكر مرتين قبل تبادل المعلومات الشخصية أو الصور/(الفيديو) التي لا تريد للآخرين رؤيتها. فبمجرد نشرك صورة أو رسالة، فإنه يصبح من الصعب أو المستحيل حذفها. لذلك كن حذرًا عند نشر الصور أو الاستجابة لرسالة مزعجة من شخص ما.

بالنسبة للأطفال الأصغر سنًا، فإن أفضل طريقة لحل مشكلة التنمر هي إخبار شخص بالغ وثقة. أما بالنسبة للشباب – بالرغم من أن إخبار شخص بالغ يعتمد على ظروف التنمر.

1. لا تحاول الانتقام أو الرد.
2. قم بحجب المتنمر وتغيير إعدادات الخصوصية الخاصة بك.
3. قم بالتبليغ عن حالة التنمر – انقر فوق زر الإبلاغ عن سوء استخدام.
4. قم بجمع الأدلة – الاحتفاظ برسائل الهاتف المحمول ورسائل البريد الإلكتروني أو طباعة محادثات على مواقع التواصل الاجتماعي.
5. تحدث إلى شخص تثق به، مثل: أحد أفراد العائلة أو صديق.

يمكن للتحدث مع المعلمين أو أولياء الأمور أن يحدث فرقًا. قد يكون لمدرستك سياسات معينة للتعامل مع المتنمرين.

استنادًا للمادة رقم (16) من قانون الإمارات العربية المتحدة لجرائم تقنية المعلومات

"يعاقب بالحبس لمدة لا تزيد عن سنتين وغرامة تتراوح ما بين (250,000 – 500,000) درهم إماراتي أو كلا العقوبتين كل من تتم إدانته باستخدام (الإنترنت) أو أي وسيلة أخرى عالية التقنية لتهديد، ابتزاز أي شخص أو تحريضه على القيام بفعل أو عدم القيام به. وقد تصل العقوبة إلى (10) سنوات إذا كان التهديد أو التحريض يشكل ضررًا بالشرف أو الحالة الذهنية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة: التهديد الإلكترونيّ هو المجال الجديد للجريمة

دبي – وفقًا لأحد أعضاء المجلس الوطنيّ الاتحاديّ ورئيس هيئة المعرفة و التنمية البشرية، بَجي تحديث التشريعات المتعلقة بالتهديد في المدارس على المدى الطويل حتى تقوم بتغطية الأنواع الجديدة من التهديد والتي تم إغفالها في السابق مثل: التهديد الإلكترونيّ.

من المهم تفعيل قواعد السلوك ضد التهديد في المدارس حتى يشعر الطلاب بالأمان والحماية، كما تزعم فاطمة المري. كما نوهت كذلك إلى أنه يجب على العمال التدريب على التعامل مع مثل هذه الحالات كخطوة مهمة أخرى لإزالة التهديد الإلكترونيّ.

يظهر الدليل السردي أن التنمر الإلكترونيّ يتزايد بالرغم من أنه ليس هناك أي أبحاث رسميَّة حول هذا الموضوع حتى الآنَ.

فطبقًا لما ذكرته سامينة شاهين أستاذ علم النفس، أنه من الممكن أن يكون التنمر الإلكترونيّ أكثر تدميرًا وخطورة من الأشكال الأخرى للتهديد. اعتاد الأطفال على الهرب إلى منازلهم لحماية أنفسهم من التهديد في المدرسة. وبالرغم من ذلك، فلا مفر من التنمر الإلكترونيّ. يندفع البلطجية من خلال الرسائل النصيَّة وغرف الدردشة أو مواقع الشبكات الاجتماعيَّة إذا ما شعروا أنهم لا يستطيعون القيام بذلك في المدرسة. وقد تسبب ذلك في تزايد حالات الانتحار، والذي يعني انتحار القائمين بالبلطجة.

جاءت إحدى هذه الحالات إلى الدكتور ديفيكا سينغ، وهو طبيب نفسانيّ في مركز دبي للأعشاب والمعالجة، وكانت فتاة صغيرة و التي لم يكشف عن مشكلتها إلا بعد أن وجدتها صديقتها ترتعد بكل ما في الكلمة من معنى. وبعد التحقيق، اكتشف أن الطفلة قد تلقت تهديدًا عبر مواقع الشبكات الاجتماعية.

التعامل مع البصمة الرقمية

البصمة الرقمية ما هو إلا استمرار تسلسلات البيانات من قبل نشاط للمستخدم في بيئة رقمية. وتأتي البصمة الرقمية من التفاعلات الخاصة بك عبر الهاتف أو (الويب) أو التفاعلات عبر (الإنترنت)، وهي تشتمل على البيانات الرقمية التي تحدد شخصيتك.

هل لديك بصمة رقمية خاص بك؟

هل استخدمت مواقع التواصل الاجتماعي من قبل للتواصل مع أصدقائك؟ وماذا عن استخدام غرف المحادثة أو استخدام رسائل البريد الإلكتروني لإرسال الرسائل؟ إذا كانت الإجابة بنعم، فهذا يعني أنك قد قمت بالفعل بإنشاء بصمة رقمية إلكتروني لك لأن كل الأنشطة التي يتم تنفيذها على جهاز رقمي تترك أثرًا إلكترونيًا.

تعرف على البصمة الرقمية الخاص بك!

هل يجب أن تتخذ الحيطة حيال البصمة الرقمية الخاص بك؟

نعم، يجب عليك ذلك. من حقك إدارة الأنشطة الإلكترونية الخاصة بك بحيث لا تؤثر سلباً على سمعتك.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الأنشطة

واجب: قم بإجراء بحث عن نفسك أو عن أحد أصدقائك، ماذا تلاحظ؟

أمثلة على سوء السلوك عبر (الإنترنت)

وفيما يلي بعض الأمثلة للأنشطة التي يمكن أن توقعك في المشكلات:

1. نشر صور لك أو لأصدقائك تنتهك القانون يمكن أن يبدو ذلك أمرًا غير مضر لك ولأصدقائك.
2. كل ما تفكر فيه هو أن تجعل أصدقائك يرون ما قمت به في الإجازة الأسبوعية السابقة، أليس كذلك؟ خطأ. احتفظ بهذه الصور لنفسك أو قم بقصها، ولكن لا تنشر صورك أو صور أصدقائك بما ينتهك القانون.
3. انشاء صفحة وهمية على (Facebook) لشخص آخر هل تعلم أنك إذا قمت بإنشاء صفحة وهمية على (Facebook) لشخص آخر، يمكن أن يتم اتهامك بالفعل بتهمة سرقة الهوية أو التحرش؟
4. نسيان من هم على (Facebook) – هل تعرف أن شركات العمل المحتملة، وبعض الكليات، وحتى بعض شركات التوظيف تبحث على (الويب) أو على مواقع الشبكات الاجتماعية قبل توظيفك أو قبولك؟ نعم، هذا صحيح. هل تعرف أيضًا أن الشركة الحالية التي تعمل بها يمكن أن تكون تقوم بنفس الأمر؟ تحقق من أنك لا تنشر أي شيء لا تحبه أن يظهر في أي مقابلة شخصية للعمل.
5. الإشارة إلى صديق ما على صورة في موقع الشبكات الاجتماعية – قد يبدو الأمر عاديًا أن تضع علامة على صورة صديق لك على (الويب). كل ما تفكر فيه هو أن تجعل صديقك يعلم أنك قد قمت بزيارة موقع الشبكات الاجتماعية الخاص به، أليس كذلك؟ خطأ. هل تدرك أن ذلك يمكن أن يؤدي إلى إساءة تفسير شخصية صديقك؟

مشاريع مقترحة:

1. قم بعمل صور متحركة/(فيديو)/رسوم أو جداول بيانية لتوضيح حقوق الملكية وانتهاكاتها.
2. قم بعمل صور متحركة/(فيديو)/رسوم أو جداول بيانية لتوضيح تأثير سرقة معلومات بطاقة الائتمان/الهوية الشخصية.
3. قم بعمل صور متحركة/(فيديو)/رسوم أو جداول بيانية لتوضيح مصداقية المواقع الإلكترونية.
4. قم بعمل صور متحركة/(فيديو)/رسوم أو جداول بيانية لتوضيح الاستخدام السيئ/اللااخلاقي لوسائل التقنية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تمرين

1. **اختر أفضل طريقة للكشف عن معلوماتك الشخصية على موقع شبكات اجتماعية بدون تعريض هويتك للخطر؟**
   - أ. انتحال شخصيَّة الآخرين.
   - ب. الكشف عن المعلومات عند الطلب.
   - ج. استخدام معلومات غير صحيحة.
   - د. الكشف عن الحد الأدنى من المعلومات.

2. **كيف يمكن أن يؤثر وضع علامات على الصور المتاحة على (الإنترنت) بشكل سلبي على فرص التوظيف المستقبلية الخاصة بك؟**
   - أ. يمكن أن يعزز ذلك من وضعية صورتك ومن شخصيتك.
   - ب. يجعلك ذلك مميزًا عن الباحثين الآخرين عن الوظائف.
   - ج. يكشف ذلك صلاتك الشخصية وتفضيلاتك الاجتماعية.
   - د. يسمح ذلك بالحكم المسبق على شخصيتك بالإضافة إلى التفسير الخطأ لشخصيتك.

3. **ما هي أفضل طريقة للتحقق من مصداقية مورد متاح على (الإنترنت)؟**
   - أ. البحث عن مواقع (الويب) السياسية التي تذكر مصادرها.
   - ب. البحث عن مواقع (الويب) التجارية التي تستخدم النطاق (.com).
   - ج. البحث عن مواقع (الويب) من خلال فهرس المكتبات على شبكة (الإنترنت).
   - د. البحث عن مواقع (ويب) المنظمات التي تستخدم النطاق (.net).

4. **بماذا يمكن أن نسمي الأشخاص الذين يقتحمون أجهزة (الكمبيوتر) بدون نوايا سيئة؟**
   - أ. المتسللون.
   - ب. (الهاكرز).
   - ج. (الكراكرز).
   - د. مقتحمو الخطوط الهاتفية.

5. **قول اتحاد البرامج التجارية أن "الأفراد يزورون مواقع شبكات النظير إلى النظير (P2P) ومواقع المزادات بأعداد ضخمة للحصول على البرامج غير القانونية أو لنقلها". بناءً على هذه العبارة، ما هي التأثيرات السلبية التي يتسبب هؤلاء الأفراد فيها؟**
   - أ. المساعدة على نشر البرامج الضارة وبرامج التجسس.
   - ب. المساعدة على تطوير صناعة البرامج.
   - ج. المساعدة في تجاوز "الفجوة الرقمية".
   - د. المساعدة في توسيع تبني التقنيات عبر برامج رخيصة الثمن.

الإجابة: 1.ب، 2.د، 3.ج، 4.ب، 5.أ

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

03 القواعد الإلكترونيَّة

حول هذه الوحدة

تقدم هذه الوحدة وتشرح التفاصيل المتعلقة بالجرائم الإلكترونية وقضايا حقوق الطبع والنشر والتأثيرات الناجمة عنها على الأشخاص والشركات. كما سنلقي نظرة على تشريع حماية البيانات، وفحواه، وأهميته في حماية الحقوق الخاصة بك.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أهداف التعلُّم

أهداف هذه الوحدة هي:

- التعرف على الأنواع المحددة للجرائم الرقمية.
- وصف آثار الجرائم الإلكترونية على قطاع معين.
- الترويج لأهمية وجود حقوق ومحاذير قانونية تحكم استخدام التكنولوجيا.

نتائج التعلُّم

في نهاية هذه الوحدة، سوف تكون قادرًا على:

- ذكر أمثلة من الجرائم الإلكترونية.
- ذكر آثار الجرائم الإلكترونية على الأفراد.
- تحديد الحقوق القانونية والقواعد واللوائح لتجنب الوقوع ضحية لجرائم (الإنترنت).
- ذكر أفضل السبل لتقييم مصداقية موقع ما على شبكة (الإنترنت).

قائمة المراجعة

البنود	التحصيل العلمي	قبل	بعد
1	يمكنني تحديد الأشكال المختلفة للجرائم الرقمية		
2	أنا على دراية كاملة بتأثير الجرائم الرقمية على الأشخاص وعلى الاقتصاد.		
3	أنا أدرك المقصود بانتهاك الملكية الفكرية.		
4	أنا أدرك أهمية الحقوق والقيود القانونية السارية والتي تساعد على التحكم في استخدام التقنيات.		

التعليمات:

بعد الانتهاء من قراءة هذه الوحدة، يُرجى إكمال الاستبيان باستخدام المقياس التالي:

المقياس:

1. ليس لدي أدنى معرفة.
2. لدي معرفة محدودة.
3. على دراية وقادر على التوضيح الجيّد.
4. ذو كفاءة وإمكانية على الممارسة الكاملة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

القواعد الإلكترونية - التحكم في استخدام الاتصالات والتقنيات الإلكترونيَّة

هل قمت من قبل بشراء برنامج أصلي؟ بشكل طبيعي، تكون التكلفة مرتفعة للغاية. والسبب في ذلك أنه لتطوير برنامج، يلزم توفير قدر كبير من الموارد، مثل: الأشخاص، والوقت، والمال. ومع ذلك، ولكي تستمتع بالامتيازات التي يوفرها البرنامج، فقد قررت أن ذلك يستحق التكلفة التي يتم دفعها.

على النقيض، هل يجعلك شراء القرص المضغوط أو قرص (DVD) والمحتوي على البرنامج المالك القانوني لهذا البرنامج؟ وبكل تأكيد، فإن القرص المضغوط أو قرص (DVD) مملوك لك الآن، ولك حرية تثبيت البرنامج على جهاز (الكمبيوتر) الخاص بك. ومع ذلك، هل يعني ذلك أنك يمكنك أن تفعل ما تشاء به؟

دعونا نلقي نظرة أقرب على هذا (السيناريو).

يأتي صديقك لزيارتك في المنزل ويراك تستخدم البرنامج الذي قمت بشرائه. ولسوء الحظ، لا يمكنه تحمل نفقة شراء البرنامج لأن ثمنه مرتفع للغاية بالنسبة له. وتقرر أن تقوم بعمل خيري معه، من خلال إعطائه نسخة من البرنامج. وأثناء استخدام صديقك لنسخة البرنامج في المنزل، يعجب أحد أفراد الأسرة بالبرنامج، ويقرر صديقك عمل نسخة أخرى له.

هل تعلم أن هذا الأمر غير قانوني؟ هل تعلم أن السماح بتثبيت البرنامج الخاص بك على جهاز كمبيوتر آخر هو بمثابة خرق للقانون؟

وهنا يأتي دور القواعد الإلكترونية.

إدراك القواعد الإلكترونية

مصطلح القواعد الإلكترونية هو المصطلح المستخدم للإشارة إلى القضايا القانونية المتعلقة بجوانب الاتصالات والعمليات والتوزيع لتقنيات وأجهزة المعلومات المتصلة عبر الشبكات.

تساعدك هذه الوحدة على الحصول على المزيد من الدراية حول ماهية القواعد لإلكترونية وأهميتها ودورها في عالم التقنيات. كما ستتعرف أيضًا على القليل من أنواع الجرائم الإلكترونية، بالإضافة إلى القضايا المتعلقة بحقوق الطبع والنشر، والتأثيرات الهامة لهذين الموضوعين على الأشخاص والشركات. كما سنلقي أيضًا نظرة على تشريع حماية البيانات، وهو مصطلح هام يجب أن تضعه نصب عينيك بمجرد أن تقدم على الدخول إلى عالم التقنيات الرقمية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الجرائم الإلكترونيّة

إدراك الجرائم الإلكترونية

إذا كنت تعتقد أن الجرائم التي ارتكبت في العالم الحقيقي كافية، فيجب عليك إعادة النظر في هذا الأمر مرة أخرى

بعض الجرائم تحدث بالفعل في العالم الافتراضي وتكون أشد حدة من الجرائم التي يتم ارتكابها في "العالم الواقعي". ويطلق على أنواع الجرائم هذه، والتي يتم ارتكابها من خلال استخدام التقنيات، اسم "الجرائم الإلكترونية".

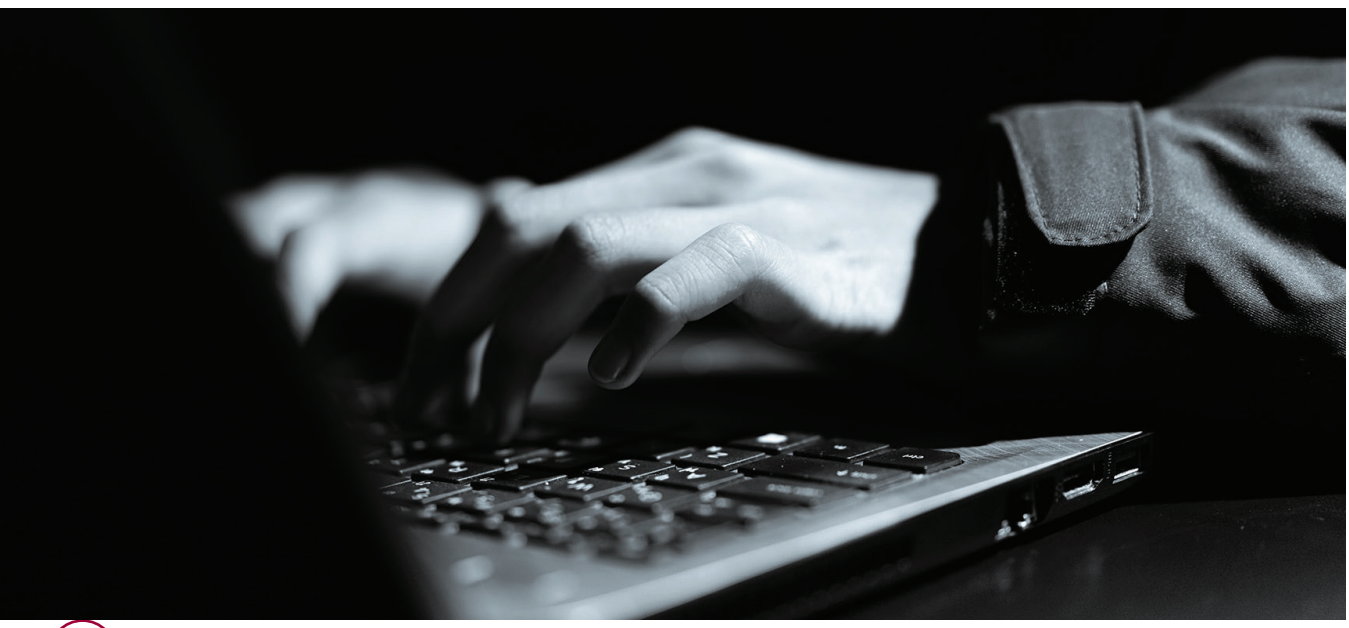
ويطلق على الجرائم الإلكترونية أيضًا أسماء جرائم (الكمبيوتر) أو الجرائم الرقمية أو (e-crime)، أو الجرائم الإلكترونية. وكل هذه المصطلحات تتشارك في شي ما، فجميعها تشير إلى أن الجرائم يتم ارتكابها من خلال استخدام التقنيات. وهي جرائم تستخدم فيها أجهزة (الكمبيوتر) لإخافة الناس أو ارتكاب جرائم الاحتيال أو سرقة المعلومات الهامة.

ولقد تحول الكثير من الجرائم "الواقعية" مثل: الابتزاز والتزييف والسرقة وغسيل الأموال والاختلاس إلى جرائم إلكترونية، لأن المجرمين الآن يستخدمون شبكة (الإنترنت) للقيام بأعمالهم الإجرامية. إن شبكة (الإنترنت) تتيح، بكل سهولة، القدرة على الوصول إلى المعلومات حول الأشخاص والشركات والأسواق على الصعيد العالمي، وبالتالي فإنها تسهل ارتكاب المزيد من الأنشطة غير الأخلاقية.

ومن خلال تطور تقنية أجهزة (الكمبيوتر)، يستخدم الكثير من الأشخاص أجهزة (الكمبيوتر) لأغراض شخصية واحترافية، وبالتالي فإنهم يصبحون أكثر عرضة للجرائم الإلكترونية، سواء كضحايا، أو من خلال ارتكاب الجرائم الإلكترونية بأنفسهم. إنها ظاهرة خطيرة تهدد أمان الأفراد، والمؤسسات، وحتى الدول في مجملها.

أمثلة على الجرائم الإلكترونيّة

يلقي هذا الموضوع الفرعي نظرة على أنواع الجرائم الإلكترونية، ويوفر توضيحات بالإضافة إلى دراسات حالة لجرائم إلكترونية واقعية. ومن خلال ذلك، ستتمكن من تحديد الأنشطة التي يمكن اعتبارها على أنها جرائم إلكترونية، بالإضافة إلى إدراك العلامات التي توضح هل أنت ضحية أم مجرم. وإليكم بعض أمثلة للجرائم الإلكترونية التي حدثت خلال السنوات الماضية.



حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الاحتيال على الأعمال المصرفية عبر (الإنترنت)

يعرّف الاحتيال على الأعمال المصرفية عبر (الإنترنت) على أنه أية عملية احتيال أو سرقة يتم ارتكابها باستخدام التقنيات المتاحة على شبكة (الإنترنت) لإزالة الأموال من حساب بنكي أو نقلها إلى حساب بنكي آخر بشكل غير قانوني. وتشتمل أنواع الاحتيال على الأعمال المصرفية على (الإنترنت) على التصيد وتعيين وسيط لنقل الأموال.

يقع التوظيف الوهمي عندما يقوم المزورون بتشغيل أشخاص لتحويل الأموال المكتسبة بطريقة غير مشروعة بالنيابة عنهم. يشغل هؤلاء الضحايا باستخدام عدة وسائل، مثل: إعلانات الوظائف الشاغرة في الصحف أو على (الإنترنت)، والإعلانات على مواقع التوظيف الشرعية، ورسائل البريد الإلكتروني العشوائية (لهؤلاء الذين يضعون سيرهم الذاتية على شبكة (الإنترنت). كما تعد غرف الدردشة، ومواقع التواصل الاجتماعي، والرسائل الفورية من الوسائل المستخدمة في هذا الغرض. وعادة ما يستهدف طلاب الجامعات والعمال المهاجرين، حيث يسهل خداعهم بتحقيق حلم الثراء السريع.

إذا تلقيت أية أموال في حسابك البنكي أو إذا قمت بنقل أو تحويل الأموال إلى دولة أخرى بموجب هذه الظروف، فيرجى الاتصال بالمؤسسة المالية التي تتعامل معها على الفور.

قانون الجرائم الإلكترونيَّة في دولة الإمارات العربيَّة المتحدة

وفقًا للمادة رقم (12)، إستخدام الشبكة المعلوماتية أو نظام المعلومات الالكتروني للحصول على بيانات بطاقة إئتمانية.

يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق، عن طرق استخدم الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية، أو أي وسيلة من وسائل الدفع الإلكتروني.

وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين، إذا قصد من ذلك استخدام البيانات والأرقام في الحصول على أموال الغير، أو الاستفادة مما تتيحه من خدمات.

فإذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير فيعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائتي ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين.

ويعاقب بذات العقوبة المنصوص عليها في الفقرة السابقة كل من نشر أو إعادة نشر أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية تعود للغير أو أي وسيلة أخرى من وسائل الدفع الإلكتروني.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة (1): عملية "الاحتيال" تصفي حسابات عملاء بنك المشرق

أصيب برافين باكليوال بالذهول لما علم أن النصابين قد سرقوا المبلغ المودع في حسابه المصرفي ومقداره (121,000) درهم مع (7,500) درهم مستحقة على بطاقته الائتمانية. وكانت أمواله قد سُحبت على دفعات (500) درهم و(1,000) درهم وهو ما يُشبه حالات أخرى.

وهو يعتقد أنهم قد سرقوا رصيده على مدار أسبوعين بداية من 1 ديسمبر، لتسوية تكاليف (135) مكالمة هاتفية، وتركوا في حسابه (140) درهم. كما ذكر أن صاحب العمل في دبي قد أقاله بسبب أخذ إجازة مطولة لبحث موضوع تلك المعاملات الاحتياليَّة.

وهناك ضحايا آخرون تعرضوا للاحتيال وفقدوا ما يقرب من (128,500) درهم (35,000) دولار أمريكيّ من حساباتهم المصرفيَّة ويلزمهم سدادها بعدما تمكن القراصنة من الوصول إلى مدخراتهم بخدعة إعادة شحن خطوط هواتف نقَّالة.

Hack In The Box, 4 April, 2010, https://news.hitb.org/content/'phishing'-raid-empties-mashreqbank-customer-accounts

التحرش

تم تنفيذ هذا النوع من الجرائم لإهانة شخص آخر لإرضاء الذات دون الحصول على مقابل مادي. وبناءً على تعريف القاموس القانوني، يتم تعريف التحرش على أنه إجراء منظم أو مستمر يشتمل على إجراءات غير مرغوبة أو تسبب ضيقًا لمجموعة أو لطرف، بما في ذلك التهديدات والمطالبات. ويدفع هذا الإجراء دوافع متنوعة، مثل: التحيز الشخصي، أو الكراهية الشخصية، أو محاولة دفع شخص لترك وظيفة، أو منح امتيازات جنسية أو لمجرد المتعة ليس إلا.

قانون الجرائم الإلكترونيَّة في دولة الإمارات العربيَّة المتحدة

وفقًا للمادة رقم (16)، إبتزاز أو تهديد شخص للقيام بفعل أو الإمتناع عنه باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات.

يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات.

وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الابتزاز

الابتزاز هو فعل يعد جريمة في نظر القانون والذي يتضمن تهديدات غير مبررة من أجل تحقيق مكاسب أو إلحاق ضرر بضحية ما في حال عدم القيام بتنفيذ مطالب الجاني. حيث أنه عبارة عن إكراه للضحية من خلال التهديد بالحاق ضرر جسدي أو بالملاحقة الجنائية أو التهديد من أجل الاستيلاء على أموال الضحية أو ممتلكاته.

قانون الجرائم الإلكترونيَّة في الإمارات العربيَّة المتحدة

وفقًا للمادة رقم (16)، إبتزاز أو تهديد شخص للقيام بفعل أو الإمتناع عنه باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات.

يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من ابتز أو هدد شخص آخر لحمله على القيام بفعل أو الامتناع عنه وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات.

وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار.

التعدي على الملكية الفكرية

يُعد التعدي على الملكية الفكرية واحدًا من أكثر الأنشطة الإجرامية المتعلقة بالأعمال التجارية تفشيًا، وهو يشتمل بشكل طبيعي على الاستخدام غير القانوني أو إعادة الإنتاج غير القانونية للمعلومات أو التقنيات المملوكة لمالك قانوني. وقد أتاحت التطورات الحادثة في قطاع تقنيات المعلومات نسخ المعلومات أو التقنيات الهامة وتخزينها في نماذجها الرقمية.

دراسة حالة (2): أقر مواطن صيني بالذنب في سرقة أسرار شركة فورد.

فقد اتهم أحد الموظفين الصينيين السابقين في شركة فورد في قضيتي سرقة أسرار تجارية. وكان الرجل يعمل كمهندس إنتاج في شركة فورد لمدة (10) سنوات وكان متاح له الوصول إلى الأسرار التجارية لشركة فورد وكذلك وثائق تصميم فورد. بعد أن قبل عرض الوظيفة في الصين، قام الموظف بنسخ (4,000) وثيقة من وثائق فورد، فضلاً عن وثائق حساسة خاصة بتصميمات فورد على قرص صلب خارجي قبل أن يخبر شركة فورد عن تركه العمل في الشركة. وقد تكلفت الأبحاث المدونة في هذه الوثائق ملايين الدولارات وأجريت في عشرات السنين. وبعد عامين تقريبًا، بدأ العمل مع شركة منافسة لشركة فورد. وحينما عاد إلى الولايات المتحدة، ألقي القبض عليه وخضع جهاز (الكمبيوتر) المحمول الخاص بالشركة التي يعمل بها للفحص. واكتشف أن جهاز (الكمبيوتر) المحمول يحتوى على (41) وثيقة لمواصفات تصميم أنظمة فورد، ودخل عليها جميعًا خلال وقت عمله في الشركة المنافسة لفورد.

The United States,Department of Justice,17 November, 2010, http://www.justice.gov/criminal/ cyber-crime/yuPlea.pdf

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

قرصنة البرمجيات

قرصنة البرمجيَّات أمر يقع عمومًا بين مستخدمي ((الكمبيوتر)) و(الإنترنت). فالناس غالبًا ما يتبادلون البرمجيات التي يشترونها ظنًا منهم أنه ليس في ذلك ما يضرهم. من الممكن أن يحدث هذا في بيئة العمل، حيث يقوم الموظفون في كثير من الأحيان بتثبيت نفس البرنامج على العديد من أجهزة ((الكمبيوتر)) باستخدام البرمجيات ذات الرخصة الواحدة. وهذا غالبًا ما يقع من جانب التاجر نفسه، الذي قد يحاول تقليل تكلفة شراء البرمجيات.

ومثل هذه الإجراءات تتعارض مع القانون، ويمكن تغريم الأشخاص الذين يتم القبض عليهم أثناء القيام بذلك أو حتى قد يحكم عليهم بالسجن. وتكمن المشكلة في أن العديد من الأشخاص يظنون أن قرصنة البرمجيَّات ليست بالصفقة الكبيرة كما أنها لا تضر بأحد. وبالنسبة لهم فإن شركات البرمجيات قد حققت الكثير من الأموال وأن هذا القدر الضئيل من قرصنة البرمجيَّات لن يضر بهم على المدى الطويل.

التطفُّل

يتم تعريف التطفل على أنه دخول غير مشروع وهجوميّ أو غير مصرح به إلى مرفق أو نظام.

دراسة حالة(3): قراصنة يقتحمون الشبكة الخاصة ببطاقات الإئتمان في الدولة.

دبي: عصابة مكونة من أربع أشخاص من إحدى الجنسيات الأوروبية استولت على ما يقارب خمسة ملايين درهم إماراتي (1.3) مليون دولار من أجهزة الصراف الآلي في دولة الإمارات العربية المتحدة. حيث قاموا بوضع لاصقات في قارئ البطاقات في أجهزة الصراف الآلي وتثبيت كاميرات لتسجيل الرموز السرية للبطاقات.

وبحسب تصريحات شرطة دبي فقد بدأت أقسام التحقيقات في البنوك المستهدفة مع إدارة التحريات العمل على هذه القضية وتم وضع خطة بالتعاون فيما بينهما لمراقبة الأماكن التي يحتمل أن تتعرض لنفس الهجوم والتي تتواجد فيها أجهزة الصراف الآلي.

بعد ذلك واصل الفريق العمل على هذه القضية وأسفر ذلك عن اعتقال المتهم الثالث وهو من نفس جنسية المتهمين الأول والثاني من إحدى دول أوروبا الشرقية والذي قام باستخدام بطاقات مزيفة لسحب الأموال من البنوك.

وأضاف المتهمون بأنهم قاموا باستخدام تقنية معروفة تعتمد على زرع أداة في أجهزة الصراف الآلي تحتوي على كاميرا وماسح لنسخ تفاصيل البطاقة وأثناء قيام صاحبها باستخدامها لسحب الأموال النقدية، وبعد ذلك يقومون بالتواصل مع أفراد آخرين في العصابة المتواجدين في دولة أوروبية لإضافة هذه البيانات إلى بطاقة مزيفة حتى يستخدمها أفراد العصابة.

كما أوضحوا أن أفراد العصابة كانوا حذرين أثناء عملية سحب الأموال حيث كانوا يقومون بسحب مبالغ مالية متفاوتة مع مراعاة عدم تجاوز الحد الأعلى المسموح به، وكانوا يستخدمون البطاقة لمرة واحدة فقط حتى يقوموا بإثارة شك البنوك المستهدفة.

كما شددوا على أهمية الاشتراك في خدمة الرسائل النصية التي تقدمها البنوك حتى يتلقى المتعامل رسالة نصية فورية من البنك عند إجراء اي تعاملات مصرفية وبالتالي يمكن الإبلاغ بسرعة عن أي محاولات لسرقة الأموال أو أي تعاملات مشبوهة من أجل اتخاذ إجراء سريع.

(The National, 15 May, 2014, http://www.emaratalyoum.com/business/local/2014-05-15-1.676141)

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الاعتداء

الاعتداء يُعرف بأنه الأفعال التي تثير الغضب أو الاستياء أو الإهانة. على سبيل المثال، في دولة الإمارات العربية المتحدة يُعد إهانة أي شريعة إسلامية أو قيم مجتمعية أو أي شيء ضد أي دين معترف به جريمة.

الأسباب الكامنة وراء الجرائم الإلكترونية

تُرتكب الجرائم الإلكترونيّة لأسباب عديدة منها ما يلي:

- سعيًا وراء الشهرة، والحصول على سمعة بالذكاء أو الألمعية.
- نتيجة سوء السلوك ليس إلا.
- لأسباب مالية.
- للثأر من شخص ما يشعر المهاجم تجاهه بالكره.
- للتعبير عن أحد أشكال الاحتجاج.
- لتعقب الأنشطة الإجرامية بشكل بحت.
- لسرقة الهُوية.
- لتزوير المستندات والرسائل.

قانون الجرائم الإلكترونيَّة في دولة الإمارات العربيَّة المتحدة

تنص المادة رقم (35) على أن إرتكاب جرائم الإساءة الى المقدسات والأديان وتحسين المعاصي عن طريق شبكة المعلوماتية.

مع عدم الإخلال بالأحكام المقررة في الشريعة الإسلامية، يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من ارتكب عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات أو على موقع إلكتروني، إحدى الجرائم التالية:

1. الإساءة إلى أحد المقدسات أو الشعائر الإسلامية.
2. الإساءة إلى أحد المقدسات أو الشعائر المقررة في الأديان الأخرى متى كانت هذه المقدسات والشعائر مصونة وفقًا لأحكام الشريعة الإسلامية.
3. سب أحد الأديان السماوية المعترف بها.
4. تحسين المعاصي أو الحض عليها أو الترويج لها.

وإذا تضمنت الجريمة إساءة للذات الإلهية أو لذات الرسل والأنبياء أو كانت مناهضة للدين الإسلامي او جرحًا للأسس والمبادئ التي يقوم عليها، أو ناهض أو جرح ما علم من شعائر وأحكام الدين الإسلامي بالضرورة، أو نال من الدين الإسلامي، أو بشر بغيره أو دعا إلى مذهب أو فكرة تنطوي على شيء مما تقدم أو حيذ لذلك أو روج له، فيعاقب بالسجن مدة لا تزيد على (7) سنوات.

وفقًا للمادة رقم (21)، الإعتداء على خصوصية شخص في غير الأحوال المصرح بها قانونيًا باستخدامه شبكة معلوماتية.

يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية، أو نظام

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً بإحدى الطرق التالية:

1. استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية.
2. التقاط صور الغير أو إعداد صور إلكترونية أن نقلها أو كشفها أو نسخها أو الاحتفاظ بها.
3. نشر أخبار أو صور إلكترونية أو صور (فوتوغرافية) أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية.

كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين، كل من استخدم نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها.

دراسة حالة (4): المدونون بالشرق الأوسط

تم إدانة إثنين من الرجال اللذيْن كانا يديران منتدى على شبكة (الإنترنت) في الإمارات العربية المتحدة وفرضت عليهما غرامة وفقًا للقانون من أجل نشر التعليقات التي تم اعتبارها تعليقات تشهيرية.

حكم على مدون بالسجن (4) سنوات بعد أن سخر من سلطة الرئيس المصري وإهانة الإسلام. يسمح قانون الصحافة لسنة 1996م بمحاكمة المجرمين عن هذه الجريمة (أنباء كاذبة)، وقانون العقوبات، الذي يمنع المواد التي تعتبر تشهيرية.

وطبقًا لما ذكره خالد السرجاني، رئيس تحرير جريدة الدستور المصرية، "فإن هناك مواضيع معينة ذات طبيعة محافظة لا يمكن عرضها على صفحات الصحف. حتى ولو لم يكن هناك اعتراض من السلطات، فإن نشر هذه المواضيع سيفتح فيضان من شكاوى القراء".

Committee to Protect Journalists, 14 October, 2009

http://www.cpj.org/reports/2009/10/middle-east-bloggers-the-street-leads-online.php

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

آثار الجريمة الإلكترونيّة

قد تتسبب الجرائم الإلكترونية في إلحاق خسائر فادحة للمنظمات فيما يتعلق بالأموال والإنتاجية والوقت، ناهيك عن السمعة.. وفيما يلي تلخيص لبعض الآثار:

1. **خسارة العوائد/الأرباح**

عد خسارة العوائد من أضخم التداعيات التي تنجم عن الجرائم الإلكترونية على الشركات. ويمكن أن يحدث ذلك عندما يتم تسريب المعلومات المالية الحساسة للشركة أو عندما تتم سرقتها واستخدامها من قبل أطراف خارجية لسحب المبالغ المالية بشكل غير قانوني من الحسابات الخاصة بالشركة. كما يمكن أن يحدث ذلك لشركة تعرض موقع التجارة الإلكترونية الخاص بها إلى الخطر، ويسبب ذلك فقدان دخل هام حيث لا يتمكن المستهلكون من الدخول إلى الموقع.

2. **إضاعة الوقت الهام**

عندما يتم إجراء الجرائم الإلكترونية، يتم إجبار موظفي تقنية المعلومات على بذل المزيد من وقتهم للتعامل مع المشكلات التي تحدث وحلها. ويؤدي ذلك إلى إضاعة الوقت حيث يمكن استغلال مهاراتهم وخبراتهم في إجراءات لأغراض إنتاجية لصالح الشركة أو المنظمة. وبدلاً من ذلك، فإنه يتم استهلاك معظم وقتهم في التعامل مع الخروقات الأمنية وغيرها من المشاكل ذات الصلة بذلك والتي تنجم عن الجرائم الإلكترونية.

3. **الإضرار بالسمعة**

عندما تؤدي جريمة إلكترونية إلى السرقة أو إلى الاستخدام غير المشروع لسجلات المستخدم، يمكن أن تتضرر سمعة الشركة للغاية، حيث يبدأ العملاء في فقد الثقة في قدرة الشركة على الحفاظ على أمانها. ويمكن أن يشجع ذلك العملاء على البحث عن الأعمال التجارية في أماكن أخرى، كما يؤدي إلى فقد الشركة المتأثرة لدخل قيم بالإضافة إلى خسارة سمعتها.

4. **تقليل الإنتاجية**

بسبب الحدوث المتكرر للجرائم الإلكترونية، بدأت الكثير من الشركات في اتخاذ إجراءات لترقية الإجراءات الأمنية الخاصة بها. ويتطلب ذلك أن يقوم المستخدمون بإدخال المزيد من كلمات المرور وأرقام التعريف الشخصية الأمنية، بالإضافة إلى القيام بإجراءات أخرى تستهلك الوقت الذي يجب أن يتم استخدامه لإتمام المهام الخاصة بهم. ونتيجة لذلك، يتم تشتيت الموظفين عن عملهم، مما يؤدي إلى تقليل الإنتاجية.

حماية نفسك من الوقوع ضحية للجرائم الإلكترونيّة

دعونا نفكر للحظة ونتأمل في الأسباب التي تجعل الجرائم الإلكترونية تتزايد يومًا بعد يوم؟ ولماذا يقع عدد كبير من البشر ضحايا لهذه الجرائم؟ ربما لا يكمن السبب في طمع وأنانية المجرمين فقط.

ما لا نستطيع رؤيته هو أن أولئك الذين ينتهي بهم المطاف كضحايا هم أيضًا مخطؤون فيما يتعلق بالجرائم التي ترتكب بحقهم. وفي الحقيقة، فإن الكثير من الجرائم الإلكترونية، بدءًا من جرائم الاحتيال الصغيرة المتعلقة ببطاقات الائتمان وحتى عمليات السرقات الضخمة للبنوك، تتم بسبب جهلنا.

غالبًا ما نقوم بإعطاء المعلومات الضرورية الخاصة بنا إلى مواقع لا يتم التحقق منها، ولا يمكننا اتخاذ الإجراءات الأمنية الملائمة للحيلولة دون اختراق أجهزة (الكمبيوتر) الخاصة بنا. وبالتالي، يلعب مستوى الإجراءات الأمنية التي يتم اتخاذها ومستوى الوعي أثناء استخدام مواقع (الويب) دورًا هامًا لضمان أمان المعلومات الشخصية الخاصة بنا.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

نصائح: كيف تحمي نفسك من الوقوع كضحية للجرائم الإلكترونيّة

- لا تقم بادخال اسم المستخدم وكلمة المرور الخاصين بك عند استلام بريد الكتروني من شخص غير معروف أو في النوافذ المنبثقة، وعوضًا عن ذلك قم بفتح المتصفح واكتب عنوان الموقع مباشرة.
- لا تقم بتحويل مخاوفك حول كيفية حماية نفسك وجهازك إلى نقطة ضعف.
- لا تقم بتصفح المواقع المشبوهة، إن زيارة مثل هذه المواقع قد يزيد من احتمالية تعرضك لهجمة إلكترونية، تصفح المواقع الموثوقة حتى تبقى بأمان.
- استخدم كلمة مرور لا تقل عن (8) خانات والتي تحتوي على حروف وأرقام ورموز خاصة.
- قم بتأمين كلمات المرور الخاصة بك ولا تقم بمشاركتها مع الغير.
- لا تفتح رسائل البريد الإلكترونيّ ومرفقات البريد الإلكترونيّ الواردة من مرسلين غير معروفين.
- لا تفتح ملفات (.EXE) أو الملفات غير المعروفة بطريقة مباشرة في بريدك.
- قم بشراء برنامج مكافحة فيروسات وبرنامج أمان جيد مع تحديث تلك البرامج بشكل منتظم (مرة واحدة في الأسبوع على الأقل).
- استخدم برامج تفحص الفيروسات في كل الأقراص والمحركات ومحركات التصفح قبل محاولة الوصول إلى البيانات.
- قم بتأمين استعراض (الويب) أثناء التواجد على (الإنترنت).
- قم بعمل نسخ احتياطية منتظمة من البيانات الخاصة بك وقم بالتحقق من سلامتها.
- قم بعمل التحديثات بشكل منتظم فيما يتعلق بنظام التشغيل (Microsoft Windows) لجهاز (الكمبيوتر) الخاص بك.
- إذا كنت تمتلك اتصالاً عال السرعة بـ (الإنترنت) في مكتبك فضع في اعتبارك شراء برامج أو معدات الجدار الناري للمساعدة في حماية أنظمة (الكمبيوتر) الخاصة بك.
- إذا كنت تعتمد على شبكة لاسلكية أو إذا كنت تقوم بتشغيلها، فخذ الوقت اللازم لتأمينها وتحقق من أنك تفهم كيفية عملها.
- كن مسئولاً واستغرق وقتًا لمعرفة كيفية الاعتناء الأفضل بجهاز (الكمبيوتر) الخاص بك.
- تذكر أن جهاز (الكمبيوتر) الخاص بك هو تمامًا مثل سيارتك، يتطلب بعض أعمال الصيانة الأساسية في النظام من أجل أن يعمل بشكل جيد.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الحقوق القانونية لحماية الملكية الفكرية

التراخيص

يحتفظ المصنعون بسجلات للاستخدام القانونيّ لمنتجاتهم من خلال تقديم تراخيص سارية المفعول والتي في مقابلها يدفع المستخدمون أو المشترون. هناك عادة ثلاثة أنواع من تراخيص البرامج:

نوع الترخيص	ما يغطيه المستخدم
ترخيص لمستخدم واحد	لا يتم تثبيت هذا النوع من البرامج إلا على جهاز كمبيوتر واحد، مما يتيح الاستخدام لشخص واحد فقط في وقت معين لا يتمكن أحد من الدخول على (الكمبيوتر) الخاص بشخص ما واستخدام برمجياته، إلا إذا توقف مالك البرنامج عن العمل على (الكمبيوتر).
ترخيص الاستخدام المتعدد	يتيح ترخيص الاستخدام المتعدد لأكثر من شخص استخدام البرنامج على عدة أجهزة، مثلاً (20) جهازًا. ولذلك فإن الترخيص لـ (20) مستخدمًا يتيح لـ (20) فردًا استخدام البرنامج في شبكة معينة في أي وقت. كان الـ (20) مستخدمًا يستخدمون البرنامج في نفس الوقت، ورغب شخص آخر في استخدامه، فلن يمكنه/يمكنها ذلك إلا إذا سجل أحد المستخدمين الأصليين خروجه من البرنامج أو أغلق البرنامج أو (الكمبيوتر).
ترخيص الموقع	ترخيص الموقع يتيح لأي شخص على موقع معين أو في مكتب ما أن يستخدم البرنامج. فيمكن تثبيته وتنزيله على جميع الحواسيب، ويمكن لأي شخص يتصفح الموقع أن يستخدمه. في بعض الحالات، يشمل ترخيص الموقع تنزيل البرنامج على أجهزة (الكمبيوتر) المحمولة الخاصة بطاقم عمل شركة ما، بحيث يمكنهم الاستفادة منه أثناء تنقلاتهم. وهذا قد يمتد ليشمل الاستخدام المنزلي، لكن هذا يتوقف على الشروط والأحكام المنصوص عليها في ترخيص الموقع. وبالتالي، فلا تفترض أنك يمكنك القيام بذلك.

البرامج المجانية والتجريبية

بغض النظر عن البرامج التي يجب أن تدفع مقابل استخدامها، يوجد نوع آخر من البرامج يطلق عليه اسم (البرامج المجانية). وتسمح البرامج المجانية للمستخدم بتنزيل أو نسخ أو تمرير أو استخدام البرنامج بدون شراء ترخيص. ولا تضع البرامج المجانية شروطًا على وقت الاستخدام، مما يعني أنه يسمح للمستخدمين بالاستفادة من تلك البرامج طالما أرادوا ذلك. وبالإضافة إلى ذلك، لا يتم تعطيل أي جزء من البرامج المجانية، مما يسمح للمستخدمين بالاستفادة الكاملة منها. ومع ذلك، فإن كون هذه البرامج مجانية لا يعني أنها غير محفوظة بحقوق الطبع والنشر، فهذه البرامج لا تزال تعتبر ملكية فكرية لمطوريها.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

	البرامج المجانية	البرامج المشتركة
ما هي	يشير هذا المصطلح إلى البرامج التي تتوفر للجميع لتحميلها عبر (الإنترنت) واستخدامها بشكل مجاني.	هي البرامج التي تعطي المستخدم الفرصة لتجربة البرنامج قبل شراءه.
الخصائص	جميع الخصائص تتوفر بشكل مجاني.	لا تحتوي على كافة الخصائص غالبًا أو يمكن استخدامها بشكل محدود، ومن أجل الاستفادة من جميع الخصائص يتعين على المستخدم شراء النسخة الكاملة.
التوزيع	توزع بشكل مجاني.	قد توزع بشكل مجاني أو بمقابل مادي. وفي أغلب الأحيان يجب الحصول على إذن من مالك البرنامج لتوزيعه.
أمثلة عليها	(Adobe reader), (VLC Player).	(Winrar)، أو أي برنامج تجريبي.
الإيجابيات	مجانية وتمنح المستخدم الصلاحيات الكاملة.	تمنح المستخدم فرصة تجربة البرامج المكلفة مجانًا.
السلبيات	لا يمكنك بيع البرامج المجانية، كما أن النسخ المعدلة منها يجب أن تكون مجانية كذلك.	لا يمكن تعديلها وعادة ما تكون نسخة غير كاملة أو مؤقتة.
http://www.diffen.com/difference/Freeware_vs_Shareware		

إتفاقية ترخيص المستخدم (End User License Agreement) – (EULA)

لا يعني شراء نسخة من البرنامج أنك امتلكت البرنامج ذاته. فما دفعت مقابله بالفعل هو مجرد ترخيص يتيح لك استخدام البرنامج بشكل قانوني. ويحق لك تحميل وتثبيت البرنامج على جهاز (الكمبيوتر) الخاص بك، كما يحق لك استخدامه لفترة زمنية غير محددة. ومع ذلك، يحظر عليك مشاركة البرنامج مع الأصدقاء من خلال تثبيته على أجهزة (الكمبيوتر) الخاصة بهم إلا إذا دفعوا مقابل الحصول على ترخيص لاستخدام هذا البرنامج.

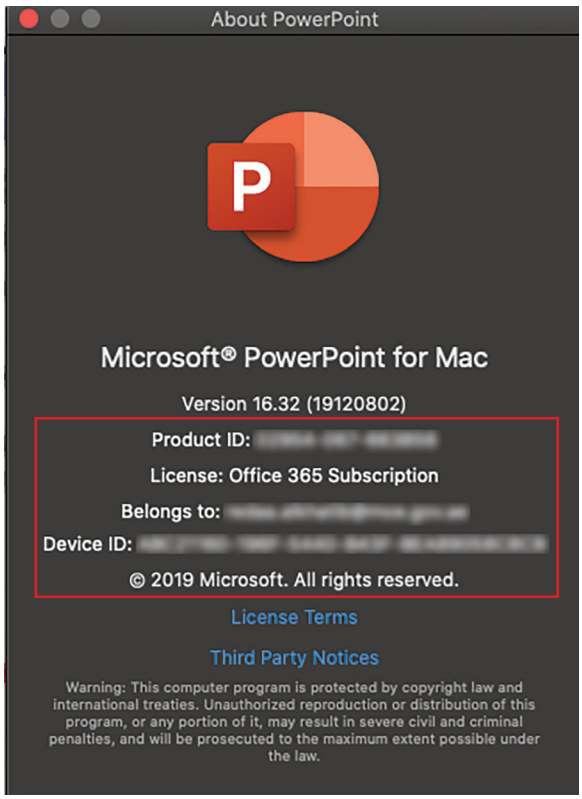
كما يطلق على الترخيص الذي يأتي مع البرامج التجارية أيضًا اسم اتفاقية ترخيص المستخدم النهائي، والتي يشار إليها اختصارًا بـ (EULA). وتوضح هذه الاتفاقية ما هو مسموح به فيما يتعلق بتثبيت البرنامج وعمل النسخ منه. وتظهر اتفاقية ترخيص المستخدم النهائي (EULA) في أول شاشة لمعالج التثبيت عندما تبدأ تثبيت البرنامج. ولمتابعة التثبيت، يجب أن تقوم بقراءة والموافقة على الشروط الموضحة في الترخيص.

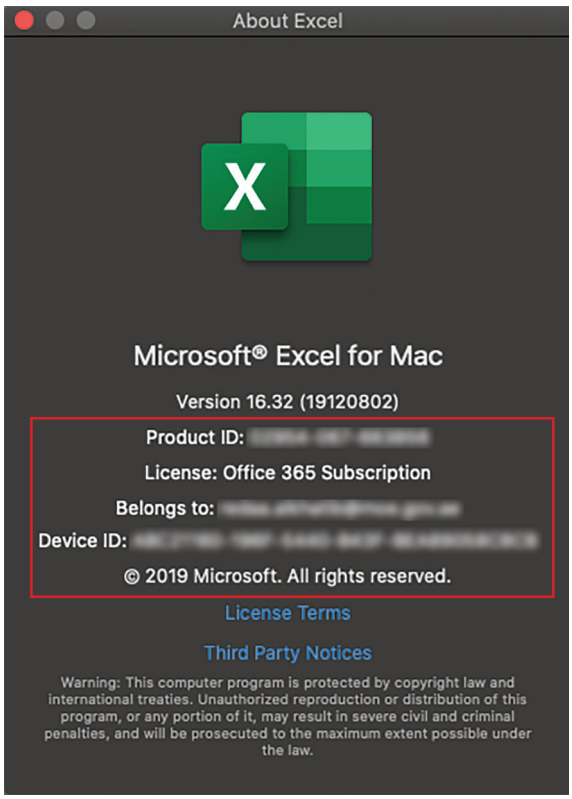
حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

رقم تعريف المنتج

يمكنك التحقق من أنك تستخدم نسخة صالحة من البرنامج من خلال التوجه إلى قائمة (Help) التعليمات ومن قائمة (Help) التعليمات، انتقل إلى خيار (About) حول. يسمح لك ذلك بعرض الشخص الذي تم ترخيص البرنامج له، بالإضافة إلى المعرف الصالح للبرنامج. جرب هذا الأمر الآن مع البرنامج الذي تستخدمه.

إذا تم منحك برنامج مجاني على أقراص مرنة أو على أقراص (CD)/(DVD) أو على شرائح ذاكرة، فتحقق من كون البرنامج نسخة أصلية، ودائمًا قم بفحص معرف البرنامج واتفاقية ترخيص المستخدم النهائي (EULA) قبل تثبيت البرنامج.





التشريعات

يغطي قانون حقوق الطبع والنشر، والتصميمات، وحقوق الطبع والنشر مشكلة القرصنة على البرامج. وهناك ثلاثة أشياء رئيسية يغطيها هذا القانون:

- لا يسمح القانون بنسخ البرامج دون الحصول على إذن من المالك. شراء الترخيص لا يجعلك صاحب البرنامج، بل فقط يتيح لك الحق في استخدامه.
- لا يُسمح قانونيًا باستخدام البرامج المقرصنة.
- لا يسمح قانونيًا بنقل البرامج المقرصنة عبر خطوط الاتصالات السلكية واللاسلكية.

يعد نسخ برنامج من قرص مدمج أو مضغوط أمرًا غير قانوني تمامًا كما هو غير قانوني إذا تم عبر شبكة (الإنترنت) أو عبر خط هاتفي، أو بنفس درجة عدم قانونية تسجيل أحدث الأفلام في السينما بما يخالف القانون.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

القواعد واللوائح التي تحكم استخدام الاتصالات والتقنيات

البيانات الشخصية

تشير البيانات الشخصية إلى أي بيانات تشير إليك، مثل: اسمك، وعنوان المنزل، وعنوان البريد الإلكتروني، ورقم الهاتف، وما إلى ذلك. وكل يوم، يتم تجميع بياناتك أو تقوم أنت بمنحها بشكل مجاني عبر شبكة (الإنترنت).

إليكم بعض أمثلة المنظمات أو المؤسسات التي يمكن الوصول إلى المعلومات الشخصية الخاصة بك من خلالها:

- المدارس والمؤسسات التعليمية – تقوم المدارس والجامعات والكليات بشكل طبيعي بتجميع المعلومات الشخصية الأساسية الخاصة بالطلبة الدارسين بها بهدف الاحتفاظ بسجلات لهم، ولأغراض إدارية كذلك. وعلى أقل تقدير، فإنهم سوف يحصلون على اسمك، وعنوان المنزل، ورقم الاتصال بك، وتاريخ الميلاد، والأوضاع الطبية، والحساسية، بالإضافة إلى أرقام الاتصال بوالديك أو الأوصياء عليك. والهدف من ذلك هو إرسال الخطابات عبر البريد والاستمرار في الاتصال بوالديك أو بالأوصياء عليك.

- المستشفيات/العيادات – في كل مرة تزود فيها مستشفى/عيادة، ستسأل هل هذه هي زيارتك الأولى. وإذا كانت تلك الزيارة هي الزيارة الأولى، يطلب منك ملء نموذج باسمك وبيانات الاتصال بك. وإذا كان لديك طبيب للعائلة، أو إذا كنت تذهب بشكل عام إلى طبيب واحد فقط، فسيطلب منك أيضًا تقديم المعلومات الشخصية الخاصة بك. والهدف من وراء ذلك هو أن يتمكنوا من الاحتفاظ بسجل بكل الأدوية التي تتناولها في كل مرة تقوم بزيارة طبيب فيها. وبالتالي، إذا حدث أي شيء خطأ، يمكنهم الرجوع إلى السجلات الخاصة بك واكتشاف المشكلة. كما تعتبر البيانات أيضًا مفيدة بالنسبة لأنظمة تحديد المواقع العالمية (GPS) لتقييم الصحة العامة للسكان المحليين.

- البنوك وبناء المجتمعات – غالبًا ما تمتلك منظمات مثل: تلك المنظمات أسماء وتفاصيل الاتصال بأعضائها أو عملائها. فكل عملية مفردة، سواء كانت عبارة عن إيداع أو دفع أموال، يتم تسجيلها، حتى إذا أثيرت أية استفسارات حيال الحساب الخاص بك، يمكن للبنك فحص التفاصيل لهذه المعاملة بعينها. ويفيد ذلك بشكل خاص لتتبع الجرائم مثل سرقة الأموال أو الاحتيال. ويمكن أن يسجل البنك أيضًا المبلغ المالي، والوقت المحدد للمعاملة، والتاريخ، والفرع الذي جرت به المعاملة، في كل مرة تقوم فيها بسحب الأموال من أجهزة الصراف الآلي التلقائية (ATM). ويمكن أن يستخدم البنك هذه المعلومات لتحديد عدد نقاط صرف الأموال اللازمة بالإضافة إلى المبالغ المالية التي يجب تحميلها في تلك الماكينات كل يوم.

- التجارة الإلكترونية – إذا تسوقت عبر (الإنترنت)، فعليك أن تعرف وتدقق في أن جميع التفاصيل الصغيرة لمعاملتك قد سجلت من قبل المتجر. فهذه البيانات تفيدهم في معرفة الأشياء التي تلقى اهتمامك بشكل كبير. وفي المرة القادمة التي تسجل فيها دخولك على المتجر، ستتلقى إعلانات أو عروض خاصة بالأشياء التي يظن المتجر أنها قد تحظى باهتمامك.

- الحكومة – تقوم الحكومة بصفة دائمة بتجميع البيانات من المواطنين كل (10) أعوام أثناء الإحصاء السكاني الذي تقوم به. ويتم استخدام هذه البيانات، بين أمور أخرى، للتخطيط للإسكان ووسائل الراحة المحلية.

وهناك العديد من الجهات والمنظمات الأخرى التي تقوم بتجميع البيانات والمعلومات الشخصية الخاصة بك. وإذا فكرت في الأمر بشكل فعلي، فقد لا تشعر بالأمان المطلق، لأن المعلومات الخاصة بك يمكن أن يتم الحصول عليها بكل سهولة، كما يمكن إساءة استخدامها من قبل أشخاص غير مسؤولين!

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

قانون حماية البيانات والمصطلحات المتعلقة به

سبب تزايد أعداد المعلومات الشخصية التي يتم تجميعها بشكل يومي، قامت بعض الدول بوضع قانون حماية البيانات لحمايتك كعميل. ويضمن هذا القانون أن يتم استخدام أية بيانات تقوم بإعطائها للغير وأن يتم تخزينها لصالحك وبما يحقق لك الأمان.

ولفهم هذا الموضوع، يجب أن تدرس وأن تتذكر المصطلحات المذكورة أدناه:

المصطلح	التعريف
البيانات الشخصية	البيانات الشخصية هي المعلومات والآراء الواقعية الخاصة بشخص ما، بما في ذلك الاسم، والعناوين، وتاريخ الميلاد، والحالة الاجتماعية،وحتى الرصيد الحالي في البنك. وتشتمل الأمثلة الأخرى على تاريخ الحالة الصحية، وتصنيف بطاقة الائتمان، والسجلات الجنائية.
موضوع البيانات	يشير ذلك إلى الشخص الذي يتم أخذ البيانات منه أو الذي تدور البيانات حوله. ويمكن أن يكون هذا الشخص أنت!
مستخدم البيانات	يشير ذلك إلى أي شخص يحتاج إلى استخدام البيانات التي تم الحصول عليها أو الوصول إلى تلك البيانات بهدف إتمام المهام المتعلقة به. ويمكن أن يكون هذا الشخص هو سكرتير المدرسة الذي يحتاج إلى معرفة عنوان المنزل الخاص بك لكي يرسل الخطابات أو الوثائق الهامة إلى أولياء أمرك. كما يمكن أن يكون طبيبك الذي يحتاج إلى معلومات حول أنواع الحساسية التي تعاني منها قبل إعطائك الدواء المناسب لك.
المتحكم في البيانات	غالبًا، ولكن ليس بالضرورة، يشير هذا المصطلح إلى رئيس، أو المسئول عن، المنظمة التي تمتلك البيانات الخاصة بك. ويكون هذا الشخص هو من يقرر نوع البيانات المطلوب تجميعها والغرض الذي يجب استخدامها من أجله. ويجب أن يطلب هذا الشخص الإذن لتجميع البيانات وتخزينها من العملاء.
مفوض البيانات	يشير هذا المصطلح إلى الشخص المسئول عن تفعيل قانون حماية البيانات، والذي يجب أن تقوم المنظمات بالتقدم بالطلبات إليه للحصول على اذن لتجميع وتخزين البيانات الشخصية.

مبادئ حماية البيانات

حماية أمان العملاء، تقع المسؤولية على عاتق المتحكم في البيانات لضمان أن المنظمات ذات الصلة التي يعملون بها تتبع المبادئ الثمانية التي تم وضعها من قبل قانون حماية البيانات بكل صرامة، متى تم التعامل مع البيانات الشخصية للأفراد. وبصفتك من العملاء، يجب أن يكون لديك إدراك كامل وواضح لهذه المبادئ، ويجب أن تكون قادرًا على مناقشة ثلاثة أو أربعة منها على الأقل. وبتلك الطريقة، سوف تكون مدركًا لحقوقك فيما يتعلق ببيانتك الشخصية بكل وضوح.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المبدأ	الشرح
يجب أن يتم الحصول على المعلومات ومعالجتها بشكل عادل وقانوني	في جميع الأحوال، يجب إعلامك بسبب جمع البيانات الخاصة بك ومتى سيتم ذلك.
موضوع البيانات	يشير ذلك إلى الشخص الذي يتم أخذ البيانات منه أو الذي تدور البيانات حوله. ويمكن أن يكون هذا الشخص أنت!
يجب ألا يتم الاحتفاظ بالبيانات الشخصية إلا من أجل أغراض محددة وقانونية	يجب أن يقدم المتحكم في البيانات أسبابه لتجميع وتخزين البيانات الخاصة بك عند الحصول على إذن للقيام بذلك. ويعتبر استخدام البيانات الخاصة بك بما يتجاوز الغرض المحدد جريمة.
يجب أن تكون البيانات الشخصية كافية، وذات صلة، وغير زائدة عن الحد مقارنة بالغرض المطلوبة من أجله	يسمح للمنظمات بتجميع البيانات المحددة التي يحتاجون إليها فقط بدون زيادة. على سبيل المثال، تحتاج المدرسة الخاصة بك إلى معلومات لمساعدتها على الاتصال بوالديك في حالات الطوارئ، إلا أنه قد لا يكون من الضروري بالنسبة لهم معرفة اسم سيارتك المفضلة أو الطعام المفضل لجدتك. ويجب ألا يتم تجميع هذا النوع من البيانات أو تخزينها لأنها تعتبر زائدة عن الحاجة وغير ذات صلة فيما يتعلق بمساعدتك بخصوص التعليم.
يجب أن تكون البيانات الشخصية دقيقة وحديثة	يجب أن تتحقق المنظمات من أن المعلومات المتوافرة لديهم عنك صحيحة في وقت تجميعها. فمن وقت لآخر، يمكن أن تتغير بعض التفاصيل. وبالتالي، يجب أن تقوم تلك المنظمات بفحص تلك المعلومات وتحديثها بشكل منتظم. على سبيل المثال، قد يطلب من والديك التحقق من المعلومات الخاصة بك أو تأكيدها كل عام للتحقق من استمرارية صحة تلك المعلومات. إذا كان هناك أي طلب من العميل لتغيير أية معلومات، فيجب أن تلتزم الشركة بذلك،شريطة أن يقوم العميل دليلاً على ضرورة وصحة هذا التغيير.
يجب ألا يتم الاحتفاظ بالبيانات الشخصية لمدة أطول من اللازم	يجب أن يتم الاحتفاظ بالبيانات الشخصية لمدة محددة فقط. على الرغم من أن المستشفيات قد تحتاج إلى الاحتفاظ بسجلات المرضى لمدة لا تقل عن (25) عامًا لأن تلك المعلومات يمكن أن تكون ضرورية لتوفير العلاج في المستقبل، إلا أنه قد لا يكون هناك سبب ملائم لتخزين المعلومات الخاصة بمقدمي الطلبات الذين لم يتمكنوا من تحقيق النجاح في الحصول على الوظائف.
يجب أن يتم التعامل مع البيانات بما يتوافق مع حقوق موضوع البيانات	يجب أن تدرك أنك لديك الحق لرؤية وفحص المعلومات التي تخزنها المنظمات (باستثناء بعض الحالات الخاصة التي سيتم توضيحها أدناه). وإذا كانت البيانات المحفوظة بخصوصك غير صحيحة، فمن حقك أن تطلب أن يتم تغيير تلك البيانات.
يجب أن يتم اتخاذ إجراءات أمان ملائمة ضد الوصول غير المرخص به	يجب أن يتم الحفاظ على سرية وأمان المعلومات الخاصة بك والتي يتم تجميعها ضد الهاكرز والموظفين الذين لا يحتاجون إلى رؤية تلك البيانات. كما يجب أيضًا أن تتم حماية كل البيانات ضد فقدها بشكل عرضي غير مقصود.
لا يمكن أن يتم نقل البيانات الشخصية إلى دول أخرى	إذا قررت شركة ما مشاركة البيانات مع منظمة أخرى في دولة أخرى، فيجب على الشركة أن تتحقق من أن الدولة التي يتم إرسال المعلومات إليها تتوافر لديها وسائل حماية كافية أو مشابهة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

مصداقية الموارد التي تتوفر على (الإنترنت)

بعد أن أصبح بإمكان أي كان أن يصبح مالكاً أو مؤلفًا لمحتوى ما عبر (الإنترنت)، فقد باتت مصداقية المواد التي يتم نشرها عبر (الإنترنت) موضعاً للشك. وعلى الرغم من هذا كله، ونظرًا للثورة الحاصلة في عمليات البحث الحديثة، تتوفر كميات هائلة من المعلومات التي لم تكن تتوفر في السابق للباحثين عبر (الإنترنت)، ويخسر الباحثون الذين لا يستفيدون من هذه الميزة الكثير.

نصائح: الطرق الشائعة للتميز بين الجيد والسيء

- ابحث عن المواقع المعروفة ذات السمعة الطبية، موقع بي بي سي على سبيل المثال: (www.bbc.com) هو عبارة عن شبكة إخبارية باللغة الإنجليزية ويتوفر منه نسخة باللغة العربية، يقع المكتب الرئيسي في لندن وفي الشرق الأوسط يقع المكتب الرئيس في القاهرة بالإضافة إلى قرابة (72) مكتب إخباري حول العالم، ويصل بثهم إلى أكثر (233) مليون منزل في أكثر من (100) دولة حول العالم. وبناء على ذلك يمكن اعتبارها مصدرًا موثوقًا للمعلومات التي تتوفر للعامة.
- يمكن معرفة فيما إذا كان مصدر المعلومات موثوقًا من اسم النطاق الخاص به، غالبًا ما تعتبر المواقع التي تنتهي بالنطاق (.gov) مصدرًا للبيانات الحكومية وبناء عليه فإن موقعًا مثل: (www.moi.gov.ae) على سبيل المثال يمكن أن يعتبر مصدرًا جيدًا للمعلومات، ومن المواقع الحكومية الموثوقة في دولة الإمارات (www.tra.gov.ae).
- لاحظ أن أغلب المواقع التجارية تستخدم النطاق (.com) ولذلك يجب عليك التعامل معها بحذر.
- إن المواقع التي تحتوي على اسم المؤلف وشهاداتها وبريده الإلكتروني يمكن اعتبارها على أنها ذات مصداقية، وأي مؤلف لا يقوم بالتعريف عن نفسه أو نفسها أو لا يمكن التواصل معه يجب التعامل معه في هذه الحالة بحذر.
- تأكد فيما إذا كان الموقع يعتمد أو يعترف بالمصادر التي يعتمد عليها، حيث يمكن لأي كان اختلاق الحقائق والأرقام. يمكنك التأكد من دقة الحقائق والأرقام إذا طالما أنها منسوبة إلى مصدر معين.

This is an excerpt from Fact and Figures from http://www.bbc.co.uk/arabic/institutional/2011/01/000000_aboutus

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الوصول غير المصرح به

أصبح الوصول غير المصرح به لأجهزة (الكمبيوتر) والخوادم والشبكات أمرًا مستجدًا في عالم التقنيات والاتصال، ويطلق على الشخص الذي يقوم بالوصول بطريقة غير مسموح بها اسم المخترق أو المخرب.

قانون الجرائم الإلكترونيَّة في دولة الإمارات العربيَّة المتحدة

المادة (2): دخول موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح.

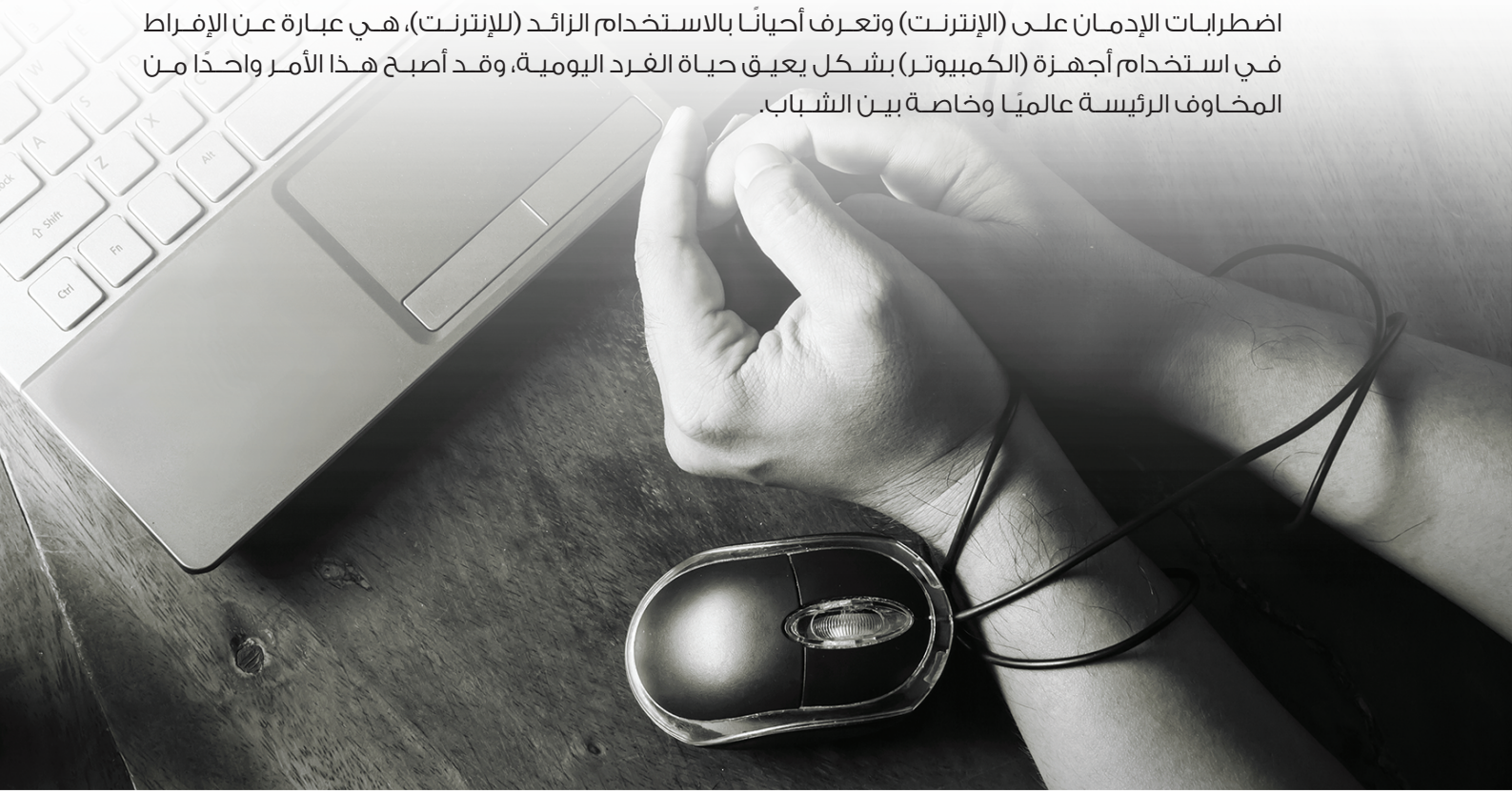
1. يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة.

2. تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب عليها بفعل من الافعال المنصوص عليها بالفقرة (1) من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات.

3. تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة (2) من هذه المادة شخصية.

اضطرابات الإدمان على (الإنترنت):

اضطرابات الإدمان على (الإنترنت) وتعرف أحيانًا بالاستخدام الزائد (للإنترنت)، هي عبارة عن الإفراط في استخدام أجهزة (الكمبيوتر) بشكل يعيق حياة الفرد اليومية، وقد أصبح هذا الأمر واحدًا من المخاوف الرئيسة عالميًا وخاصة بين الشباب.



حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تمرين

1. **بماذا يمكن أن نسمي الأشخاص الذين يقتحمون أجهزة (الكمبيوتر) بدون نوايا سيئة؟**
   - أ. المتسللون.
   - ب. (الهاكرز).
   - ج. (الكراكرز).
   - د. مقتحمو الخطوط الهاتفية.

2. **يقول اتحاد البرامج التجارية أن "الأفراد يزورون مواقع شبكات النظير إلى النظير (P2P) ومواقع المزادات بأعداد ضخمة للحصول على البرامج غير القانونية أو لنقلها". بناءً على هذه العبارة، ما هي التأثيرات السلبية التي يتسبب هؤلاء الأفراد فيها؟**
   - أ. المساعدة في انتشار البرامج الضارة وبرامج التجسس.
   - ب. المساهمة في ترويج صناعة البرمجيات.
   - ج. المساعدة في تجاوز "الفجوة الرقمية".
   - د. المساعدة في توسيع تبني التقنيات عبر برامج رخيصة الثمن.

3. **أي الأشياء التالية لا يعد من آثار استخدام البرمجيات المقرصنة؟**
   - أ. المساعدة في انتشار الفيروسات للمستخدم النهائي.
   - ب. خسارة مصنع البرمجيات للعائدات.
   - ج. ضييع الوقت في مكافحة قضايا القرصنة.
   - د. خطر عدم منح المستخدم النهائي ضمان للمنتج.

4. **قمت للتو بشراء بعض ملفات الموسيقى من متجر على (الإنترنت). أي من الإجراءات التالية يعتبر قانونيًا؟**
   - أ. تبادل الأغاني على موقعك الشخصي.
   - ب. إرسال نسخ من الأغاني عبر البريد الإلكتروني لأصدقائك المقربين.
   - ج. تحويل الأغاني إلى نغمات رنين للاستخدام الشخصي.
   - د. بيع الأغاني إلى أصدقائك المقربين بسعر أقل.

5. **اذكر سببين هامين يوضحان حاجة القانون الإلكتروني للتطوير المستمر (اختر إجابتين).**
   - أ. للتعامل بشكل أفضل مع النمو الحادث في استخدام (الإنترنت).
   - ب. لتوفير الوسائل الملائمة للنمو السريع في التجارة الإلكترونية.
   - ج. لتبرير الحاجة إلى المزيد من محترفي قانون (الإنترنت).
   - د. لتفسير العدد المتزايد من الوسائط الرقمية.
   - ه. لإدارة التهديدات التي تظهر من أنشطة (الإنترنت) الجديدة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

6. **لقد طور آدم برنامجًا ويرغب في بيعه على (الإنترنت) فما هي أفضل وسيلة لحماية الملكية الفكرية للبرنامج؟**

أ. تسجيل براءة اختراع للبرنامج.

ب. الاشتراك في خدمة (https).

ج. إعداد اتفاقية ترخيص المستخدم.

د. التحكم في مفتاح التنشيط عبر التسجيل.

الإجابة: 1.ب، 3.أ، 4.د، 5.ب وه، 6.أ

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

04 الأمان الإلكترونيّ

ترشدك هذه الوحدة، الأمان الإلكتروني، حيال كيفية حماية المعلومات الهامة من التهديدات التي تظهر على شبكة (الإنترنت).

وتغطي هذه الوحدة الإجراءات وأفضل الممارسات فيما يتعلق بحماية الأمان الشخصي الخاص بك. وهي تعرض لمفهوم اللصوص والإباحية، والمشهور اختصارًا بـ (2P). كما تلقي هذه الوحدة الضوء أيضًا على بعض الاحتياطات التي يجب اتخاذها لضمان أمان الشبكات الخاصة بك. إن حماية المعدات الخاصة بالشخص ليست مسألة مسئولية شخصية فقط، بل إن هذا الأمر ضروري أيضًا لحماية المجتمع.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أهداف التعلُّم

أهداف هذه الوحدة هي:

- توفير معلومات عن الاختراقات والهجمات الإلكترونية.
- توضيح عواقب الاختراقات والهجمات الإلكترونية.
- توفير أدلة حماية من الاختراقات والهجمات الإلكترونية.
- التركيز على القضايا المتعلقة بالسلامة الإلكترونية.
- التمييز بين استغلال المصادر المتبادلة والمخصصة.

نواتج التعلُّم

في نهاية هذه الوحدة، سوف تكون قادرًا على:

- تحديد شروط وآثار الهجمات الإلكترونية.
- التعرف على الأنواع المختلفة من وسائل الحماية ضد الإنتهاكات على (الإنترنت).
- شرح أهمية والتأكيد على سلامة (الإنترنت) الخاص بك.
- توضيح المخاوف الأمنية والأخطار على الخصوصية عند استعمال شبكات التواصل الاجتماعية والحوسبة السحابية.

قائمة المراجعة

البنود	التحصيل العلمي	قبل	بعد
1	يمكن أن أصف الأشكال المختلفة للهجمات الإلكترونية واتخاذ الاحتياطات اللازمة ضد تلك الانتهاكات.		
2	يمكن أن أشرح كيف أقوم بتحديث برنامج الحماية ضد الفيروسات، وحماية المعلومات الشخصية.		
3	يمكن أن أقوم بتحديد القيود المفروضة على الموارد التي تتم مشاركتها في الأنظمة العالمية المربوطة من خلال الشبكات.		
4	يمكن أن أقوم بتقييم الإجراءات والقضايا الأمنية الرقمية غير الأخلاقية التي تؤثر على أمان البيانات الإلكترونية.		

التعليمات:

بعد الانتهاء من قراءة هذه الوحدة، يُرجى إكمال الاستبيان باستخدام المقياس التالي:

المقياس:

1. ليس لدي أدنى معرفة.
2. لدي معرفة محدودة.
3. على دراية وقادر على التوضيح الجيّد.
4. ذو كفاءة وإمكانية على الممارسة الكاملة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الأمان الإلكتروني - الإجراءات وأفضل الممارسات أثناء التواجد على (الإنترنت)

توفر شبكة (الإنترنت) الكثير من الموارد الرائعة لإجراء الأبحاث وتكوين الصداقات والاستمتاع.

ولسوء الحظ، إذا لم تكن حذرًا، يمكن أن تتم سرقة المعلومات الشخصية الخاصة بك، أو يمكن أن تصبح هدفًا للصوص (الإنترنت).

المخاطر المتعلقة بشبكة (الإنترنت)

1. يمكن أن تأتي التهديدات المتعلقة بشبكة (الإنترنت) بأشكال أو هجمات متنوعة.
2. يمكن أن تخلق شبكة (الإنترنت) وهمًا يقضي بأن الغرباء هم "أصدقاء" في واقع الأمر.
3. يمكن أن تسيء شبكة (الإنترنت) إلى سمعتك.

الأشكال الشائعة لانتهاكات الأمان الرقمي

سرقة الهوية

تحدث سرقة الهوية عندما يستخدم شخص ما المعلومات الشخصية الخاصة بك مثل: الاسم أو العنوان أو المعلومات المالية لتحقيق مصالح خاصة به. فبمجرد وصول اللصوص الإلكترونيين إلى المعلومات الشخصية الخاصة بك، يمكنهم إجراء عمليات شراء باستخدام بطاقة الائتمان الخاصة بك، أو فتح حساب ببطاقة ائتمان جديدة باسمك.

ولا تتوقف الأضرار الناجمة عن سرقة الهوية عند مجرد الخسائر المالية، بل يمتد الأمر إلى أن يتم إقران الضحايا بشكل وهمي بالأنشطة الإجرامية التي لم يقوموا بها مطلقًا.

دراسة حالة(5): رومانيون مسجونون بتهمة محاولة اختراق بيانات لعملاء بنك

حكمت محكمة الاستئناف في أبوظبي وقضت بسجن ثلاثة رومانيين لمدة ثلاثة سنوات وتغريمهم (30,000) درهم بعد سرقتهم لأموال من حسابات المصرف. تم القبض على الثلاثة عندما حاولوا تثبيت بعض الأجهزة الإلكترونيّة في عدة أجهزة للصراف الآلي في أبوظبي. عندما يستخدم الزبائن أجهزة الصراف الآلي، تقوم تلك الأجهزة بالكشف عن بيانات العملاء من خلال بطاقاتهم المصرفية وتمكّن الثلاثة من سرقة أموال العملاء. وكانت النيابة العامة قد أرفقت صورًا وأقراص (CD) تحوي صورًا للمتهمين أثناء تركيب وإزالة الأجهزة.

وكان المتهم الأول قد اعترف بتهمة تركيب الجهاز إلا أنه أنكر نية السطو زاعمًا أن هناك شخص مجهول قد طلب منه تركيب هذه الأجهزة. واعتقد أنها تابعة لوكالات تسويق أو وكالات إعلانية، وزعم أنه لم يعلم بكونها بيانات خاصة ببطاقات مصرفية إلى أن قُبض عليه.

ووفقًا لما ذكره المدعى عليه الثاني، فإنه قد طلب منه نزع الجهاز وأنه لم يسحب أية أموال. وقد اعترف أيضًا أمام المحكمة أنه سجن لمدة عام في دبي في أربع قضايا مشابهة وأكد أنه لم يعرف طبيعة الجهاز ولا استخدامه.

بينما اعترف الثالث أنه متهم بتوصيل الجهازين الأول والثاني. وقال أنه كان يبحث عن عمل في رومانيا حين طلب منه أحد المتهمين السابقين السفر إلى الإمارات لتوصيل الجهاز. ولم يكن يعلم أنه يستخدم في السطو.

الإمارات اليوم، 23 يونيو 2011

http://www.emaratalyoum.com/local-section/accidents/2011-06-23-1.405100

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الرسائل الإلكترونيّة الاحتيالية

الاحتيال هو الغش عن طريق البريد الإلكترونيّ حيث يقوم الجاني بإرسال رسائل بريد إلكترونيّ في صورة مشروعة في محاولة لجمع معلومات شخصية ومالية من مستلمي الرسالة.

أرسلت رسائل بريد الكتروني إلى عناوين بريد عشوائية مع الزعم بأنها مرسلة من مؤسسة أو شخص معروف، وتحث هذه الرسائل المستلمين على النقر على رابط إلى موقع وهمي.

تصعب التفرقة بين الموقع السليم والموقع الوهمي لأن المجرمين يقومون بنسخ اسم الموقع الأصلي باستثناء الجزء الأخير منه. فإذا قمت بزيارة موقع دون استخدام أي برنامج حماية أو متصفح (ويب) محمي، حينها يتمكن المتطفلون من تشغيل برامج ضارة مثل: أحصنة طروادة على جهاز (الكمبيوتر) الخاص بك. وغالبًا ما تخفي ملفات أحصنة طروادة نفسها في صورة برامج غير ضارة، مثل: الألعاب أو رسائل البريد الإلكترونية التي تحتوي على مرفقات. وعادة ما تطلب ملفات تروجان من المستلم فتح المرفقات أو النقر على رابط ينشط الفيروس على (الكمبيوتر).

دراسة حالة (6): الاحتيال، قد يُذهبُ أموالك

وَقَعَت موظفة تنفيذية في شركة نفط وغاز فريسة لعملية احتيال للاستيلاء على المال عندما قامت بتحديث حسابها المصرفيّ في موقع إلكتروني مزيف. تلقت الموظفة التي تبلغ من العمر (34) عامًا رسالة بالبريد الإلكترونيّ والتي كان من المفترض أن تكون من البنك، تطلب منها تحديث حسابها لأن البنك يجري تحديثات للخوادم. بدت الرسالة حقيقية والموقع بدا تمامًا مثل الموقع الأصليّ حتى أنها لم تتردد في تحديث حسابها. ومع ذلك، عندما حاولت سحب الأموال من حسابها بعد بضعة أيام، وجدته فارغًا. أدعت المرأة أنها لم تكن على بينة من عملية الاحتيال ونتيجة لذلك فقدت (4,100) رينغيت ماليزيّ. وقالت "بأنه من الصعب حقًا أن أقول أن الموقع وهميّ".

ذا ستار أون لاين، 18 يناير 2009 ،

http://thestar.com.my/news/story.asp?file=/2009/1/18/focus/3011417&sec=focus

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

القراصنة والمخترقين

يعرف القرصان بأنه الشخص الذي يتمتع بمعرفة لغات البرمجة وأنظمة (الكمبيوتر) ويمكن اعتباره خبيرًا في هذين الأمرين. وعادة ما يكون القراصنة مبرمجون يحاولون البحث عن ثغرات في الأنظمة لتعزيز معارفهم. وفي بعض الأحيان، قد يتبادل القراصنة المعلومات التي يعثرون عليها مع بعضهم البعض، ولكن ليس بنية الدخول إلى النظام أو الحصول على البيانات الشخصية لآخرين.

بينما المخترق، من جهة أخرى، هو الشخص الذي يدخل بصورة غير قانونية إلى نظام شخص آخر، بنية توزيع البرامج الخطيرة. فعلى سبيل المثال، يمكن للمخترق إفساد النظام بإتلاف البيانات الرئيسة.

قانون الجرائم الإلكترونيَّة في دولة الإمارات العربيَّة المتحدة

وفقا للمادة رقم (7)، تعديل أو إتلاف أو إفشاء معلومات أو بيانات متعلقة بفحوصات طبية أو تشخيص طبي أو علاج بغير تصريح.

يعاقب بالسجن المؤقت كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى بغير تصريح بيانات أي مستند إلكتروني أو معلومات إلكترونية عن طريق الشبكة المعلوماتية أو موقع إلكتروني أو نظام المعلومات الإلكتروني أو وسيلة تقنية معلومات وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي، أو علاج أو رعاية طبية أو سجلات طبية.

المادة رقم (10)، إدخال عمدًا وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام المعلومات الإلكتروني.

يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من أدخل عمدًا وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات.

وتكون العقوبة السجن والغرامة التي لا تجاوز خمسمائة ألف درهم أو إحدى هاتين العقوبتين إذا لم تتحقق النتيجة.

وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي يقصد به إغراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته.

تنص المادة رقم (14)، الحصول بدون تصريح على رقم سري أو شفرة أو كلمة مرور للدخول إلى وسيلة تقنية المعلومات.

يعاقب بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من حصل، بدون تصريح، على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات، أو موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو معلومات إلكترونية.

ويعاقب بذات العقوبة كل من أعد أو صمم أو أنتج أو باع أو اشترى أو استورد أو عرض للبيع أو أتاح أي برنامج معلوماتي أو أي وسيلة تقنية معلومات، أو روج بأي طريقة روابط لمواقع إلكترونية أو برنامج معلوماتي، أو أي وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة(7): تم طرد الطلاب وذلك لاختراقهم والعبث بنتائج الامتحانات

فقد فصلت المدرسة الثانوية للتكنولوجيا التطبيقية في أبو ظبي ثلاثة طلاب في الصف الحادي عشر لاختراقهم خادم المدرسة ومن ثم التلاعب في نتائج امتحاناتهم وكذلك في نسبة الغياب والحضور.

كما أجروا تعديلات مشابهة على نتائج زملائهم، ومنحوا أنفسهم درجات إضافية كمجاملة أو مساعدة، على حد قولهم في التحقيق. ومع ذلك، فقد أبلغ أحد هؤلاء الطلاب الإدارة عنهم.

وبعد التحقيق مع ثلاثتهم والحصول على اعترافات كتابية منهم، قرر معهد التكنولوجيا في أبوظبي فصلهم، في إشارة إلى أنهم قد ارتكبوا بالفعل عدة انتهاكات. ومن ذلك الاحتيال، والتزوير، وانتحال شخصيات الغير، والإدلاء ببيانات كاذبة، والتلاعب في مستندات رسمية. وأوصت اللجنة التعليمية بالمعهد بالفصل التأديبي للطلاب الثلاثة بعد منحهم فرصة دخول الإمتحان النهائي حرصًا على مستقبلهم. وشرحت اللجنة أن هذا الإجراء لا يهدف إلى تشويه سمعة الطلاب، ولكن لتلقينهم درسًا حتى يكفوا عن انتهاك قوانين المدرسة. وأعلن الطلاب الثلاثة أنهم لم يتخيلوا أن القضية قد تصل إلى هذه الدرجة وأن الأمر كان بالنسبة لهم مجرد مزحة وليس أمرًا جدي. واعتبروا إن إجراء الفصل التأديبي يعد جورًا عليهم، ويشعرون أنه لا يبدي أي تسامح معهم للحفاظ على مستقبلهم.

وقال أحد الطلاب الثلاثة بأن حلمه بالالتحاق بكلية الهندسة قد انهار تمامًا بعد اتخاذ هذا الإجراء في حقه. فهو لا يعرف أين يذهب، ولا يعرف إذا ما كانت هناك جامعة أخرى ستقبله. بينما وصف الطالب الثاني القرار بأنه قاس للغاية، مضيفًا أنه أثر على مستقبله وأسرته. وهو يشعر بالخزي من هذه الحادثة. بينما عبر الثالث عن أمنياته بمنحهم فرصة أخرى بعد أن أدرك جدية أفعاله.

وفي المقابل، أكد وكيل المدرسة الثانوية للتكنولوجيا التطبيقية، أن القرار اتخذ بعد عقد تحقيق في المخالفات، واعتراف الطلاب باختراقهم للنظام الأمني للمدرسة. وشدد على أن القرار يتوافق مع قواعد وأحكام المدرسة الثانوية، وأن إجراء الفصل التأديبي قد وافق عليه أعضاء اللجنة بالإجماع. كما منح الطلاب فرصة دخول امتحان هذا العام لمساعدتهم على الالتحاق بأية مدرسة أخرى في الإمارة، باستثناء مدارس التكنولوجيا التطبيقية.

وعزا قدرة الطلاب على قرصنة النظام الإلكتروني للمدرسة، لجودة التعليم والتدريب الفني الممتاز الذي كانوا يتلقونه. وعلى كل حال، فإن الطلاب قد استغلوا قدرتهم العلمية بشكل سلبي وغير قانوني، وهو ما أدى بهم إلى الحال الذي هم عليه الآن. كما أشار إلى أن المدرسة قد اتصلت بآبائهم قبل اتخاذ قرار وأطلعتهم على جميع الأدلة والتحقيقات. ولم ترفق شهادة سوء سلوك مع ملفاتهم حفاظًا على مستقبلهم، حتى يمكنهم استكمال تعليمهم في مدرسة أخرى.

الإمارات اليوم، 19 يونيو 2011

http://www.emaratalyoum.com/local-section/education/2011-06-19-1.404284

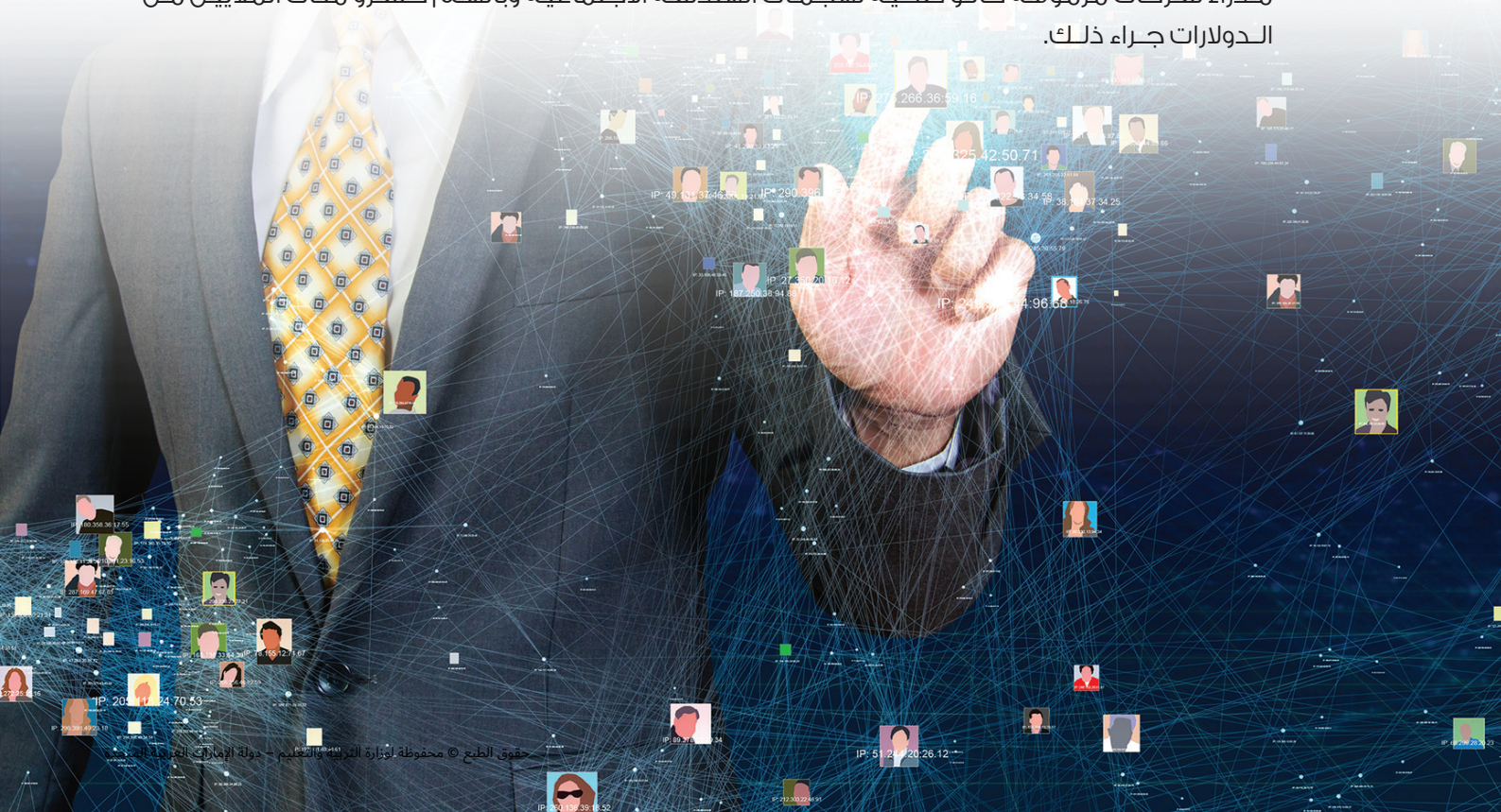
حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الهندسة الاجتماعية:

عند سؤال المستخدمين في التفكير في بأمن وسلامة بياناتهم ومعلوماتهم فإن أول أمر يطرأ على بال الكثيرين هي حماية أجهزتهم الذكية و الشخصية ويتم اهمال الجانب الآخر من القصة و هو العنصر البشري " والقصد هنا الشخص نفسه"، حيث يقوم الكثير من المستخدمين في هذه الأيام بحماية أنظمتهم واجهزتهم من حوادث الاختراق والقرصنة وسرقة البيانات من خلال التزود بأحدث أنظمة الحماية المتوفرة ويهملون بأنهم هم أنفسهم قد يكونون عرضة للتلاعب والخداع دون استخدام الكثير من التقنيات الحديثة وهذا مايراهن عليه الكثير من المخترقين في عصرنا الحالي. الإغراء، الخداع، فن التلاعب بمشاعر وأفكار المستخدم ، كلها وسائل ينتهجها المخترق في عصرنا الحالي للوصول إلى أكبر قدر من المعلومات والبيانات.

تُعرف الهندسة الاجتماعية (فن اختراق العقول) بأنها فن التلاعب النفسي بغرض خداع الضحية للوصول الى غرض ما – والهدف من ذلك في اغلبه هو الحصول على معلومات حساسة وفي غاية الأهمية، حيث يستخدم المتحايل مهاراته وقدارته لخداع ضحيته والاستيلاء على مايريده من معلومات قيمة قد تمثل كنزًا للمتحايل نفسه. والسؤال المطروح هنا "كيف يقوم المتحايل بايقاع ضحيته وخداعها"، الاجابة تمكن في قدرة المتحايل على الخداع والتضليل من خلال اعتماده على العامل النفسي كزرع الخوف في نفس الضحية وايهامها باختراق جهازه مثلاً وللحيلولة من ذلك وجب عليه إفشاء بعض المعلومات الحساسة ككلمات المرور، أو من خلال اللعب على وتر الإغراء بأن يتم إعلام الضحية بفوزه بجائزة مغرية وللحصول عليها وجب عليه إرسال بعض المعلومات الحساسة إلى المتحايل.

ربما يتبادر إلى ذهنك الآن بأن تلك الخدع لن تنطلي عليك وأنك حريص بما فيه الكفاية لافشاء معلومات وبيانات حساسة ككلمات المرور مثلاً أو أرقام بطاقات الائتمان، لكن يكفيك معرفة بأن مدراء شركات مرموقة كانو ضحية لهجمات الهندسة الاجتماعية وبأنهم خسرو مئات الملايين من الدولارات جراء ذلك.



حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

اقسام الهندسة الاجتماعية:

أولاً الهندسة الاجتماعية القائمة على العامل البشري (العامل النفسي).

ثانيًا الهندسة الاجتماعية القائمة على التقنيات مثل التصيد الاحتيالي عبر البريد الإلكتروني والاحتيال الصوتي وغيرها من التقنيات.

كيف أقوم بحماية نفسي وبياناتي من الهندسة الاجتماعية:

أولاً: تحقق دائمًا من الجهة التي تتحدث معها قبل القيام بمشاركة أي معلومات أو بيانات حساسة أو مهمة وتذكر دائمًا بعدم إفشاء معلومات ككلمات المرور أو أرقام بطاقات الائتمان إلى أي شخص أو جهة أيًا كانت.

ثانيًا: لا تنساق وراء المغريات الجذابة أو الإعلانات فقد تكون فخا يهدف إلى جمع المعلومات "كالضغط على صورة عبر البريد الإلكتروني تطلب منك التبرع لمؤسسات خيرية مثلاً".

ثالثًا: التأكد من تثبيت أحدث التقنيات المضادة للبرمجيات الخبيثة في الأجهزة وتحديثها باستمرار.

رابعًا: قم بالتبليغ عن أي حادثة تعرضت إليها إلى الجهات المختصة ولا تردد أبدًا في ذلك.

دراسة حالة (8): نصب بتقنية «الهندسة الاجتماعية»

كشفت الشرطة تفاصيل إحدى عمليات النصب التي كان ضحيتها شخص من الجنسية الآسيوية وتبدأ الحكاية عندما تلقّى هذا الشخص اتّصالاً هاتفيًا عشوائيًا من مجهول يتكلم بلغة آسيوية يفيده بأنه ربح جائزة مالية قدرها (200) ألف درهم، معرّفًا أنه المنظم التسويقي للجهة المهنية التي منحته الجائزة ووكيل خدماتها، طالبًا من الضحية نفسه إرسال مبلغ مالي، عبارة عن أرقام تعبئة الرصيد الهاتفي، وذلك ليتسنى له تسلّم جائزته على الفور، ليكتشف الضحية أنه وقع لعملية نصب، بعد أن أرسل تلك الأرقام التي كلفته مبلغًا كبيرًا، حيث عاود الاتصال بالمسوق ليجد أنه قد أغلق هاتفه المتحرك نهائيًا.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المطاردة الإلكترونية

تعتبر المطاردة الإلكترونيّة هي استخدام شبكة (الإنترنت) أو أي جهاز إلكتروني لمطاردة الآخرين. يحاول صائدو (الإنترنت) إيجاد معلومات عن ضحاياهم من مصادر مختلفة مثل: المدونات وخدمات البحث والمواقع الإلكترونيّة الاجتماعية.

حافظ على معلوماتك الشخصية آمنة؛ لا تجعلها عرضة للآخرين. لا تستخدم اسمك الحقيقي عند الاتصال في المنتديات وغرف الدردشة. استخدم أسماء المستخدمين التي لا تكشف عن نوع الجنس، وخاصة بالنسبة للنساء.

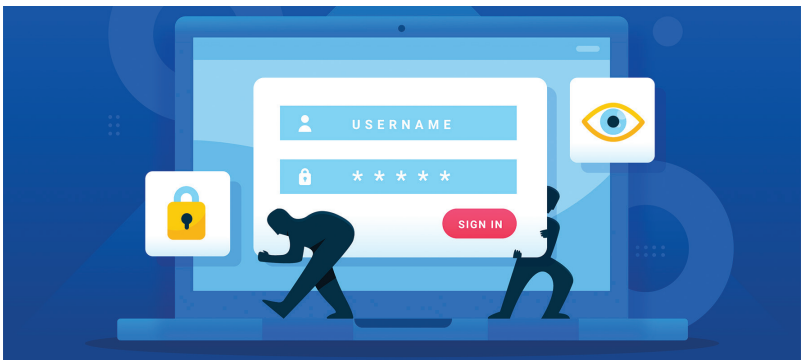
مفترس (الإنترنت)

مفترس (الإنترنت) هو من يبحث عن فريسة جنسية على (الإنترنت).

رسالة تحذير

عادة، ما يكون مفترسو (الإنترنت):

- ذكر.
- يقوم بإغواء الآخرين.
- منطوي.
- سادي (حُب تعذيب الآخرين).
- غير مميز جنسيًا.



لقد تم اعتراض أكثر من ضحية في وقت واحد باستخدام تقنيات مختلفة. البحث عن الضحايا في المواقع الشهيرة التي يزورها الصغار، والتظاهر بأنهم في نفس العمر.

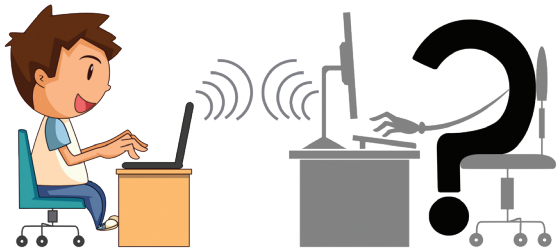
يبدأ مخترقوا (الإنترنت) عادة التحرش من خلال الطرق الخفية التي لا يمكن الكشف عنها من قبل معظم الشباب، وخاصة الأطفال. يتصرفون بلطف ومحاولة كسب ثقة الفتيات أو الأولاد حتى يتمكنوا من الالتقاء بهم في مكان خاص.

يظهر مخترقي (الإنترنت) الاهتمام والمودة والعطف وأحيانًا الهدايا. وبفعل ذلك يسلبون قلوب ضحاياهم، الذين يعانون عادة من الوحدة وإهمال آبائهم أو أولياء أمورهم لهم في بيوتهم. وعادة ما يرغب هؤلاء المفترسون في تقضية أوقات كبيرة، وبذل قدر كبير من المال والجهد في سبيل جذب ضحاياهم.

ويقضون وقتًا في ملاحظة أحدث الملفات الموسيقية والأنشطة التي تهم الأطفال، ويصبرون على سماع المشكلات. كما يحاولون الحد من كبح الشباب الصغير لرغباتهم، من خلال طرح محتوى في محادثاتهم. وقد وقع العديد من الشباب ضحايا لهذه المواقف، حيث تعرضوا للتحرش غير الأخلاقي من خلال غرف الدردشة أو عبر البريد الإلكتروني.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

وقد وقع بعض شباب مستخدمي (الإنترنت) ضحايا لهذه المشاكل بشكل أسهل من غيرهم. وبالتالي، فإن المعلومات التالية قد تساعدك على ملاحظتهم حيث أنهم غالبًا ما يظهرون بالسمات التالية:



- عدم معرفتهم بالآداب الحاسوبية.
- السعي الحثيث لجذب الانتباه أو العاطفة.
- التمرد.
- العزلة أو الوحدة.
- الفضول.
- الارتباك فيما يتعلق بالهوية الجنسية.
- يسهل خداعه من البالغين.
- الافتتان بالثقافات التي تبعد عن عالم والديه.

كيف يمكن مسح البيانات من (الكمبيوتر) القديم تمامًا

يقوم الناس في الوقت الحالي باستبدال أجهزة (الكمبيوتر) المحمولة أو المكتبية الخاصة بهم كل ثلاث أو أربع سنوات. وللأسف، فإن الكثيرين لا يعرفون كيفية التخلص من أجهزتهم القديمة بشكل سليم .

هل تعلم أنه حتى إذا قمت بالفعل بحذف جميع الملفات الموجودة في (الكمبيوتر) القديم، فإن الآخرين قد يجدوا وسيلة لاستعادة البيانات من القرص الصلب؟

اتبع ثلاث خطوات بسيطة لمحو البيانات بشكل دائم من (الكمبيوتر):

1. أولاً: فك جهاز (الكمبيوتر) المكتبي أو المحمول.
2. ثانيًا: أخرج القرص الصلب.
3. ثالثًا: قم بتدمير مكونات القرص الصلب بيدك.

إذا كنت تنوي التبرع بـ (الكمبيوتر) القديم أو (الكمبيوتر) المحمول إلى المدرسة، أو ترغب في بيعها للآخرين، يجب عليك شراء برمجيات التقطيع لمحو البيانات الموجودة على القرص الصلب تمامًا.

دراسة حالة (9): مُهمة تدمير البيانات الحكومية القديمة

مختصو المركز الأمني الإلكترونيّ الماليزي (CM)، والأمن الإلكترونيّ الوطنيّ تحت إشراف وزارة العلوم والتكنولوجيا والابتكار، سوف يساعدون (بيربادانان بوتراجايا) (PPJ) في تدمير أسرار الحكومة الموجودة على الأقراص الصلبة التالفة/غير المستخدمة. يُعتبر الأمن الإلكترونيّ الماليزيّ بمثابة شرطيّ (الإنترنت) للتأكد من أنه لا يمكن استرجاع المعلومات التي تم تدميرها.

ذا ستار أون لاين، 5 أبريل 2010 ،

http://thestar.com.my/metro/story.asp?file=/2010/4/5/central/5987279&sec=central

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الحوسبة السحابية

الحوسبة السحابية هي عبارة عن تقديم الخدمات الحاسوبية عبر (الإنترنت)، حيث تمكن خدمات الحوسبة السحابية كلاً من الأفراد والمؤسسات من استخدام البرامج وأجهزة (الكمبيوتر) التي يتم إدارتها من قبل طرف ثالث.

"الحوسبة السحابية هي استخدام العامة للخدمات الحاسوبية التقليدية ولكن من خلال بيئة افتراضية وبنية مرجعية يتم إنشاؤها وإتاحتها للمستخدمين من قبل مزودين معينين بدلاً من أن يعمل المستخدمون على توفير هذه الخدمات التي يحتاجونها بأنفسهم".

Chris Poelkar

إيجابيات وسلبيات الحوسبة السحابية.

إيجابيات الحوسبة السحابية

1. **المرونة:** يستطيع المستخدمون الوصول إلى المعلومات المخزنة سحابيًا في أي مكان وزمان.
2. **قلة التكلفة:** تتوفر للاستخدام الفردي وللمؤسسات بتكاليف قليلة.
3. **آلية بشكل كبير:** لا توجد حاجة لشراء برامج حديثة، كل شيء معد سلفًا وجاهز للاستخدام.
4. **خدمة سريعة:** يمكن الحصول على خدمات الحوسبة السحابية نفس اللحظة.
5. **مساحات تخزين إضافية:** يمكن زيادة المساحة التخزينية المتاحة دائمًا.

سلبيات الحوسبة السحابية

1. **الخصوصية:** يتم تخزين بياناتك وملفاتك على أجهزة تعود إلى طرف ثالث.
2. **الحماية:** هل يقوم الطرف الثالث بتوفير الحماية الكاملة لملفاتك وبياناتك؟
3. **القدرة على التحويل:** ليس من السهل الانتقال من مزود خدمة سحابي إلى آخر نظراً لأن عملية النقل هذه ستتطلب وقتًا لنقل الملفات.
4. **توقف الخدمة عن العمل:** لا يوجد خيار لتفادي توقف الخدمة عن العمل، وهذا أكثر ما يخيف أصحاب المؤسسات في حال توقف الموقع عن العمل ولو لبعض الوقت.

الحوسبة السحابية والحماية.

عادة ما يتم تخزين وتثبيت البرامج والبيانات على وحدات تخزين، وفي بيئة الحوسبة السحابية يعمل المستخدمون على البرامج والبيانات المخزنة على وحدات مشتركة في بيئة تعتمد على (الويب) بدلاً من الأجهزة المادية أو المشتركة الموجودة في مقر المستخدم، تجذب خدمات الحوسبة السحابية العديد من المؤسسات نظراً لسهولة تعميمها وقلة تكاليفها بالإضافة إلى المرونة التي تتمتع بها.

مخاطر الحوسبة السحابية (الحماية المثالية والخصوصية)

لا يمتلك مستخدمو تقنيات الحوسبة السحابية القدرة على التحكم في كيف وأين يتم الاحتفاظ ببياناتهم أو من يستطيع الوصول إلى هذه البيانات وبالتالي قد تكون عرضة لإساءة استخدامها، إن مراعاة المخاطر المتعلقة بالحماية والخصوصية عند تقديم خدمات الحوسبة السحابية وتقديم الحلول الفعالة والناجعة لهذه المشكلة تعد أمراً حاسماً لضمان نجاحها.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة (10): اختراق حسابات المشاهير على خدمة أبل السحابية

تعرض العديد من المشاهير – بما فيهم (جينيفر لورانس) الفائزة بجائزة الأوسكار – إلى ما يعتقد أنه أكبر عملية اختراق يتعرض لها مشاهير. حيث تمكن المخترقون من الاستيلاء على مئات الصور ومقاطع (الفيديو) الخاصة والعائدة لعدد كبير من المشاهير والتي تم تسريبها لاحقًا للعالم. وعلى الرغم من كون هذه الحادثة تعد الأكثر إحراجًا للضحايا إلا أن المدى الذي وصل إليه هذا الهجوم أشعل الحديث حول الخصوصية وحول الحقوق القانونية المتعلقة بالتخزين السحابي.

وقد اعترفت شركة (أبل) أن المخترقين تمكنوا من النفاذ إلى حسابات عدد من المشاهير وسرقة صورهم الشخصية ونشرها عبر (الإنترنت)، وقد ألقت شركة (أبل) باللائمة على ثغرة أمنية مكنت المخترقين من معرفة كلمات المرور الخاصة بالمشاهير وتجاوز كافة وسائل الحماية الأخرى، كما أضافت شركة (أبل) بأنها لم تجد أي دليل على وجود مشكلة كبيرة في خدمتها السحابية أو في خدمة العثور على أيفون التي تقدمهما. وعوضًا عن ذلك فإن السبب الذي أدى إلى تعرض حسابات المشاهير للاختراق هو معرفة المخترقين معلومات كافية عن هذه الحسابات مثل: اسماء المستخدمين وكلمات المرور وإجابات أسئلة الحماية التي تستخدم لمنع الوصول غير المصرح بحسب (أبل).

(Gulf News, 3 September 2014,http://gulfnews.com/arts-entertainment/celebrity/hollywood/nude-shots-taken-from-stars-accounts-says-apple-1.1379960
(Gulf News, 3 September 2014,http://gulfnews.com/arts-entertainment/celebrity/hollywood/apple-admits-hacking-of-celebrity-accounts-1.1379953)

وسائل التواصل الاجتماعي

وسائل التواصل الاجتماعي هي أدوات حاسوبية تسمح للمستخدمين لإنشاء وتبادل المعلومات والأفكار، والصور، (الفيديو) في العالم الإفتراضي. وتعرف وسائل التواصل الاجتماعي بأنها مجموعة من التطبيقات القائمة على (الإنترنت) التي تستند على نظام (WEB 2.0) والتي تسمح بإنشاء وتبادل المحتوى الذي ينشئه المستخدم.

وسائل التواصل الاجتماعي وقضايا الحماية والخصوصية

يستطيع مستخدمو وسائل التواصل الاجتماعي مشاركة بياناتهم الشخصية مع الآخرين ولكن من الممكن أن يتم إساءة استغلالها، إن مشاركة البيانات الشخصية قد تؤدي إلى اساءة استخدامها سواء بشكل متعمد أو غير متعمد، على سبيل المثال، يقوم بعض الأشخاص بمشاركة تفاصيل حساباتهم مثل الإسم الكامل والجنس ورقم الهاتف مع مستخدمي الموقع، وكمثال آخر، قد يتم استغلال المعلومات التي تتعلق بالحالة الاجتماعية أيضًا.

جذب مقدار الوصول للمعلومات الشخصية المتوفرة عبر مواقع التواصل الاجتماعي أصحاب النوايا الإجرامية الذين يسعون لاستغلالها والاستفادة منها، إن هذه التقنيات ذاتها التي تجذب المستخدمين للمشاركة فيها قد تؤدي لتعريض هذه المواقع للإصابة بالبرامج الضارة التي قد تؤدي لتعطيل الشبكة الخاصة بالمؤسسة، وقد يتم استخدام أدوات تسجيل النقرات على لوحات المفاتيح مما يؤدي لسرقة كلمات المرور. من المخاطر الشائعة والتي تترتب على استخدام مواقع التواصل الاجتماعي التصيد الموجه والهندسة الاجتماعية والاحتيال والهجمات التي تنفذ من خلال تطبيقات (الويب) لسرقة الهوية، وغالبًا ما تنجح هذه الهجمات بسبب افتراض المستخدم أنه في بيئة تواصل اجتماعي موثوقة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أنواع الحماية على (الإنترنت)

يمكن تشغيل الحماية على (الإنترنت) من خلال هذه العناصر:

الوعي الشخصي

تتبع أو تعقب ما يتركه الناس

البصمة الرقمية هي تلك المعلومات التي يتركها الشخص على (الإنترنت). وهي قد تسبب مشكلات لهؤلاء الذين قد يكونون قد أرسلوا بعض التعليقات، أو الصور، أو حكايات عن أنفسهم قد تتسم بالفكاهة، إلا أنه قد يكون لها أثر سلبي على مستقبلهم مع صاحب العمل، أو مع شريك الحياة المنتظر.

وفيما يلي بعض الخطوات التي تتيح لك مراقبة سمعتك الرقمية على (الإنترنت) والمحافظة عليها:

1. ابحث عن المعلومات التي تتعلق بك على (الإنترنت) باستخدام محركات البحث أو المواقع الاجتماعية.
2. صحح التعليقات السلبية التي لها صلة بك في الموقع أو المدونة. إن لم يمكنك التخلص منها، فأعد اجابات إذا ما سئلت عنها فيما بعد. إن كنت تمتلك موقع شخصي أو مدونة شخصية، فراجع المحتوى الذي كتبته.
3. تحل بالحكمة دائمًا في اختيار المواقع التي تنضم إليها. تأكد من أن الموقع لا يؤثر سلبيًا على سمعتك. ارفع من شأن سمعتك عن طريق المشاركة في صفحات (الويب) المهنية، أو المؤتمرات.
4. لا تقبل طلبات الصداقة من الغرباء.
5. اضبط اعدادت الخصوصية بحيث يتمكن أصدقاؤك فقط من معرفة بياناتك الشخصية.
6. لا تقم بنشر أي محتويات غير لائقة تجاه عملك أو مدرستك أو أي شخص آخر.
7. تجنب نشر الصور غير اللائقة.
8. تأكد أن كل ما تقوم بنشره يراعي حدود اللباقة العامة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

إليك تاليًا بعض النصائح لحماية خصوصية بياناتك

1. احتفظ بنسخة احتياطية

يتعين عليك الاحتفاظ بنسخة احتياطية من بياناتك السحابية على وحدة تخزين خارجية كالأقراص الصلبة وغيرها حتى تتمكن من الوصول إلى بياناتك عند ضعف الاتصال بـ (الإنترنت) أو فقدانه.

2. تجنب تخزين البيانات الحساسة

احتفظ فقط بالبيانات التي تحتاج إليها بشكل مستمر وتجنب تخزين المستندات التي تحتوي على كلمات مرور لأي حسابات أو المستندات التي تحتوي على بيانات شخصية مثل رقم بطاقة الائتمان ورقم الهوية الإماراتية وعنوان المنزل وغيرها.

إذا كان يتحتم عليك تحميل مثل هذه البيانات، تأكد من تشفيرها قبل تحميلها على حسابك السحابي.

3. استخدم الخدمات السحابية التي توفر إمكانية تشفير بياناتك

من أسهل الطرق لحماية بياناتك هو استخدام خدمة سحابية تتيح لك خاصية تشفير بياناتك عند تخزينها.

4. قم بتشفير بياناتك قبل رفعها على الخدمات السحابية.

استخدم برامج التشفير التي يمكن الحصول عليها من طرف ثالث لتشفير البيانات وحمايتها بكلمة مرور قبل تحميلها على السحابة.

5. استخدم كلمة مرور قوية بالاضافة إلى خاصية التحقق بخطوتين.

استخدم كلمة مرور قوية وفريدة وقم بتغييرها باستمرار ولا تستخدمها لحماية حساباتك الأخرى، ولإضافة المزيد من الحماية، استخدم خاصية التحقق بخطوتين عند تسجيل الدخول إذا كان مزود الخدمة يتيح هذه الميزة.

6. انتبه لتصرفاتك عبر (الإنترنت)

يعتمد أمن بياناتك على الخدمات السحابية على ما تقوم به عبر (الإنترنت)، وخاصة عند استخدام حواسيب أو وصلات (إنترنت) عامة، وفي هذه الحالة يتعين عليك عدم تخزين كلمات المرور والتأكد من تسجيل الخروج من حسابك قبل المغادرة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

مواقع شبكات التواصل الاجتماعي

تشير وسائل الإعلام الاجتماعية إلى التجمعات الاجتماعية ذات محتوى (الويب) التي تتضمن ملفات (فيديو)، وصور محتوى صوتي، بإنتاج مستخدمين أو عملاء معينين ممن لا يعملون بشكل مباشر في الموقع.

وكلما ازدادت شعبية المواقع الاجتماعية، ازدادت مخاطر استخدامها. فالقراصنة، ومرسلو رسائل البريد العشوائية، وصانعو الفيروسات، وسارقو الهويات، وغيرهم من المجرمين يتعقبون استخدام الشبكة.

تساعدك النصائح التالية في حماية نفسك أثناء استخدام مواقع التواصل الاجتماعي.

1. كن حذرًا عند نشر أي معلومات تتعلق بك.
2. لا تصدق أن الرسالة التي تصلك قد وصلتك فعلاً من المرسل الحقيقي. في حال اشتبهت في رسالة ما، تواصل مع المرسل بطريقة أخرى للتأكد من أنه هو من قام بارسال الرسالة فعلاً.
3. لا تسمح لمواقع التواصل الاجتماعي بالوصول إلى بريدك الإلكتروني. عند الانضمام لموقع تواصل اجتماعي، قد يعرض عليك منحه صلاحية الوصول إلى بريدك الإلكتروني لمساعدتك في العثور على أصدقاء محتملين، قد يقوم الموقع باستخدام هذه المعلومات لإرسال بريد إلكتروني لكافة جهات الاتصال لديك أو حتى لكل من قمت بالتراسل معهم، يتعين على مواقع التواصل الاجتماعي الإفصاح في حال رغبتهم بالقيام بهذا الأمر ولكن بعضها لا يلتزم بهذا الأمر.
4. لا تقم بالضغط على الروابط التي تؤدي إلى موقع التواصل الاجتماعي الذي تستخدمه، اعتمد كتابة العنوان مباشرة في المتصفح أو استخدم قائمة المحفوظات لديك. إذا قمت بالضغط على رابط مؤدي لهذا الموقع سواء وصلك من خلال رسالة بريد إلكتروني أو من موقع آخر فإن هناك احتمالاً بأن تكون هذه الصفحة وهمية وبالتالي قد يتم سرقة كلمة المرور بالاضافة إلى بياناتك الشخصية.
5. تعامل بحرص مع طلبات الصداقة التي تقوم بقبولها عبر مواقع التواصل الاجتماعي.
6. ضع في اعتبارك أن كل ما تنشره عبر (الإنترنت) سيبقى هناك إلى الأبد. حتى لو قمت بحذف حسابك لا يمكنك مسح الصور والفيديوهات التي تم تخزينها من قبل الموقع، علاوة على ذلك، لن يتم مسح الصور التي تم الإشارة فيها إليك.
7. توخ الحذر عند تثبيت التطبيقات التي يتم الحصول عليها من طرف ثالث. تسمح العديد من مواقع التواصل الاجتماعي للمستخدمين باستخدام تطبيقات من طرف ثالث لإضفاء المزيد على صفحاتهم الشخصية، قد يلجأ بعض المجرمين لمثل هذه التطبيقات لسرقة بياناتك الشخصية.
8. فكر مرتين قبل استخدام مواقع التواصل الاجتماعي في العمل.
9. ثقف أفراد أسرتك حول مواقع التواصل الاجتماعي.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الحسابات المالية على (الإنترنت)

قد تسهل عليك الصفقات المالية على (الإنترنت) حياتك أو تسبب لك المشكلات إذا لم تتوخ المزيد من المحاذير.

افعل	لا تفعل
تغيير كلمة المرور بصفة دورية للحيلولة دون سرقة المعرف.	إعطاء رقم تعريف الهوية الشخصي أو كلمة المرور لآخرين أو تبادلها معهم.
التأكد من التعامل مع الموقع الصحيح. كتابة محدد مواقع (الويب) (URL) في محدد مواقع المتصفح أو الإشارة المرجعية للصفحة.	إعطاء معلومات مثل: رقم تعريف الهوية الشخصي، إرسال كلمة المرور أو بيانات الحساب عبر البريد الإلكتروني أو عبر الهاتف إلى آخرين.
تحديث المتصفح حين خروج إصدارات جديدة لأنها غالبًا تتضمن سمات تأمين جديدة.	النقر على أي رابط في البريد الإلكتروني لإتمام المعاملات المصرفية أو المالية.
التحقق دائمًا من التخزين المؤقت عند تسجيل الخروج للحيلولة دون قيام آخرين بالدخول على المعلومات الشخصية أو الأنشطة على (الإنترنت).	المواصلة مع أي معاملة إذا ما كان البريد الإلكتروني يبدو مريبًا.

التكنولوجيا

مضادات الفيروسات

لا تثبت إلا برامج مضادات الفيروسات الجيدة التي اشتريتها مباشرة من بائعين ثقات أو وكلائهم. فهناك حالات باع فيها البائعون برامج تروجان متنكرة في البرامج المضادة للفيروسات، ولذلك اختر البائعين الذين يمكن التحقق منهم والوثوق بهم.

في كل يوم تظهر فيروسات جديدة على (الإنترنت). ومن المهم بالنسبة لك أن تنزل التحديثات الخاصة بالبرنامج المضاد للفيروسات الذي لديك لضمان تضمنه لآخر بيانات تعريف الفيروسات.

الحماية من برامج التجسس

يمكن استخدام برامج الحماية من برامج التجسس لتعقب وإزالة برامج التجسس الموجودة بالفعل على (الكمبيوتر) الخاص بك. يمكنك ضبط جدول الكشف عن هذه البرامج شهريًا، أو أسبوعيًا، أو يوميًا. كما سيتيح لك هذا البرنامج قائمة بجميع المخاطر الموجودة، ويسمح لك باختيار ما تريد حذفه وما تريد الإبقاء عليه.

الجدار الناري

تحظى بعض أنظمة التشغيل بجدر حماية داخلية التي يفترض أن تحول دون مخاطر (الإنترنت). وينبغي عليك أن تترك هذه السمة مفعلة إلى أن تستبدلها ببرنامج أو جهاز خارجي. فإن جدر الحماية تمنع الأخطار الصادرة والواردة على السواء.

تحكم الآباء

تحكم الآباء عبارة عن برنامج يصفي صفحات (الويب) التي لا تناسب الأطفال. وهذا البرنامج يعد أحد "الأبواب الأمامية" الرئيسة على (الإنترنت) لحماية الأطفال. ولا تتوقف مزايا هذا البرنامج على تحديد أيام وساعات استخدام (الإنترنت)، بل إنه يتيح لك معرفة ما إذا كان الطفل يتواصل باستمرار مع شخص ما من خلال حسابه/حسابها على شبكة التواصل الاجتماعي.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أمان المتصفح

لقد أصبح (الإنترنت) هو الوسيلة الرئيسية للحصول على المعلومات. ومن ثم، فمن المهم تهيئة كل متصفح مثبت بشكل مناسب حتى لا تكون هناك ثغرات تسمح بالتطفل.

وهذا مفيد إذا ما كان (الكمبيوتر) الخاص بك مثبت عليه أكثر من متصفح (للإنترنت). يمكنك استخدام متصفح لتصفح الأنشطة الحساسة مثل: الخدمات المصرفية على (الإنترنت) أو التسوق عبر (الإنترنت)، بينما يمكن استخدام متصفح آخر للأغراض العامة. والغرض من ذلك هو الحد من احتمال قيام موقع ضار أو (تروجان) سيء بسرقة معلومات الهامة خلال قيامك بتصفح (الويب).

التحديث التلقائي

لضمان أمان (الكمبيوتر) الخاص بك، فأنت بحاجة لتثبيت التحديثات الجديدة. وهذه التحديثات ستقوم بتصحيح الأخطاء وتحسن من وظيفية أنظمة التشغيل، ومضادات الفيروسات، وبرامج الأمان الأخرى التي لديك.

النسخ الاحتياطي

هناك عدة حالات قد تتسبب في فقدك للمعلومات التي على (الكمبيوتر) الخاص بك، منها الاستخدام السيئ، أو ضياع (الكمبيوتر)، أو تلف الجهاز بسبب كوارث طبيعية مثل: البرق والفيضانات. ومع ذلك، فيمكنك إجراء نسخ احتياطي للملفات الخاصة بك لأجل استعادة معلوماتك في حالة وقوع حادث غير متوقع.

وإن أفضل وسيلة لنسخ ما على حاسوبك احتياطيًا هو تخزين معلوماتك على أجهزة خارجية، مثل: (Thumb Drive) أو جهاز أقراص (CD) أو (DVD)، أو تحميل نسخ احتياطية على (الإنترنت).

وفيما يلي بعض الاقتراحات حول أنواع الملفات التي قد تحتاج إلى نسخها احتياطيًا:

- السجلات المصرفية والمعلومات المالية الأخرى.
- الصور الرقمية.
- البرامج والملفات الموسيقية التي اشتريتها أو قمت بتحميلها من (الإنترنت).
- المشروعات الشخصية.
- عناوين البريد الإلكتروني، ودفتر العناوين، والتقويم.
- الإشارات المرجعية (للإنترنت).

بروتوكولات الحماية المستخدمة في تأمين الشبكات اللاسلكية

عند استخدامك للشبكات اللاسلكية فإنك تقوم بارسال البيانات من جهازك عبر نقطة وصول ومن ثم عبر (الإنترنت) إلى خادم ما. يكمن الضعف في هذا الاتصال ما بين جهازك ونقطة الوصول، وبالتالي يستطيع أي شخص ضمن مدى شبكتك اللاسلكية وباستخدام برامج معينة التلصص على حركة البيانات من بين جهازك ونقطة الوصول.

هناك نوعان شائعان من (بروتوكولات) الحماية التي تستخدم حاليًا وهما

(Wi-Fi Protected Access) (WPA or WPA2).
(Wired Equivalent Privacy) (WEP).

عند ضبط إعدادات نقطة الاتصال لديك يتعين عليك استخدام البروتوكول (WPA) أو (WPA2) لنقل البيانات بين جهازك ونقطة الاتصال، تجنب استخدام البروتوكول (WEP) نظرًا لتدني مستوى الحماية التي يقدمها.

للأسف لا يمكن تحديد (البروتوكول) المستخدم في الحماية من قبل المستخدمين وإنما من قبل صاحب نقطة الوصول.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الأخطاء الشائعة	تجنب	افعل
• تعطيل خاصية عرض اسم الشبكة يخفيها ويحميها من المستخدمين غير المصرحين. • اعتماد التصفية بناء على عناوين (MAC) يمنع المستخدمين غير المصرح لهم من الاتصال بشبكتك. • خفض مستوى الإشارة من الراوتر أو وضعه في مكان بحيث لا تخرج الإشارة خارج حدود المنزل أو المؤسسة. • ايقاف (DHCP) أو استخدام عناوين (IP) ثابتة يعد طريقة لمنع الوصول غير المصرح به. • تشفير اسم الشبكة أو تغييره باستمرار يزيد من مستوى حماية شبكتك اللاسلكية.	• لا تترك الشبكة اللاسلكية غير محمية. • لا تستخدم بروتوكول (WEP). • لا تشارك كلمات المرور مع الغير.	• أطفئ جهاز الراوتر اللاسلكي في حال عدم استخدام الشبكة. • استخدم (البروتوكولات) (WPA) أو (WPA2) لحماية شبكتك اللاسلكية. • قم بتقييد الوصول إلى شبكتك اللاسلكية (استخدم كلمة مرور قوية وعطل خيارات الإدارة عن بعد أو من خلال الاتصال اللاسلكي). • فعل خاصية التسجيل على جهاز الراوتر اللاسلكي لديك.

تنفيذ السياسات الخاصة بالموارد المشتركة

الموارد المشتركة تشير إلى الأجهزة أو المعلومات على (الكمبيوتر) التي يمكن الوصول إليها من حواسيب أخرى عبر شبكة داخلية أو عبر (الإنترنت). وقد تكون ملفات، أو طابعات، أو ماسحات ضوئية أو أشياء أخرى. وعادة ما تكون الموارد المشتركة محمية بجدر الحماية من خارج الشبكات الداخلية أو (الإنترنت). وقد تصبح الموارد المشتركة التزام أمان إذا ما وصل إليها متطفل أو فيروس.

وفيما يلي قائمة ببعض المواقف التي قد يتم من خلالها اختراق البيانات أثناء استخدام الموارد المشتركة:

1. ترك المستخدمين حساباتهم مفتوحة بدون متابعة. ولذلك احرص دائمًا على إغلاق الحساب بعد استخدامه.
2. السماح للمستخدمين بالدخول على الشبكة بأكملها.
3. دخول المستخدمين على مواقع غير جديرة بالثقة وتصبح الشبكة بأكملها عرضة للإصابة بالفيروسات. حاجة مسؤولي الشبكات لفرض سياسات للحيلولة دون حدوث ذلك.

أفضل الممارسات فيما يتعلق بالموارد المشتركة

في أي مؤسسة، يمثل تنفيذ أفضل الممارسات أهمية لإدارة الموارد المشتركة. هناك العديد من الخطوات التي يمكن للمؤسسة أن تنتهجها:

1. تقييد الوصول.

- فحص المستخدمين من خلال الإطلاع على سيرهم الذاتية، أو ملفات التعريف الشخصية أو شخصياتهم.
- الهدف من هذه الخطوة هو التأكد من وصول المستخدمين المناسبين فقط إلى الموارد المشتركة.
- تقييد توافر المجلدات المشتركة لمستخدمين محددين. يمكنك ضبط حقوق الوصول على التحكم الكامل، أو القراءة والتغيير أو القراءة فقط.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

2. إدارة كلمة المرور والحساب. تأكد من استعمال المستخدمين لكلمات المرور. تعيين موقع في الشبكة يمكن الوصول إليه من قِبَل المستخدمين ذوي الصلة.
3. التدريب على وعي أمن المعلومات. توفير التدريب للمستخدمين حول كيفية حدوث سرقة المعلومات، والآثار المترتبة عليها وكيفية الوقاية منها.
4. المراقبات والمراجعة. إنشاء السجل في ملف الموارد المشتركة مثل: سجل الطابعة. تأكد من قيام المستخدمين بتسجيل الخروج من حساباتهم أثناء تناولهم للغداء أو عندما يكونوا خارج المكتب. والهدف من هذا هو ضمان عدم دخول مستخدمين آخرين إلى الحسابات الخاصة بهم في حالة عدم وجودهم قريبين.
5. النسخ الاحتياطي والاستعادة. يجب دائمًا عمل نسخ احتياطية للبيانات الهامة من الموارد المشتركة. في حالة وجود أخطاء أو أعطال في الموارد المشتركة، فيمكن بسهولة استعادتها على الفور. من أجل ضمان استمرارية عمل المؤسسة بشكل سلس دون أي انقطاع.

استخدام كلمة مرور جيدة

كلمة المرور هي كلمة أو خيط من الحروف السرية تستخدم للمصادقة لإثبات هوية أي شخص والوصول إلى الموارد. في هذه الأيام، تستخدم معظم الأنظمة كلمات المرور باعتبارها الحماية الأساسية لهذه الأنظمة، وهناك آخرون يستخدمون وسائل أكثر تعقيدًا مثل البطاقات الذكية، وأنظمة المقياس الحيوية، ...إلخ.

يستمد معظم الأشخاص كلمات المرور الخاصة بهم من معلوماتهم الشخصية. ولسوء الحظ، لا يعد هذا استخدامًا جيدًا لأن المتطفلين يمكنهم تعقب كلمات المرور هذه بسهولة.

نصائح: اختيار كلمة سر جيدة

- استخدام مزيج من الحروف القوية لتكون كلمة السر. استخدم على الأقل (8) حروف من خلال الدمج بين الحروف الصغيرة، والحروف الكبيرة والأرقام والرموز
- قم بخلط الحروف الكبيرة مع الحروف الصغيرة والأرقام واكتب الكلمات التي تختارها بهجاء خاطئ.
- استخدم الكلمات التي يصعب تخمينها. استخدام كلمات من قاموس لغتك الأم.
- تجنب ترتيب الحروف على لوحة المفاتيح مثل: "ضصثقفغ" أو "123456" والمعلومات الشخصية مثل: تاريخ الميلاد وأرقام بطاقات الهُوية.
- قم بتغيير كلمة السر بصورة دوريّة، ويفضل كل شهرين.
- لا تقم بمشاركة كلمة السر الخاصة بك مع شخص آخر.
- الأكثر أهمية هو تذكر كلمة المرور الخاصة بك.

الحماية من تهديدات (الإنترنت)

هناك العديد من الطرق لحماية نفسك من تهديدات شبكة (الإنترنت). نُركّز هنا على اثنين:

- من خلال ممارسة الممارسات الذاتية بطريقة جيدة.
- من خلال نشر أفضل الممارسات في مجال تنمية المواهب.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

شاشتك

- إذا كنت ستمضي بعيدًا عن جهاز (الكمبيوتر) الخاص بك، قم بإغلاق الغطاء أو شغّل شاشة التوقف.
- تأكد من حمايته بكلمة سر تمكّنك من العودة إلى الشاشة الرئيسة.

كن مسئولاً وواعيًا

- أنت مسئول عما يحدث على جهاز (الكمبيوتر) الخاص بك وبحسابك.
- تعرَّف على السياسة الأمنية (سياسة الاستخدام المقبول).

اختيار كلمة السر

- قم بخلط الحروف الكبيرة مع الحروف الصغيرة والأرقام واكتب الكلمات التي تختارها بهجاء خاطئ.
- لا تكتبها على ورق.
- لا تقم بمشاركة كلمة السر الخاصة بك مع أي شخص آخر.
- لا تعتمد على كلمة سر واحدة لكل شيء في حالة وجود خرق.

تصفح بحكمة

- تصفح وكأن هناك أشخاصًا آخرين يراقبونك.
- توخ الحذر حول توفير المعلومات الشخصية في مواقع (الويب). كل ذلك مسجل.
- كل ضغطة على البريد الإلكترونيّ، كل تراسل الفوري وكل شيء يمكن القيام به على الشبكة أو في البريد الإلكترونيّ يتم تسجيله في مكان ما.

ممارسة الوصول الآمن

- كن حذرًا عند فتح أي مرفقات خاصة ببريدك الإلكترونيّ. ينطبق ذلك بصفة خاصة إذا كنت لا تعرف المرسل، ولكن حتى لو فعلت ذلك، فمن الممكن للبرمجيات الخبيثة أن تستخدم عنوان بريد إلكتروني وهمي أو حتى تسرق بيانات عنوان البريد الإلكترونيّ من جهاز (الكمبيوتر) وإرسالها من دون معرفة المالك.

حماية هُويتك

- لا ترد أو تنقر على وصلات في أي رسالة تطلب معلومات شخصية أو مالية.
- راقب أموالك. راجع بياناتك الائتمانية الخاصة بك بشكل لا يقل عن ربع سنوي.
- لا تحمل البرامج من الشركات التي لا تعرفها.
- قم بحماية جهاز (الكمبيوتر) الخاص بك. امنع النوافذ المنبثقة.

اعمل نسخ احتياطية من البيانات

- قم بعمل نسخ احتياطية للبيانات على الأقراص، والأقراص الصلبة الخارجية، ومحركات الأقراص أو الخادم.
- قم بإنشاء جدول.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أفضل الممارسات في مجال تنمية المواهب من أجل السلامة الإلكترونيّة

تـم تأسـيس مركـز عمليـات التشـغيل الإلكترونيـة للتميـز التابـع لجامعـة الخليفـة بالتعـاون مـع شـركة (كاسـيديان) و(إيميراجـي) للأنظمـة ذات المسـئولية المحـدودة. والهـدف مـن ذلـك هـو تطويـر الخبـرة فـي مجـال عمليـات التشـغيل الإلكترونيـة، وعلـى وجـه الخصـوص التعامـل مـع المسـائل الأمنيـة والمخاطـر التـي تواجههـا بشـكل متزايـد البنـى التحتيـة القوميـة، وأنظمـة التحكـم الصناعيـة، والبنـى التحتيـة للمعلومـات الهامـة.

يعـد هـذا المركـز مركـزًا متخصصًـا فـي المسـائل الأمنية المتعلقـة بالشـبكات والمجـالات القابلـة للحركة، بالإضافـة إلـى مجـالات التشـفير، والمناظـرات الرقمية، وأمـن الأجهـزة المضمنة.

تأسسـت جامعـة خليفـة فـي فبرايـر مـن عـام 2007م، لبنـاء الاقتصـاد القائـم علـى المعرفـة وهـذا مـن شـأنه أن يسـاهم بشـكل فعـال فـي تنميـة دولـة الإمـارات.

الأنشطة

النشاط رقم (1): إنشاء كلمة مرور قوية لموقع (الويب)

الموقع: (http://www.passwordmeter.com).

The Password Meter

Test Your Password		Minimum Requirements
Password:	•••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	57%	
Complexity:	Good	

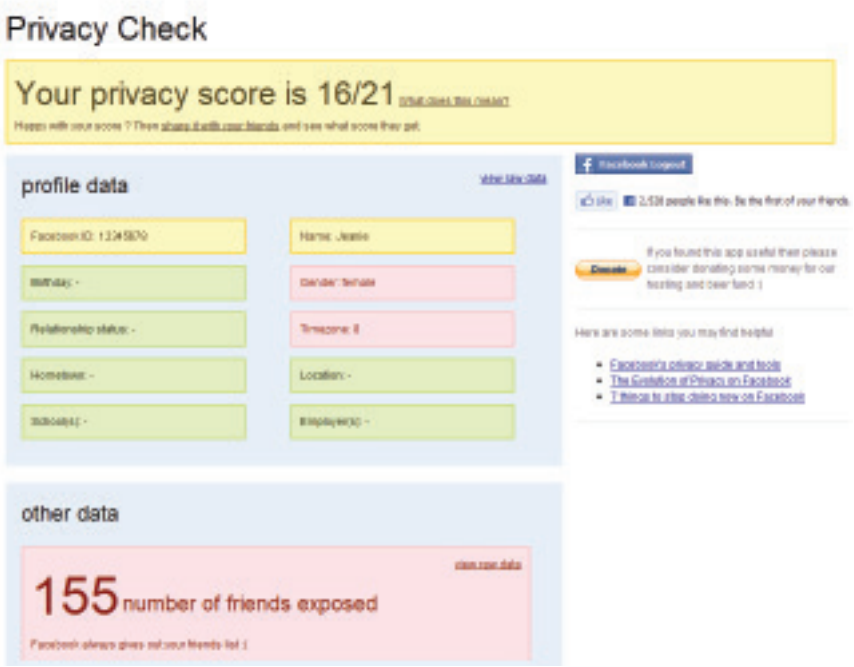
Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 14
Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 4
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
Requirements	Flat	+(n*2)	4	+ 8
Deductions				

النشاط رقم (2): فحص خصوصية موقع (ويب) (فيسبوك) الخاص بك

الموقع: (http://www.rabidgremlin.com/fbprivacy).

مصدر الوصف على النحو التالي: (http://www.f-secure.com/weblog).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة



ما المراد بذلك؟

يعد هذا أحد مصادر الخصوصية البالغ عددها (21) مصدرًا.

إذا كان مربع النقاط الخاص بك باللون الأخضر فقد أحرزت (21/21)، وبالتالي تختفي كافة المعلومات الخاصة بك من مواقع (الويب) وعن العامة. ممتاز.

وإذا كان مربع النقاط الخاص بك باللون الأصفر، فقد قمت بتأمين معظم المعلومات الخاصة بك. البرامج الجيدة.

إذا كان مربع النقاط الخاص بك باللون الأحمر، تكون الكثير من معلوماتك الخاصة معروضة، ويتعين عليك على الفور مراجعة إعدادات خصوصية ال(فيسبوك) الخاصة بك.

ملاحظة: لأن الـ (فيسبوك) لا يسمح لك بإخفاء كافة المعلومات الخاصة بك، بالتالي لا يمكنك إحراز نقاط أفضل من بين النقاط البالغة (21). من خلال تأمين كل شيء، فإن أفضل النقاط التي يمكن تحقيقها هي (15/21) (ما لم تقم بملء معلومات الملف التعريفي الخاص بك، مثل نوعك، الأشياء التي تفضلها، أو عدم وجود أي أصدقاء لديك، وبالتالي يمكنك إحراز نقاط أكثر)!

الأنشطة

النشاط رقم (3): البحث عن المعلومات الخاصة بك باستخدام محرك البحث

هل البصمة الرقمية الخاصة بك بصمة نظيفة؟ يمكنك اكتشاف ذلك من خلال البحث عن المعلومات الشخصية الخاصة بك باستخدام محركات البحث الشائعة:

- (جوجل): (http://www.google.com).
- الـ (فيسبوك) (http://www.facebook.com).
- (ياهوو) (http://www.yahoo.com).
- (آسك) (http://www.ask.com).
- (بينج) (http://bing.com).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تمرين

1. **وجد مسؤول النظام أن أحدًا ما قام بشكل غير قانوني بتغيير السجلات الموجودة على ملقم المدرسة خلال فترة عطلة نهاية الأسبوع. ما هي أكثر الأسباب المحتملة التي تمكن شخص ما من الوصول بسهولة إلى ملقم المدرسة؟**

   أ. الملقم مازال يعمل خلال فترة عطلة نهاية الأسبوع.

   ب. غفل مسئول النظام عن عمل مسح للوقاية من الفيروسات.

   ج. الملقم محمي بواسطة كلمة مرور يسهل تخمينها.

   د. لم يقم مسؤول النظام بعمل تحديث لتصحيحات الأمان بشكل منتظم.

2. **قام أحد القراصنة بسرقة معلومات بطاقة الائتمان الخاصة بك. ما هما الشيئان اللذان يجب البحث عنهما؟ (اختر إجابتين).**

   أ. خطاب من المصرف الخاص بك يعرض فيه زيادة الحد الائتماني الخاص بك.

   ب. زيادة واضحة في حجم البريد الإلكتروني العشوائي الذي تستلمه.

   ج. اتصالات غير مطلوبة من بائعين على رقم الهاتف المنزلي الخاص بك.

   د. معاملات تجارية بالباقة الائتمانية في منطقة مختلفة من البلد.

   هـ. اتصال هاتفي من المصرف الخاص بك يتساءل عن أحدث أنشطة حسابية لك.

3. **ما هو أفضل مكان لإجراء المعاملات المصرفية عبر (الإنترنت)؟**

   أ. في المنزل.

   ب. جهاز كمبيوتر المكتبة.

   ج. المقهي الإلكتروني.

   د. غرفة (الإنترنت) في المطار.

4. **لماذا يتعين عليك فحص الملفات التي تم تنزيلها قبل فتحها؟**

   أ. للتحقق من كفاءة برنامج الفيروسات الخاصة بك.

   ب. للكشف عن وجود برامج ضارة قد تدمر البيانات الخاصة بك.

   ج. لضمان دقة المعلومات المضمنة في هذه الملفات.

   د. لتقييم ما إذا كان محتوى الملف يتطابق مع المحتوى الذي يشير إليه اسم الملف.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

5. **تلاحظ وجود عدد من أصدقاء المدرسة يتابعون (الفيديو) هات والموسيقى بشكل مستمر، مما يعمل على إبطاء سرعة (الإنترنت). ما هي أفضل الحلول الفعالة لمنع مثل هذه الحالة؟**

أ. تثبيت برنامج ترشيح لإغلاق مواقع (الويب).

ب. وضع لافتة تمنع المتابعة المستمرة (للفيديو) والموسيقى.

ج. إعلام المدرس بالمشكلة دون ذكر أية أسماء.

د. إرسال بريد إلكتروني إلى الأصدقاء تحذرهم من التداعيات.

الإجابة: 1. ج ، 2. ب، 3. أ، 4. ب، 5. ج

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

05 التفاعل والتعاون الإلكترونيّ

تلقي هذه الوحدة الضوء على تبادل ومشاركة المعلومات باستخدام الأنظمة أو الأدوات الرقمية. وهي تحتوي على أهمية الاتسام بالتواضع والولاء والاحترام تجاه الآخرين أثناء التواصل معهم.

فعند استخدام الأدوات الرقمية بالشكل الصحيح، فإنها يمكن أن تدعم تحقيق الوحدة. ففي بعض المجتمعات، يعد توجيه الرسائل النصية ورسائل البريد الإلكتروني بدون فحص درجة موثوقيتها ومصدرها أمرًا غير مقبول من الناحية الاجتماعية.

وتهدف هذه الوحدة إلى تعليم مستخدمي (الإنترنت) المسؤولين كيف يمكن أن يصبحوا مفكرين رائعين فيما يتعلق بتحليل مصادر المعلومات وتقييم مدى التأثير على الآخرين. الهدف من هذه الوحدة هو مساعدتك في اتخاذ القرارات الأخلاقية أثناء التواجد على (الإنترنت).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أهداف التعلُّم

أهداف هذه الوحدة هي:

- التعرف على مفاهيم متعلقة بالأشكال المختلفة للاتصال والتعاون الرقمي المعاصر.
- تمييز النوايا (من خلال الأسباب الجيدة والسيئة) فيما يتعلق باستخدام أدوات الاتصال والتعاون الرقمي المتنوعة.
- القيام بممارسات أخلاقية عند تبادل ومشاركة المعلومات عبر أنظمة الشبكات.
- إدراك أهمية تبعات السلوكيات على (الإنترنت).

نواتج التعلُّم

في نهاية هذه الوحدة، سوف تكون قادرًا على:

- وصف الإستخدامات المناسبة للأدوات الرقمية.
- عرض السلوكيات الأخلاقية وغير الأخلاقية عند مشاركة المعلومات عبر الشبكات
- شرح عواقب السلوك عبر (الإنترنت) وتأثيراتها على الواقع.
- إستخدام الشبكات الاجتماعية لتطوير فرق العمل ومهارات التعاون.
- تقييم تأثير إستراتيجيات وسائل الإعلام الاجتماعية.

قائمة المراجعة

التعليمات:

بعد الانتهاء من قراءة هذه الوحدة، يُرجى إكمال الاستبيان باستخدام المقياس التالي:

المقياس:

1. ليس لدي أدنى معرفة.
2. لدي معرفة محدودة.
3. على دراية وقادر على التوضيح الجيّد.
4. ذو كفاءة وإمكانية على الممارسة الكاملة.

البنود	التحصيل العلمي	قبل	بعد
1	يمكنني أن أذكر على الأقل ثلاث (3) أدوات لوسائط حديثة.		
2	أدرك متى وكيفية استخدام مواقع الشبكات الاجتماعية لأغراض حسنة.		
3	يمكنني تعريف ثلاثة (3) تداعيات لانتهاك الموارد المشتركة.		
4	يمكنني توضيح تبعات إرسال رسائل نصية أثناء القيادة.		

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

كيف غيَّرت التكنولوجيا الجديدة طريقة تواصلنا مع بعضنا البعض

هل تدرك أن التقنيات الحديثة قد غيرت الطريقة التي نتواصل بها اليوم؟ فقط انظر حولك.

لقد غيرت الهواتف المحمولة، والبريد الإلكتروني، ومواقع التواصل الاجتماعي وما تلك إلا أمثلة قليلة الطريقة التي نتواصل بها. لقد خلقت تقنيات شبكات التواصل الاجتماعي تلك هياكل اجتماعية جديدة لمن وتوقيت وكيفية ونوعية التفاعل الحادث بين الأفراد والمجموعات.

واليوم، من السهل الحصول على الأجهزة الرقمية الحديثة وتعلم كيفية استخدامها في لمح البصر. ويمكنك استخدام هذه الأجهزة في مواقف الحافلات، وفي المقاهي، وفي المكتبات، وفي المدارس، والكليات، وأماكن العمل، والمستشفيات، وتقريبًا في أي مكان، وفي أي وقت. لكن كيف تدرك أنك لا تسيء استخدام تلك الأجهزة؟ كيف يمكن أن تتحقق من أنك تدرك كيفية تشغيل هذه الأجهزة بالشكل الملائم، والأهم من ذلك، بطريقة أخلاقية؟

فهم التفاعل والتعاون الإلكتروني

إن التفاعل الإلكتروني والذي يشار إليه باللغة الإنجليزية باسم (e-Interaction) عبارة عن اتصال عبر (الإنترنت) بين شخص وآخر عبر التقنيات الرقمية، مثل البريد الإلكتروني، أو المنتديات، أو صفحات (البلوج).

أما التعاون الإلكتروني والذي يشار إليه باللغة الإنجليزية باسم (e-Collaboration) عبارة عن الإجراء المتعلق بالعمل معًا ومشاركة الأفكار والمعلومات باستخدام التقنيات المتاحة عبر (الإنترنت). فهو يوضح كيف يمكن استخدام التقنيات من تفعيل الاتصالات الفعالة والقيمة بين الأشخاص والمعلومات. وفي الاقتصاد العالمي، الذي يعتمد على الخدمات بشكل متزايد، تعد المعلومات أصلاً هامًا للغاية، ويعد التعاون هو المحرك الذي يخلق القيمة من هذا الأصل.

التعرف على العديد من أشكال أدوات الاتصال والتعاون الرقمية

البريد الإلكترونيّ

البريد الإلكتروني، والذي يشار إليه باللغة الإنجليزية باسم (email)، ما هو إلا مثل الخطابات، ولكنه لا يختلف إلا في كونه يتم تبادله بطريقة مختلفة. وعندما نرسل الخطابات التي نضع الطوابع عليها عبر مكاتب البريد، يتطلب الأمر عدة أيام للوصول إلى المتلقين، أما البريد الإلكتروني فينتقل إلكترونيًا خلال ثوانٍ. وتستخدم أجهزة (الكمبيوتر) مجموعة مكونات (بروتوكول) (TCP/IP) لإرسال رسائل البريد الإلكتروني في شكل حزم. على سبيل المثال: بريد (ياهو)، و(هوت ميل)، و(جي ميل).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

قواعد البريد الإلكتروني

إليك بعض الأوامر والنواهي التي يجب مراعاتها عند كتابة البريد الإلكتروني.

افعل	لا تفعل
قم بملاحظة الهجاء الخاص بك – فربما أدى ذلك إلى توصيل رسالة مختلفة في مجملها.	استخدام الكلمات التي لا تفهمها.
استخدم قواعد لغوية قصيرة ومبسطة.	تجاهل علامات الترقيم الخاص بك.
استخدم الفقرات القصيرة والبارعة.	كتابة جميع الأحرف كبيرة ما لم تكن في حالة الاحتفال – فمن الصعوبة بمكان القراءة والمراجعة أثناء الصياح.
استخدم علامات التعجب للمساعدة في نقل الحماسة إلى البريد الإلكتروني.	استخدم الاختصارات على سبيل المثال: (LOL، LMAO،... إلخ) إذا كنت متأكد أن المستلم سيفهم هذه الاختصارات.

مواقع شبكة التواصل الاجتماعي

موقع شبكة التواصل الاجتماعي هو موقع (ويب) يستطيع الأفراد من خلاله إنشاء ملف تعريف عبر موقع الشبكة الاجتماعية هو عبارة عن موقع (ويب) يمكن للأشخاص من خلاله إعداد ملف تعريف على (الإنترنت) يوضح اهتماماتهم مع وجود إمكانية الارتباط بملفات التعريف الأخرى. وبشكل عام، يكون لدى المستخدمين القدرة على نشر المعلومات التي تشتمل على الصور، ومقاطع (الفيديو)، وإدخالات صفحات (البلوج).

من أمثلة مواقع الشبكات الاجتماعية الشهيرة:

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المدونات

بشكل أساسي، صفحة (البلوج) ليست مثل الصحيفة أو الجريدة على (الإنترنت). فيمكن أن يتحدث المؤلف عن أي شيء وعن كل شيء. والعديد من صفحات (البلوج) مليئة بالارتباطات الممتعة التي يقوم المؤلف بوضعها. وغالبًا ما تحتوي صفحات (البلوج) على قصص أو مختصرات من المعلومات الممتعة للمؤلف.

وعلى الرغم من أن صفحات (البلوج) يمكن أن تكون حرة تمامًا، إلا أن الكثير من صفحات (البلوج) تركز على شيء واحد. على سبيل المثال: إذا كان المدون يهتم بالتقنيات، فيمكن أن يتوجه المدون إلى معرض إلكترونيات المستهلكين ويعرض إدخالات للأشياء التي يراها هناك. وإذا كان المدون يهتم بمرض معين، فيمكن أن ينشر المقالات والأبحاث الجديدة المتعلقة بهذا المرض. وإذا كان المدون مهتمًا بالأمور الاقتصادية، فيمكن أن ينشر ارتباطات إلى مقالات تناقش الأمور الاقتصادية، ثم يقوم بعمل تعليقات عليها.

كما يستخدم بعض المدونين صفحات (البلوج) الخاصة بهم كسجلات للقصاصات الخاصة بهم، وهو أحد أشكال الذاكرة المتاحة عبر (الإنترنت). عندما يجد المؤلف ارتباطًا أو مختصرات للمعلومات يرغب في تذكرها، يقوم بنشرها في صفحة (البلوج). حتى إذا لم يطلع عليها أي شخص آخر، فإنها تفيد المؤلف لأن (البلوج) عبارة عن وسيطة إلكترونية يمكن البحث فيها ويمكن للمؤلف الوصول إليها من خلال مستعرض (ويب) في أي مكان في العالم.

منتديات (الإنترنت)

مثل مجموعات النقاش المعتادة وجهًا لوجه، يعتبر المنتدى المتاح عبر (الإنترنت) مكانًا يمكن للمشاركين (المستخدمين) من ذوي الاهتمامات المشتركة تبادل الرسائل المفتوحة في العالم الافتراضي.

الرسائل الفورية

ومن أشكال الاتصال الرقمي الشائعة إرسال الرسائل الفورية، وفيها يتبادل شخصان أو أكثر الرسائل المكتوبة على الفور على (الإنترنت). يمكن أيضًا من خلال برامج إرسال الرسائل الفورية الأكثر تقدمًا الخاصة بالعملاء التواصل باستخدام نماذج أكثر تقدمًا مثل الصوت الحي أو الاتصال.

مواقع التواصل الاجتماعي في التعليم

إن التعاون والمشاركة والطبيعة المنفتحة لشبكات التواصل الاجتماعي تشكل عددًا من الفرص للتعلم والابتكار. تساعد أدوات الشبكات الاجتماعية في التمهيد للممارسات التعليمية المبتكرة والفريدة التي تركز على التعاون وتبادل المعلومات. وخلافًا للتكنولوجيات الموجودة في السابق، تساعد مواقع التواصل الاجتماعي على كسر حواجز الزمان والمكان والتسلسل الهرمي المعلوماتي لتمكين التفاعل في الوقت الحقيقي وتبادل المعلومات على نطاق أوسع وبشكل أكثر تأثيرًا واستهدافًا. (مدرسة دبي الحكومية، 2013م).

إن مثل هذه الخصائص تساهم في جعل مواقع التواصل الاجتماعي أداة تعليمية ذكية تساعد في التغلب على بعض التحديات التي تواجه المؤسسات التعليمية في المنطقة العربية. وقد أدي استخدام مواقع التواصل الاجتماعي في البيئة التعليمية إلى بروز تحديات في وجه الطلاب والمعلمين وأولياء الأمور.

وعلى الصعيد الأكاديمي يستطيع العديد من طلبة الكليات في الجامعات العربية والعالمية استخدام شبكات التواصل الاجتماعي للتواصل مع زملائهم من الطلاب في سبيل إنشاء بيئة تعليمية جاذبة ذات شفافية حيث يلعب الطلاب دورهم في تولي المسؤولية وليس مجرد البقاء كمتلقي للمعلومات التي يتم تدريسها من قبل المعلمين في القاعات الدراسية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

ميزات استخدام مواقع التواصل الاجتماعي في التعليم

- الدمج بين التعليم الفردي والجماعي
- تطوير الإجراءات التعليمية من تلقي المعلومة من خلال التدريس إلى التعلم من خلال بناء بيئة تعلم ذاتية.
- يبرز التعاون والتفاعل في العملية التعليمية من خلال مواقع التواصل الاجتماعي من خلال النقاشات والحوارات التي يتم عقدها.
- تكمن القوة في تحفيز الطلاب وتشجيعهم على الاشتراك في العملية التعليمية.
- تحقيق الشفافية بين الطلبة.
- تتميز مواقع التواصل الاجتماعية بإمكانية التعامل مع المشاكل الذاتية، والتي تعد واحدة من أهم نقاط مناهج التعلم الذاتي والتي تعتمد على الانتاج والإبداع والحوار والتعاون.
- تسهيل المشاريع الدارسية بين الطلاب أنفسهم، وبينهم وبين معلميهم.
- استخدام الوسائل المعروفة من قبل غالبية الطلاب.
- تفعيل مبدأ النقاش والحوار لتحفيز التفكير الإبداعي.
- تحفيز مهارات الطلاب من خلال استخدام الحوافز التعليمية.

تطبيقات التواصل الاجتماعي التعليمية

1. (Twiducate):

موقع تواصل اجتماعي تعليمي بالإضافة إلى كونه موقعًا مجانيًا، يحفز هذا الموقع التعاون والمشاركة بين الطلاب والمعلمين، حيث يمكن المعلمين من إنشاء مجموعات منفصلة واستخدام رموز لهذه المجموعات بدلاً من استخدام عنوان البريد الإلكتروني، كما يعطي المعلمين الصلاحيات الكاملة والقدرة على التحكم في المجموعات المشتركين فيها، ومراقبة كل ما يتم نشره عن طريق الأعضاء.

2. (TweenTribune):

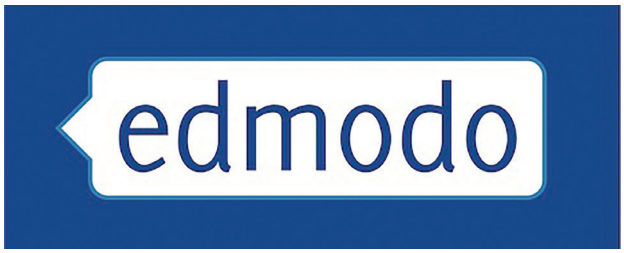
يوفر هذا الموقع أخبارًا يومية للأطفال سواء كانوا من مستويات أكاديمية مختلفة أو مراحل عمرية مختلفة، يتم اختيار الأخبار والمقالات التعليمية من قبل مجلس تحرير يتضمن مراسلين محترفين ومتخصصين في شؤون الأطفال والمراهقين، كما يستطيع الأطفال التعليق على هذه المواضيع تحت إشراف وموافقة معلميهم قبل نشر هذه التعليقات. كما يمكن هذا الموقع الأطفال والمراهقين من انتاج ما يقارب (99%) من محتويات الموقع كوسيلة لإشراكهم في هذه العملية، سجل هذا الموقع مشاركة ما يزيد على (100) ألف معلم.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

3. (Coursera):

تعتبر منصة (كورسيرا) واحدة من أشهر منصات التعلم عن بُعد، حيث تقدم آلاف الدورات التدريبية عبر (الإنترنت) كما توفر المنصة (17) درجة عبر (الإنترنت) وما يقرب من عشرين برنامجًا يمنح شهادات في مختلف المجالات.

4. (Edmodo):



موقع تواصل اجتماعي للاستخدام التعليمي اعتمادًا على تقنيات الجيل الثاني من (الويب) يدمج ما بين منصات (فيسبوك) و(بلاك بورد). يتولى المعلم فيه السيطرة من خلال التواصل مع الطلاب باستخدام مساحة مفتوحة لتبادل النصوص والرسائل الصوتية ومناقشة المواضيع ذات الصلة بالأمور التي يتم دراستها.

5. (Twitter):

أحد أشهر مواقع التواصل الاجتماعي التي تستخدم للأغراض التعليمية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

القضايا الأخلاقية والقانونية المتعلقة باستخدام مواقع التواصل الاجتماعي

عند استخدام مواقع التواصل الاجتماعي يتعين عليك أن تتأكد من أن تبني سيرتك البحثية بشكل صحيح، إن الأساس للقيام بمثل هذا الأمر يتمثل في تذكر أن القوانين والسياسات والقواعد الاجتماعية التي تنطبق على حياتنا الحقيقية تنطبق كذلك على حياتنا على (الإنترنت).

إن المواد التي يتم نشرها عبر (الإنترنت) محمية بحقوق للنشر فلا يحق لك نسخ عمل الآخرين (كالأفكار والصور والبيانات وغيرها) أو نشرها عبر (الإنترنت)، كما يجب عليك تعريف الآخرين بما يمكنهم وما لايمكنهم فعله من أعمالك التي تنشرها عبر (الإنترنت)، اتخذ من عملية استعراض الشروط والأحكام للمواقع التي تقوم بنشر مؤلفاتك الفكرية (كالأفكار والصور والبيانات وغيرها عليها عادة لك، لا يزال الكثير من الناس يعتقدون أن بإمكانهم فعل ما يحلو لهم بالمواد التي يتم نشرها عبر (الإنترنت).

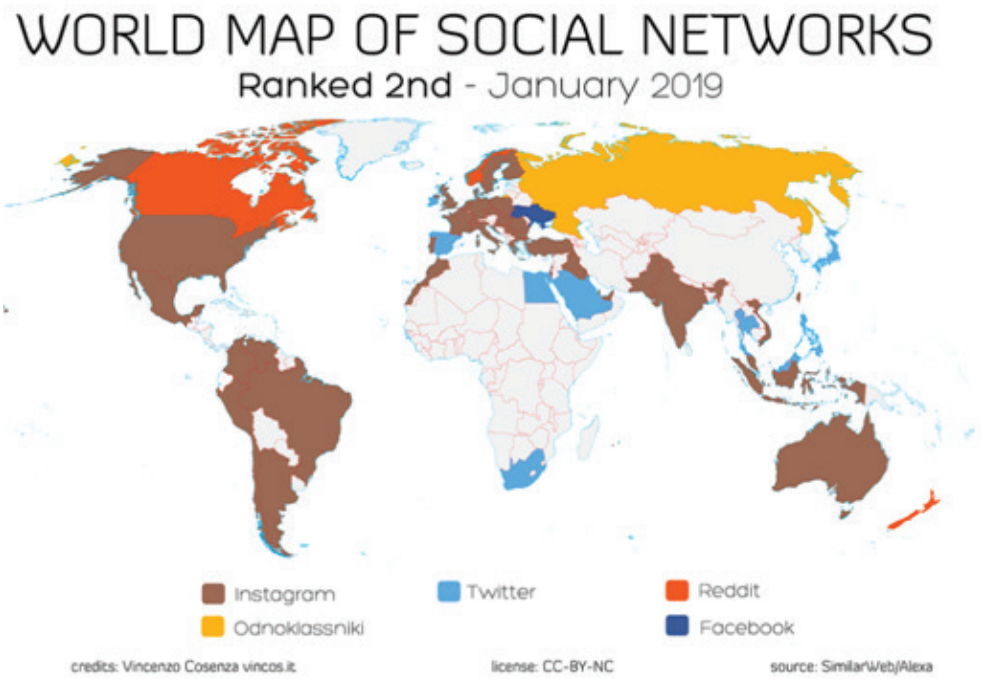
عند قيامك بالتسجيل في موقع تواصل اجتماعي فإنك توافق بهذا على شروطهم واحكامهم، تأكد من قراءة الشروط والأحكام حتى تعرف ما الذي يستطيع القائمون على الموقع فعله بالمحتويات التي تقوم بنشرها بالإضافة إلى بياناتك الشخصية.

قانون الجرائم الإلكترونيَّة في دولة الإمارات العربيَّة المتحدة

بحسب نص المادة رقم (20): يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم أو خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من سب الغير أو أسند إليه واقعة من شأنها أن تجعله محلاً للعقاب أو الازدراء من قبل الآخرين، وذلك باستخدام شبكة معلوماتية، أو وسيلة تقنية معلومات.

الحقائق والأرقام

الخريطة العالمية لشبكات التواصل الاجتماعي



حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

استخدام أدوات التواصل والتعاون الرقمي بشكل ملائم وأخلاقي

عندما تتواجد في عالم افتراضي، قد لا يبدو من الضروري أن تتصرف بشكل ملائم، ربما لأنك في الغالب لا تعرف الأشخاص الذين تتواصل معهم. ومن المذهل أنه هناك بعض الأشخاص ممن يتصرفون بشكل مختلف أثناء التواجد على (الإنترنت) لأنهم يمكنهم الاختباء خلف اسم مستخدم والبقاء مجهولين.

ولكن، مهما اختلفت الوسيطة التي تستخدمها للتواصل، من الضروري أن تتصرف بشكل يتسم بالأدب على (الإنترنت) تمامًا كما هو الحال عندما تتصرف وجهًا لوجه.

لكن كيف تدرك أنك تتصرف بشكل ملائم أثناء التواجد على (الإنترنت)؟

التواصل بشكل ملائم أثناء التواجد عبر (الإنترنت)

لا يهم ما إذا كنت تتواصل عبر (الإنترنت) أو وجهًا لوجه، فالأمر برمته يتوقف على الشعور العام. والمبدأ الرئيس الذي تسير عليه هو "أن تعامل الآخرين بنفس الطريقة التي ترغب أن يعاملوك بها". ما يلي بعض المقترحات حول كيفية التواصل عبر (الإنترنت):

1. **استخدام اللغة المناسبة**

اليوم، يفضل الكثيرون استخدام الاختصارات، خصوصًا بين أوساط الشباب. ومن المقبول استخدام تلك الاختصارات أثناء الحديث مع الأصدقاء الذين يمكنهم فهم تلك اللغة. ولكن لا يفهم الجميع ما تشير إليه هذه الاختصارات، وبالتالي، يمكن أن يؤدي ذلك إلى خلق حالة من الارتباك. ويمكن أن ينتهي بك المطاف بمضايقة الناس، لمجرد أنهم لا يستطيعون فهم ما تقوله.

2. **تعامل مع الناس كما لو كنت تتعامل معهم وجهًا لوجه**

كما ذكرنا من قبل، من الضروري التعامل مع الآخرين بنفس الطريقة التي ترغب أن يعاملوك بها، وبالتالي فإنه من الضروري أن تتصرف بشكل جيد وأن تتحلى بالأدب عند التحدث إلى الأشخاص عبر (الإنترنت) أو عند نشر التعليقات الخاصة بك. فقد تجرح أحاسيسهم، فاحذر ذلك.

3. **إذا كنت لا تجد شيئًا جيدًا لتقوله، فلا تقل شيئًا**

لا يمكن أن يجبرك أحد على الموافقة على فكرة شخص آخر. إذا لم تكن توافق، فلا تقم بنشر التعليقات السيئة. إذا كان يتوجب عليك التعليق، أو إذا فرض عليك الحديث، فيجب أن تتحدث بطريقة تتسم بالأدب والرقة.

4. **من المقبول ألا توافق، إلا أنه يجب أن توفر المبررات**

لا يمكن أن تكون الآراء خاطئة أو حمقاء. وبالتالي، إذا كان هناك شخص له رأي آخر حيال أمر ما، فلا ترده في وجهه. فقط أخبره برأيك وقم بتوضيح أسبابك بشكل محترم.

5. **لا تشجع وقوع الشجارات في حالة استشعار حدوث تلك الشجارات**

إذا رأيت شخصًا ما ينشر تعليقات مسيئة عن شخص آخر، فأخبر الشخص المسؤول. وإذا لم يكن هناك شخص مسئول، فاطلب من هذا الشخص التوقف عن نشر التعليقات المسيئة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

استخدام أدوات الشبكات الاجتماعية لأسباب جيدة

"إذا أدركنا الطريقة التي يمكن أن تفيد بها الشبكات الاجتماعية، تكون لدينا الفرصة لتحقيق أشياء لم نتمكن من تحقيقها لأنفسنا من قبل. فالعالم الذي اعتدنا أن يكون عالمًا خطيًا، حيث يجب أن نصعد فيه درج السلم لنرتقي في التصنيف، وحيث الصفوف التي تنتظر الموارد المحدودة، أصبح هذا العالم الآن مكونًا من شبكات شاسعة وتتسم بالمرونة، بعضها فضفاض والبعض الآخر صارم. فشبكاتنا الاجتماعية، سواء تلك ذات الطراز القديم في الحياة الواقعية، أو تلك الحديثة التي يتم إنشاؤها من خلال برامج التواصل الاجتماعي، توفر لنا القدرة على القيام بأشياء رائعة لأنفسنا وللآخرين".

كريس بروجان، مؤلف كتاب Trust Agents and Social Media Expert

إن التأثير في مواقع شبكات التواصل الاجتماعي الشائعة لهو مثال كبير على الاستخدام الفعال والسريع للتكنولوجيا في الأغراض الجيدة. فلنقرأ الدراسات التالية من أجل فهم الأمر بطريقة أفضل.

تقرير: يعد الـ (فيسبوك) بمثابة الصديق الذي يجمع جامعات دبي من خلال الوسائط الاجتماعية

تمكنت جامعات دبي من العثور على مواقع شبكات اجتماعية تساعدها بشكل كبير في الوصول إلى الطلاب المتوقعين. كان كل من موقعي (فيسبوك) و(تويتر) مسئولين عن التحاق على الأقل (5%) إلى (20%) بالعديد من الجامعات، ومن المتوقع أن يزيد هذا الرقم على مدار السنوات. أثبت (فيسبوك) على وجه الخصوص بأنه أكثر فاعلية لأنه وفر المجتمع الذي يمكن من خلاله أن يظل الطلاب المحتملون والحاليون على اتصال. تلعب الوسائط الاجتماعية في الوقت الحالي دورًا هامًا للجامعات من خلال تسويق برامجها. ويعد الـ (فيسبوك) أيضًا أكثر الوسائل فاعلية وأرخصها للوصول إلى الطلاب مقارنة بالوسائط المطبوعة.

The National, 25 September, 2010 http://www.thenational.ae/news/uae-news/education/face-book-proves-friend-for-dubai-universitiesrecruiting-through-social-media

تبادل ومشاركة المعلومات عبر أنظمة الشبكات بشكل يتسم بالأخلاقية

الموارد المشتركة مقابل الموارد المخصصة

فيما يتعلق بأجهزة (الكمبيوتر)، تشير الموارد المشتركة إلى الأجهزة أو المعلومات المتاحة على جهاز (كمبيوتر) والتي يمكن الوصول إليها من أجهزة (كمبيوتر) أخرى عبر الشبكات المحلية أو عبر شبكة (الإنترنت). وبمعنى آخر، يمكن مشاركتها أو الوصول إليها من قبل الكثير من الأشخاص، على سبيل المثال، الوصول إلى المجلدات، والملفات، والملحقات (الطابعات، والماسحات، والملقمات)، ورسائل البريد الإلكتروني، وغير ذلك.

واليوم، لا يعني مشاركة الموارد مشاركة الملحقات المادية فقط، بل يشير ذلك أيضًا إلى الموارد المتاحة على شبكة تشتمل على المهارات والمواهب والخبرات والوصول والأموال.

ومن عدة أوجه، يعتبر السماح لك بالوصول إلى الموارد المشتركة في المدرسة، أو الحرم الجامعي، أو المجموعة، أو المنظمة، ميزة هامة. وفي المقابل، يتوقع منك إظهار أعلى درجات الاحترام لحقوق الآخرين أثناء استخدامهم لتلك الموارد.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الموارد المشتركة	الموارد المخصصة
تطوير الموارد بشكل مشترك باستخدام منصات مثل: (wikis).	طباعة الأوراق غير المحدودة باستخدام طابعة.
إنشاء شبكة في شركة لتوصيل الأعضاء والموارد.	متصلة بشكل مباشر بجهاز (الكمبيوتر) الدفتري الخاص بك.
إنشاء مجلد خاص لفصلك، بحيث يمكن لكل الأعضاء في الفصل الدراسي مشاركة الملفات.	طباعة المهام من خلال طابعة محلية في معمل أجهزة (الكمبيوتر) في المدرسة.
طباعة المهام من خلال طابعة الشبكة في معمل أجهزة (الكمبيوتر) في المدرسة.	تخزين الصور من نشاط للفصل في مجلد شخصي .
تخزين الصور من نشاط للفصل في مجلد عام.	استخدام وسائل التعريف الحيوية للدخول إلى المنشأة.
استخدام طرف عام في المكتبة للوصول إلى شبكة (الإنترنت).	
إنشاء مورد على (الإنترنت) لمجتمع مدرسة.	
استخدام موارد المدرسة المتاحة على (الإنترنت) إلى أقصى حد مخصص.	
استخدام شبكة المدرسة لإتمام مشروع مجموعة للفصل.	

على الجانب الآخر، هناك الموارد المخصصة، وهي أداة موجودة على جهاز (الكمبيوتر) ترتبط بجهاز واحد فقط، ولا يمكن الوصول إليها إلى من خلال شخص واحد فقط في نفس الوقت.

ما يلي بعض نماذج أو (سيناريوهات) التطبيقات الأخلاقية للاستفادة من الموارد المشتركة أو الموارد المخصصة:

فيما يلي بعض الأمثلة أو (السيناريوهات) للسلوك غير الأخلاقيّ عند الاستفادة من الموارد المشتركة:

1. تحميل البرامج المقرصنة.
2. طباعة العديد من الملفات الشخصية.
3. تخزين الملفات التي لا علاقة لها بالعمل مثل: ملفات الصور الشخصية ضمن ملفات التخزين المشتركة.
4. تنزيل الملفات الكبيرة غير الضرورية أثناء ساعات الدراسة.
5. إرسال بريد إلكترونيّ لشخص آخر.

تداعيات انتهاك استخدام الموارد المشتركة

تعتبر إساءة استخدام الموارد المشتركة مشكلة خطيرة لأن التبعات لا تؤثر فقط على شخص واحد، ولكن تؤثر على كل المستخدمين على الشبكة. عند مشاركة الموارد، يجب أن تحد من استخدامك حتى يتمكن الآخرون الموجودون على نفس الشبكة من استخدامها هم أيضًا. إذا خرج عدد الاستخدامات من قبل عدد قليل من المستخدمين عن السيطرة، تعيد الموارد المشتركة رسائل خطأ، ثم، في النهاية، لا يمكن الوصول إلى تلك الموارد بأي شكل من الأشكال.

فيما يلي بعض عواقب سوء استخدام الموارد المشتركة:

1. الانتهاكات الأمنية.
2. يمكن أن يحدث ازدحام أو إشغال شامل لعرض النطاق الترددي.
3. زيادة مستوى قرصنة البرامج.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

احترام الآخرين عند استخدام الهواتف المحمولة

اليوم، أصبحت الهواتف المحمولة منتشرة في كل مكان! ويمكنك استخدام هاتفك المحمول بشكل عملي في أي مكان وفي أي وقت. لقد أدت سهولة استخدام الهواتف المحمولة إلى نقص عام في الوعي فيما يتعلق باستخدام الهواتف المحمولة بشكل ملائم. وفي حين أن الهواتف يمكن أن تساعد على زيادة الإنتاجية وتحسين نوعية الحياة الخاصة بنا، إلا أنها خلقت أيضًا بيئة من نغمات الرنين التي لا يمكن تجنبها، أو الأشخاص الذين يتحدثون بصوت مرتفع للغاية، أو الأشخاص الذين لديهم عادات سيئة فيما يتعلق بالهواتف المحمولة. واليوم، يعد من المشاهد المعتادة رؤية الأشخاص يتحدثون في الهواتف المحمولة في دور السينما، والمستشفيات، وحتى أثناء القيادة.

لذلك، كيف لنا أن نضع حدودًا لهذا؟ فيما يلي قائمة تضم (43) سلوك خاصة بالهاتف المحمول:

1. الالتزام بحالات حظر الهواتف المحمولة

هناك أسباب لفرض بعض الأماكن المحددة للقواعد فيما يتعلق بإغلاق الهواتف المحمولة. ويجب الالتزام بهذه القواعد بكل بساطة. استخدم الوضع الصامت أو وضع الاهتزاز إذا كنت ترغب في الاستمرار في حالة اتصال. يمكنك دائمًا فحص البريد الصوتي، أو الرسائل النصية، أو الرد على الخدمات فيما بعد. وإذا كان من الضروري لك إجراء المكالمات أو تلقيها، فاترك المنطقة كلها. استخدام الشعور العام، وعندما تشعر بالشك، اترك الهاتف المحمول جانبًا بكل بساطة.

2. تحدث بصوت منخفض، وليس بصوت مرتفع

هل لاحظت مطلقًا أنك تميل إلى الحديث أو الكلام بصوت أعلى أثناء الحديث على الهاتف؟ لا، يجب ألا تصرخ بصوت مرتفع كي لا يتمكن الآخرون من سماعك. لقد تم تصميم الهواتف المحمولة لإجراء المحادثات بمستويات صوت عادية، لذا، يجب الإبقاء على صوتك منخفضًا وهادئًا من خلال توجيه وجهك لأسفل قليلاً تجاه صدرك. وبكل جدية، إذا لم تكن متأكدًا حيال هل تتكلم بصوت مرتفع أم لا، فقط راقب الناس بالقرب منك وحولك حتى ترى ردود أفعالهم .

3. ابتعد عن الآخرين الموجودين حولك

هناك قاعدة غير متفق عليها وهي أن كل شخص يكون محاطًا بمساحة شخصية خاصة به. لذا، احترم تلك المساحة من خلال الحديث بعيدًا عن الآخرين، لنقل (5) أمتار على الأقل من أقرب شخص منك. وبالطبع، إذا لم تكن هناك مساحة فاصلة أو خاصة متاحة لإجراء الاتصال الخاص بك، فتحدث بصوت منخفض.

4. حافظ على خصوصية مكالماتك الخاصة

وعند الرد على الهاتف، لا تقم برفع صوتك ونشر المحادثة للعالم كله، إلا إذا كان ذلك أمرًا ضروريًا. فلا يوجد أي شخص آخر يرغب في الاستماع إلى المحادثة الخاصة بك. وبالإضافة إلى ذلك، لا يوجد ما هو أسوأ من معرفة أن الأشخاص الموجودين حولك يستمعون إلى الأمور السرية الخاصة بك، سواء فيما يتعلق بالأعمال التجارية أو الأمور الشخصية، فمن شأن ذلك أن يعرض حياتك أو مستقبل الأعمال التجارية الخاصة بشركتك للخطر.

5. احترم قواعد استخدام كاميرات الهواتف

حسنًا، من الرائع للغاية أن تمتلك هاتف مزود بكاميرا. ومع ذلك، يمكن أن يصبح امتلاك هاتف مزود بكاميرا مشكلة كبيرة في حالة إساءة استخدام الهاتف. احترم خصوصية الآخرين ولا تقم بالتقاط الصور للآخرين بدون الحصول على إذن. فأنت لا تعرف أين ينتهي الأمر بتلك الصور.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الرد على الهواتف المحمولة في المواقع "غير الملائمة"

يجب أن تكون مستخدمًا مسؤولاً للهواتف المحمولة من خلال مراعاة شعور الآخرين. ولسوء الحظ، لا تكون تلك هي الحالة في الكثير من المواقف. فالكثيرون لا يظهرون إلا أقل القليل من الاحترام لحالات حظر استخدام الهواتف في دور السينما، أو المطاعم، أو حتى أثناء القيادة. ألا تسبب المقاطعات الناجمة عن الهواتف المحمولة مضايقات، أثناء مشاهدة الأفلام في دور السينما؟

هناك بعض الأماكن التي يعتبر تلقي الاتصالات الهاتفية أو صدور أصوات نغمات الرنين فيها أمرًا غير مقبول:

- الأماكن الدينية أو أماكن العبادة مثل: المساجد والمعابد والكنائس.
- المكتبات.
- المتاحف.
- المستشفيات.
- دور السينما ودور العرض.
- أي نوع من الاحتفالات الخاصة مثل: الجنازات، ومراسم قبل الدفن والأعراس.
- أي نوع من أنواع الأعمال الرسمية مثل: المؤتمرات والاجتماعات.

تحديد إساءة استخدام التكنولوجيا

استخدام مواقع الشبكات الاجتماعية لأسباب خاطئة

دراسة حالة (11): تتناول محكمة دبي أول قضية تشهير عبر الـ (فيسبوك)

دبي – جرت المحاكمة الأولى التي تتناول إساءة استخدام الـ (فيسبوك) في الأعمال غير المشروعة بعد اعتراف شريك تجاري بتحميل عدة صور لموظف لديه ونشر تعليق تشهيري تحت كل صورة منها.

وفقًا للمدّعى عليه، فقد كان لديه شراكة مع شقيق الموظف لديه في مطعم ووجد هذا الموظف يسرق المال من الصراف. "لقد اعتاد على إخبار الزبائن أنه باع المطعم ولم يعد له علاقة له بعد اليوم. لقد استفزني تصرفه هذا، ولذلك نشرت تعليق على الـ (فيسبوك)" نقلاً عن شخص يبلغ من العمر (26) عام.

لقد أظهرت السجلات أن المدعى عليه متهم من قِبَل المدعي الذي استجوبه. أجل القاضي المحاكمة حتى يحضر محامي المدعى عليه دفاعه.

أخبار الخليج، 18 نوفمبر 2009 ،

http://gulfnews.com/news/gulf/uae/crime/dubai-court-gets-first-facebook-libel-case-1.528875

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة (12): قانون المدارس ضد الطلاب الذين يعملون على "إشعال الكراهية في المدونات ضد المعلمين

لقد تم عقاب خمس طالبات في المدارس الإعدادية لقيامهن بنشر تصريحات مسيئة عن اثنين من المدرسين، ونائب مدير المدرسة على (الإنترنت). كان على الفتيات إزالة تلك التصريحات من المدونة وتم إيقافهن لمدة ثلاثة أيام.

هذه الحوادث في تزايد بالتوازي مع زيادة عدد المدونين. ووفقًا للمحامين، يمكن رفع دعوى ضد الطلاب بتهمة التشهير طالما كان هناك من يستطيع التعرف على المعلم من البيان التشهيريّ المعلَن على (الإنترنت). المعلمون لديهم أسباب قانونية للمحاكمة إذا كانوا يرغبون في القيام بذلك.

احترام الآخرين عند استخدام الهواتف المحمولة

تعريض سلامتك للخطر عند إرسال رسائل نصية أثناء القيادة

تقرير: هناك (20,000) انتهاك لاستخدام الهاتف المحمول أثناء القيادة

أبوظبي – وفقًا لما قاله مهندس الكباري، حسين أحمد الحرثي، مدير المرور ودورية الشركة في أبوظبي في تصريح له إلى مجلة الأمن (999)، يجب على كل شخص احترام قواعد وتنظيمات المرور. وأضاف أيضًا، يتعين على كل شخص عدم استخدام الهاتف المحمول أثناء القيادة فربما تقع حادثة في أقل من ثانية أثناء حديث أحدهم في الهاتف.

وأشار إلى أن الحديث في الهاتف المحمول دون استخدام سماعات الرأس أثناء القيادة من الأخطاء الشائعة التي يقترفها السائقين. فهذا من شأنه أن يؤدي إلى وقوع حوادث مرورية وارتباك مروري، ومن ثم يؤدي إلى الازدحام المروري. ففي العام الماضي وحده، وقع ما يزيد على (2,000) حالة انتهاك من هذا النوع.

ووفقًا لنتائج الدراسات المتخصصة، يؤدي استخدام الهاتف المحمول أثناء القيادة إلى قليل قدرة السائق على التركيز والتفاعل بمقدار ثلاثة أضعاف. أي منتهك يستخدم الهاتف المحمول دون وضع سماعة الرأس أثناء القيادة سيتم تغريمه(800)درهم إماراتي، وخصم أربع نقاط في سجل السائق لدى المرور.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة (13): أب حزين يتوسل بشكل عاطفي إلى السائقين

تُوفي أحد لاعبي كرة القدم الدوليين في حادثة عندما اصطدمت سيارته بشاحنة ثابتة. ووفقًا لكلام صديقه الذي كان يقود خلفه، أكد أن نجم الكرة لم يفرمل قبل اصطدامه بالشاحنة. وهذا من شأنه، بالإضافة إلى الشواهد التي تدل على عدم وجود علامة انزلاق على الطريق، أن تجعل الشرطة ووالد نجم الكرة بأن اللاعب لم يشاهد الطريق ولكنه كان يرسل رسائل من هاتفه المحمول عند وقوع الحادثة. حث الأب كافة السائقين على عدم استخدام هواتفهم المحمولة أو الأجهزة الرقمية الأخرى أثناء القيادة.

ما رأي سكان دولة الإمارات حول إرسال الرسائل النصية أثناء القيادة؟

في الإمارات، نجد أن غالبية السائقين لا يستطيعون إرسال رسائل نصية أو الرد على العروض والإعلانات المغرية من محطة الراديو المفضلة لديهم أثناء السفر. في العام 2008م، أجرى "حديث المدينة" التابع لموقع (GulfNews.com) استطلاعًا مع بعض المقيمين في دولة الإمارات، حول إذا ما قاموا بإرسال رسائل نصيَّة إلى مسابقات الراديو أثناء القيادة من قبل أم لا، وما آراؤهم واعتقاداتهم حيال عواقب هذا الأمر.

لاحظت وجود العديد من مستمعي برامج الراديو ممن يرسلون رسائل نصية ويتحدثون إلى البرامج، وأنا أسأل نفسي كيف يشعر هؤلاء بالأمان؟ لا بد من التركيز على الطريق، ومن عدم المسؤولية المشاركة في إرسال رسائل نصية أثناء القيادة. أحيانًا عند توقف السيارة في إشارة مرور وأنت في حالة وقوف، فربما يكون استخدام الهاتف حينئذ آمنًا، وعلى الرغم من ذلك، فقد يؤدي هذا إلى تشتيت ذهنك وذهن السائقين من حولك."

على خليل قاسم، عامل بالخطوط الجوية

"لم أعر اهتمامي يومًا من الأيام بإرسال الرسائل النصية لأنني أعرف مدى خطورتها. إنه من الصعوبة بمكان بالقدر الكافي أن تقود وتتحدث في الهاتف لأن التركيز على الطريق حينئذ سيكون عُرضة للخطر، هذا بالإضافة إلى أن إرسال الرسائل يؤدي بالفعل إلى صرف عينك عن الطريق وهذا هو الخطر الحقيقي لكافة مستخدمي الطريق. أعتقد أن من عدم المسؤولية من جهة مقدمي الراديو أن يطلبوا تعليقات السائقين أو أن يقرأوها دون الإشارة إلى إرشادات السلامة الأساسية كإرشاد إلى كافة مستخدمي الطريق."

إبراهيم محمد القويض، وكيل تأجير سيارات

"اعتدت أن أرسل رسائل نصية وبالكاد نجوت من العديد من الحوادث. لذلك توقفت عن إرسال الرسائل أثناء القيادة. والآن، وعندما أشاهد الآخرين يقودون سياراتهم ويلعبون بهواتفهم المحمولة أشعر بالارتياب لأن ما يفعلونه على الطريق يعد بالفعل أخطاء حمقاء. اعتدنا على وجود حملة قوية مناهضة للسائقين الذين يستخدمون هواتفهم المحمولة، لكن هذا الأمر لم يعد ذا أهمية بعد الآن، ولا تفعل الشرطة أي شيء. "يجب إعادة طرح الحملة المناهضة للهواتف المحمولة."

فادي غانم، مدير

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

استخدام الهواتف المحمولة للغش في الامتحانات

دراسة حالة (14): جامعة أبوظبي تطرد (34) طالبًا بسبب الغش

تسببت سياسات صارمة للنزاهة الأكاديمية في طرد (34) طالبًا من جامعة أبوظبي (ADU) للغش والتلاعب. تم إجراء ما يقرب من (510) تحقيقًا بسبب انتهاك قانون الجامعة الأكاديميّ داخل المجتمع الطلابي والذي يتكون من أكثر من (4,000) طالبًا.

تم ضبط الطلاب المفصولين متلبسين في حالة غش أثناء الامتحان مستخدمين ورقة غش أو السماح لطلاب آخرين بأداء الامتحان نيابة عنهم. استخدم طلاب آخرون سماعة أذن للسماح للأشخاص الموجودين خارج غرفة الامتحان بتلقينهم الإجابات. هناك أيضًا بعض الطلاب المستبعدين نتيجة إرسال شهادة مزورة لنظام اختبار اللغة الإنجليزية الدولية (IELTS) متضمنة نتائج مزيفة.

Gulf News, 27 December, 2010, http://gulfnews.com/news/gulf/uae/education/university-cracks-whip-on-cheating-1.736433

استخدام الحاسب الآلي الخارجيّ لاقتحام نظام المدرسة

دراسة حالة (15): تم إلقاء القبض على طالب لاستخدامه الحاسوب في أعمال القرصنة في المدرسة

تم اعتقال طالب يبلغ من العمر (17) سنة في مدرسة خاصة في دبي بسبب اختراق جهاز الكمبيوتر في المدرسة والحصول على البيانات الخاصة به عن طريق جهاز كمبيوتر خارجيّ. قام أيضًا بتوزيع أوراق الامتحان على الطلاب الآخرين. بعد حوادث كثيرة من هذا القبيل، تمكنت المَدرسة من معرفة المزيد عن التسريبات وأبلغت الشرطة.

http://gulfnews.com/news/gulf/uae/crime/dubai-police-arrest-student-for-hacking-into-computer-and-stealing-

تشغيل الألعاب الإلكترونيّة على الطائرات

دراسة حالة (16): تشير الدراسة إلى أن الركاب يخاطرون بالسلامة بتجاهل قواعد الطيران.

وهذا وَضْع مقلق حيث أن العديد والمزيد من شركات الطيران تعتمد على نظام تحديد المواقع للتأكد الدقة.

يقول العلماء والمسؤولون الحكوميون أن الأجهزة التي تعمل بالبطاريات بما في ذلك الهواتف المحمولة وأجهزة (الكمبيوتر) المحمولة والألعاب (خاصة تلك التي ترسل إشارات لاسلكية) قد تعطل نظام ملاحة الطائرة.

وفقًا للدكتور (مورغان جرانجر) من جامعة (كارنيجي ميلون)، فقد اكتشف الكثير من التداخل في نظام الأقمار الصناعية العالمية لتحديد المواقع (GPS) عندما أجرى الناس مكالمات هاتفية أثناء الإقلاع والهبوط "هناك العديد من النماذج التي توضح التدخل الخطير" وفقًا لما قاله الدكتور (جرانجر).

"لا توجد أية حوادث لا يمكن السيطرة عليها، ومع ذلك، ومع تزايد استخدام الهواتف اللاسلكية بشكل أكثر على الطائرات، أعتقد أنها مسألة وقت حتى نبدأ في المعاناة من مشكلات حقيقية."

أخبار الإمارات العربية المتحدة: أخبار ليلية، 3 يناير 2006 ، http://www.msnbc.msn.com/id/11627970

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

نشر الخدع عبر الرسائل النصية ورسائل البريد الإلكترونيّ

دراسة حالة (17): خروج القطار عن مساره في مترو دبي ليست سوى إشاعة

انتشر خبر خروج عربات قطار مترو دبي عن مسارها بالقرب من محطة "الراشدية" عبر الهواتف المحمولة. أشارت الإشاعة إلى وقوع (15) ضحية و (22) إصابة خطيرة بالإضافة إلى تلف عدد كبير من السيارات.

أضاف (برهام) أن الأخبار التي تواترت عن انهيار مترو دبي هي أخبار مغلوطة، موضحًا أن الهواتف المحمولة ساعدت في سرعة نشر الإشاعة دون التحقق من مصدرها أو صحة المعلومات الواردة. يتعين على السلطات أن تتعامل مع الإشاعات بأسلوب منظم لتقليل أثرها والسيطرة عليها.

أكد (بيمان يونس براهام)، مدير التسويق والاتصالات المؤسسية، وهيئة الطرق والنقل أن الهيئة ستتعاون مع الشرطة لمقاضاة مروجي الشائعات. هناك إجراءات صارمة سيتم اتخاذها للحد من الشائعات التي تهدد مصلحة البلاد.

أعلن المدير التنفيذي لهيئة السكك الحديدية بهيئة الطرق والنقل، المهندس عبد الله ماجد الخاجي أن سقوط مترو دبي مجرد إشاعة لا يمكن حدوثها. وهذا لأن سياسة السلطات تطبق السلامة على طرق المترو، وتلتزم بمعايير السلامة للقاطرات وفقًا لممارسات السلامة البريطانية والأمريكية والأوروبية. تشتمل السياسة أيضًا على المعايير القومية الخاصة بالوقاية من الحرائق وتقييم المخاطر.

وأضاف عبد الله، في حالة حدوث أي شيء، فإن المترو أعد بالفعل خطة طوارئ لضمان سلامة وراحة المسافرين. تتم مراقبة رحلات القطارات بشكل مستمر من خلال كاميرات أمامية وخلفية عن طريق العاملين بأمن المحطات والقطارات ممن تلقوا تدريبًا للتعامل مع المواقف الطارئة. علاوة على أن القطارات أيضًا مجهزة بأنظمة لاسلكية تربط القطار بخدمات الطوارئ من أجل توفير الاستجابة الفورية أثناء الحوادث.

أضاف الخاجي أن قطارات المترو التي تعمل تلقائيًا لم تسجل أية حوادث أثناء الأعوام القليلة الماضية. وأشار إلى أن أنظمة الحماية المستخدمة في مترو دبي هي التقنية المعتمدة والمستخدمة في جميع أنحاء العالم.

Emarat Al Youm, 21 November, 2009, http://www.emaratalyoum.com/local-section/2009-11-21-1.149539

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

اتخاذ القرارات الأخلاقية

ليس من السهل اتخاذ القرارات الأخلاقية، إلا أنه، على الرغم من ذلك، يجب أن تتوافر لدينا القدرة على اتخاذ القرارات. يمكن أن يكون اتخاذ القرارات الأخلاقية أمرًا موضوعيًا للغاية، وتسري العلاقات المتعلقة بهذا الأمر حالة بحالة. وقد لا يكون القرار الجيد بالنسبة لك بنفس درجة الجودة بالنسبة للآخرين.

لذلك، وقبل أن تتخذ قرارًا محددًا، يجب أن تسأل نفسك عدة أسئلة:

1. **معرفة إذا ما كان هناك أي مسألة أخلاقية**
   - هل يمكن أن يضر أو أن يؤثر القرار الخاص بك على شخص أو مجموعة بالسلب؟
   - هل يمكن أن يعرض القرار سلامتك للخطر؟
   - هل تعاني من معضلة حقيقية لاتخاذ القرار؟
   - هل القرار الخاص بك قانونيًا؟
   - هل يمكن أن تظهر أية تعارضات؟

2. **كن محددًا واحصل على الحقائق الصحيحة**
   - هل تعرف الحقائق المتعلقة بموقف أو بحالة معرفة حقيقية؟
   - هل لديك من المعلومات ما يكفي لاتخاذ القرار؟
   - هل تحتاج إلى الحصول على المزيد من المعلومات؟
   - هل تحتاج إلى التحقق من الأمر أو استشارة شخص آخر لديه المزيد من السلطات؟

3. **قيّم كل خيار**
   - ما هو الخيار الذي يؤدي إلى الحصول على أفضل الأمور ويأتي من خلاله أقل
   - قدر من الضرر؟
   - ما هو أفضل خيار يواجه الموقف أو الحالة؟
   - ما هو أفضل خيار يحترم حقوق الأطراف المعنيين؟
   - ما هو أفضل خيار يوفر حقوق متساوية)عادلة(لكل الأطراف المعنيين؟

وأخيرًا، يجب التفكير لوهلة في النتائج المحتملة من القرار الذي أنت على وشك اتخاذه. فإذا لم تكن تشعر بالراحة، فإن ذلك يعني وجود شيء خطأ..

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تمرين

1. **أثارت هزة أرضية في دولة مجاورة حملة قومية لتوفير الإغاثة لسكان هذه الدولة من تلكالكارثة. وقد أطلقت مدرستك حملة لتجميع التبرعات. وقد ساعدت في تصميم الحملة على موقعويب المدرسة، بالإضافة إلى نشر الأخبار إلى المجتمع الذي تقيم فيه عبر البريد الإلكتروني. إلاما يشير هذا السيناريو؟**

   أ. الاستخدام المتميز للتقنيات لزيادة شعبية المدرسة.

   ب. الاستخدام السريع والفعال للتقنيات لتجميع الأموال.

   ج. طريقة الاستخدام الصحيحة للتقنيات للوصول بشكل يتسم بالعدل والمساواة.

   د. سبب جيد لاستخدام التقنيات للحصول على التمويل من خلال المدارس.

2. **ما هي الأنشطة الأخلاقية التي يجب مراعاتها عند استخدام شبكة التواصل الاجتماعي؟**

   أ. استعراض مجلدات المستخدمين الآخرين الموجودة على ملقم المدرسة.

   ب. نشر تعليق شخصي على المنتدى عبر (الإنترنت).

   ج. تنزيل مقاطع فيديو من ملقم المدرسة من أجل مهمة ما.

   د. تثبيت برامج مجانية لتحسين أداء الشبكة.

3. **ترغب صديقتك في إرسال رسالة نصية إلى والدتها لأنها أدركت للتو أنها تركت محفظة نقودها في المنزل، إلا أن الرحلة الجوية الخاصة بها على وشك الإقلاع. وتماشيًا مع سياسة شركة الطيران، أعلنت المضيفة أن على جميع الركاب إيقاف تشغيل الهواتف المحمولة الخاصة بها، من أجل أمان الطائرة. ما الذي يجب عليك فعله؟**

   أ. توجيه النصيحة لها بأن ترسل تلك الرسالة النصية إلى والدتها عند الوصول إلى المطار التالي.

   ب. لا تفعل أي شيء لأن الأمر لا يهمك.

   ج. إخبارها بإرسال رسالة نصية قصيرة بسرعة.

   د. الحصول على مساعدة المضيفة لإرسال الرسالة النصية.

4. **قام زميل لك يشعر بالغيظ الشديد بنشر العبارة الآتية "أكره مادة الفلسفة. لأنها عديمة الفائدة!" على أحد مواقع التواصل الاجتماعي الخاصة به. ما الذي يجب عليك فعله؟**

   أ. إضافة تعليق لدعم هذا الادعاء.

   ب. توجيه تلك الرسالة إلى أصدقائك.

   ج. تجاهل الرسالة لأنها لا تعنيك.

   د. توجيه النصيحة إلى زميلك لإعادة التفكير في الأمر وحذف الرسالة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

5. **وجدت مقالاً على (الإنترنت) يتطابق بشكل تام مع مقال مطلوب منك كتابته الآن ولكن بلغة مختلفة. ما الذي يجب عليك فعله بعد ذلك؟؟**

أ. ترجمة هذا المقال واستخدامه كما هو.

ب. ترجمة هذا المقال واستخدام أجزاء منه فقط.

ج. إعادة توجيه البحث الخاص بك للتركيز على أمر مختلف.

د. تجاهل المقال والاستمرار في البحث الخاص بك.

الإجابة: 1.ب، 2.ج، 3.أ، 4.د، 5.ج

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

06 المشروعات الإلكترونيّة

تعرض هذه الوحدة وتشرح تفاصيل كيفية تنفيذ المعاملات على (الإنترنت). وتركز هذه الوحدة على تبعات الممارسات السيئة، مثل: الاندفاع نحو الشراء وتقديم العطاءات في الأسواق المتاحة عبر (الإنترنت) (وما هذه الأمثلة إلا أمثلة قليلة).

كما أنها تلقي الضوء على أهمية حماية المعلومات الشخصية الخاصة بك أثناء التسوق عبر شبكة (الإنترنت). وبالإضافة إلى ذلك، فإن هذه الوحدة توفر لك إرشادات حول كيفية تحديد هل موقع (الويب) آمن أم لا.

حقوق الطبع ©

أهداف التعلُّم

أهداف هذه الوحدة هي:

- عرض الطرق الخاصة بتحديد صلاحية الموقع.
- سرد طرق الحماية من الاحتيال على بطاقات الائتمان.
- سرد طرق الحماية من سرقة الهوية.
- كشف النتائج المحتملة للشراء المندفع على (الإنترنت).

نواتج التعلُّم

في نهاية هذه الوحدة، سوف تكون قادرًا على:

- وصف المشاريع الإلكترونية والطرق المستخدمة لتحديد صلاحية الموقع لإجراء معاملة إلكترونية.
- ذكر طرق الحماية من الإحتيال على بطاقات الإئتمان.
- التعرف على الآثار السلبية للشراء المندفع عبر (الإنترنت).

قائمة المراجعة

التعليمات:

بعد الانتهاء من قراءة هذه الوحدة، يُرجى إكمال الاستبيان باستخدام المقياس التالي:

المقياس:

1. ليس لدي أدنى معرفة.
2. لدي معرفة محدودة.
3. على دراية وقادر على التوضيح الجيّد.
4. ذو كفاءة وإمكانية على الممارسة الكاملة.

البنود	التحصيل العلمي	قبل	بعد
1	أدرك كيف أحدد ما إذا كان موقع (الويب) آمنًا لأنشطة المعاملات الخاصة بي على (الإنترنت).		
2	أنا أدرك ما هو الاحتيال المتعلق ببطاقات الائتمان وأعرف الطرق الصحيحة لحماية نفسي من هذا النوع من الاحتيال.		
3	أدرك كيف يمكن أن أحافظ على تفاصيل كل المعاملات الخاصة بي آمنة ضد سرقة الهُوية.		
4	أنا أدرك ما هو المقصود بالشراء المندفع وتأثيره على سلوكيات الشراء الخاصة بي.		

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المشروعات الإلكترونية - ممارسة الأعمال التجارية عبر (الإنترنت)

فهم طبيعة المشروعات الإلكترونية

لقد تم تصميم هذه الوحدة لإعلامك بالسلوكيات الملائمة للشراء على (الإنترنت)، وقنواته، بالإضافة إلى إستراتيجيات إجراء معاملات آمنة على (الإنترنت). لقد خلق توفير التطبيقات القائمة على شبكة (الإنترنت) في حياتنا اليومية، مثل التجارية الإلكترونية، ضرورة القيام بما يلي:

1. حماية المعلومات الشخصية الخاصة بنا أثناء تنفيذ المعاملات/الأعمال التجارية على (الإنترنت). يمكن العثور على التفاصيل الشخصية الخاصة بنا، مثل: العنوان، وأرقام الاتصال، والصور، في عدد من النماذج على شبكة (الإنترنت).
2. إدراك القواعد الأساسية المتعلقة بالمعاملات عبر (الإنترنت) لتجنب سوء الفهم في المستقبل.
3. اعتماد سلوك إيجابي أثناء التواجد على (الإنترنت).

تحديد أنواع المعاملات التجارية عبر (الإنترنت)

أنواع التجارة الإلكترونية

يمكن تقسيم أنواع التجارة الإلكترونية إلى الفئات الرئيسية التالية:

1. **بين الموسسات** (Business-to-Business) (B2B):

تقوم الشركات ببيع منتجاتها عبر (الإنترنت) لمؤسسات أخرى دون أن تكون طرفاً في إيصالها إلى المستهلكين، حيث تحتوي منافذ البيع عبر (الإنترنت) على أسعار محددة ومجموعات متنوعة من المنتجات وخصومات للزبائن.

2. **من الشركات إلى المستهلكين** (Business-to-Consumer) (B2C):

تقوم الشركات في هذا النوع من التجارة الإلكترونية ببيع منتجاتها مباشرة للمستهلكين الذين يعدون المستخدم النهائي لهذه المنتجات أو الخدمات، ومن الأمثلة عليها (amazon.ae).

3. **من المستهلكين إلى المؤسسات** (Consumer-to-Business) (C2B):

في هذا النوع من التجارة الإلكترونية يقوم المستهلكون ببيع منتجاتهم أو خدماتهم عبر (الإنترنت) للشركات التي تستطيع تقديم عروضها السعرية، بعدها يقوم المستهلك بمراجعة العروض المقدمة ومن ثم يختار الشركة التي تقدم السعر المناسب، ومن الأمثلة عليها.

4. **من المستهلك إلى المستهلك** (Consumer-to-Consumer) (C2C):

و هذا النوع يقوم المستهلك ببيع بضائعه لمستهلكين آخرين، ومن الأمثلة عليها(dubizzle.com).

التجارة الإلكترونية/التسوق عبر (الإنترنت)

تعني التجارة الإلكترونية والتي يشار إليها باللغة الإنجليزية بالاسم (E-commerce) أو التسوق عبر (الإنترنت) تنفيذ الأعمال التجارية على شبكة (الإنترنت)، وهي تشتمل على بيع وشراء البضائع أو الخدمات عبر (الإنترنت).

واليوم، تستخدم الكثير من الشركات الشهيرة هذا الأسلوب لتنفيذ الأعمال التجارية لتغطية أسواق أوسع.

وتوفر مواقع (الويب) الشهيرة هذه للتسوق عبر (الإنترنت) لعملائها إمكانية إجراء المعاملات الآمنة عبر (الإنترنت). فمن خلال الجلوس أمام شاشة (الكمبيوتر)، يمكن أن يؤكد المشتري عمليات الشراء الخاصة به كما يمكن أن يقوم بالدفع عبر (الإنترنت) أيضًا. ويتم شحن البضائع التي يتم شراؤها وإرسالها إلى عنوان المشتري بشكل مباشر.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

ولسوء الحظ، فإن عمليات الشراء عبر (الإنترنت) يمكن أن تؤدي في بعض الأحيان إلى حدوث ارتباكات تتمثل في تأخير تسليم البضائع، أو عدم اتفاق جودة البضائع مع الأوصاف المعروضة على موقع (الويب)، أو عدم وصول البضائع على الإطلاق!

ما الذي يجب القيام به قبل تنفيذ معاملة عبر (الإنترنت)؟

توفر مواقع (الويب) المتاحة على (الإنترنت) معلومات خاصة ضرورية يجب الالتفات إليها قبل تنفيذ المعاملات على (الإنترنت). وتشتمل تلك المعلومات على ما يلي:

1. اسم البائع، وعنوانه، ورقم الهاتف الخاص به.
2. عنوان البريد الإلكتروني الخاص بالبائع (إن وجد).
3. وصف للبضائع أو الخدمات.
4. السعر الإجمالي بالإضافة إلى بيان تفصيلي بشروط الدفع.
5. تاريخ تسليم البضائع أو الخدمات.
6. العملة التي يتم دفع الثمن بها.
7. توضيح كيفية شحن البضائع إليك.
8. سياسة الإرجاع أو الاستبدال للبائع، إن وجدت.
9. يجب إعطاؤك نسخة من العقد.
10. يجب أن يحتوي الموقع الإلكترونيّ على بروتوكول آمن.

نصائح: التسوق عبر (الإنترنت)

- كن على علم بمواضع شبكة (WiFi). هناك نقاط فعالة غير آمنة، مما يمكن القراصنة من التقاط أي وكافة المعلومات التي تتدفق إلى ومن أي نقطة فعالة، مما يمكنهم من سرقة المعلومات السرية والشخصية (معلومات تسجيل الدخول، وكلمات المرور، ورسائل البريد الإلكتروني، والوثائق المرفقة) المخزنة على جهاز المحمول الخاص بك.
- ابحث عن المواقع التي توفر الدفع الآمن – سيظهر رمز قفل على الشاشة أثناء ملء تفاصيل الدفع.
- كن على حذر من الحيل والعروض غير المرغوب فيها. يمكن أن يكون الموقع المعلن عنه ضارًا ويساهم في تنزيل البرمجيات الخبيثة على جهاز (الكمبيوتر) الخاص بك. أو يمكن أن يكون وراءه عملية نصب واحتيال، وهذا يعني أنك لن تتلقى أبدًا ما طلبت الحصول عليه!
- لا تثق في نتائج محرك البحث. الهجمات على محسّنات نتائج محرك البحث هي إحدى وسائل مجرمي (الإنترنت) لتغيير خوارزمية محرك البحث في ترتيب المواقع من أجل دفع بعض المواقع إلى أعلى قوائم نتائج البحث عن بعض الكلمات المفتاحية.
- احذر من رسائل البريد الإلكترونيّ التي تقول "مرحبًا راجع تخفيضات العطلة لدينا هنا!" أو "توفر هنا تخفيضات بنسبة (50%) على المبيعات في أعياد الميلاد!" يمكن أن يكون (كمبيوتر) المرسل مصاب بالبرمجيات الخبيثة المبرمجة للانتقال من خلال عنوان البريد الإلكترونيّ والتي ترسل روابط خبيثة إلى الجميع.
- يجب أن تحمي خصوصياتك. لا تقم ببساطة بالكشف عن تفاصيلك الخاصة.
- قم بمراجعة ما إذا كانت الشركة لديها بيان خصوصية يخبرك ماذا سيفعل بالمعلومات الشخصية الخاصة بك.
- تأكد من أنك تعلم التفاصيل الكاملة عن التاجر. يمكن استخدام هذه التفاصيل كمعلومات احتياطية إذا كنت في حاجة لتقديم تقرير عن تعرضك للاحتيال.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

رسالة تحذير

إذا لم يقم البائع بالإفصاح عن المعلومات اللازمة، فيُنصح أن تبحث عن بائع آخر.

ما الذي يمكنك القيام به لحماية نفسك؟

1. تعرف على المنتج عبر الهاتف أو عبر رسائل البريد الإلكتروني.
2. ادفع الثمن من خلال بطاقة الائتمان وتتبع كل المعاملات.
3. إذا كنت تدفع الثمن عبر (الإنترنت)، فتحقق من أمان موقع (الويب). يجب البحث عن ختم الضمان أو بيان الأمان الخاص بالشركة.

العمليات المصرفية عبر (الإنترنت)

يتم تعريف الخدمات المصرفية عبر (الإنترنت) باعتبارها نظام الخدمات المصرفية عبر (الإنترنت) التي تُوفر فقط كل الخدمات التقليدية المتاحة من خلال الفرع المحلّي. إنها تتيح لعملاء البنك إجراء المعاملات المصرفية بشكل أسرع عن طريق (الإنترنت).

نصائح: تقليل مخاطر الخدمات المصرفية عن طريق (الإنترنت)

على الرغم من مزايا الخدمات المصرفية عبر (الإنترنت)، إلا أن العملاء يواجهون مخاطر مثل سرقة الهُوية والاحتيال لبطاقات الائتمان. يمكن للنصائح التالية أن تساعد على ضمان التمتع بمعاملة آمنة على (الإنترنت).

1. الحفاظ على كلمات السر الخاصة بك، ورقم التعريف الشخصي (PIN) وأرقام البطاقة في سرية لا تقم بمشاركة كلمة السر الخاصة بك مع أي شخص آخر. قم بتغيير كلمة المرور الخاصة بك بصفة دورية، واستخدم كلمة مرور مختلفة لكل موقع ويب مختلف. اجعل من الصعوبة بمكان على أي فرد أن يخمن كلمات المرور الخاصة بك باستخدام مجموعة من الحروف والأرقام.
2. ابحث عن أيقونة "الإغلاق" قبل إدخال أية معلومات شخصية إلى أي موقع ويب، ابحث عن أيقونة "الإغلاق" في المستعرض الخاص بك. يشير "الإغلاق" المغلق إلى أن موقع (الويب) آمنًا. شكل آخر من أشكال تأمين موقع (الويب)، عندما يبدأ محدد موقع المعلومات (URL) بـ (https://).
3. استخدم جدار حماية قم بتثبيت أحدث برنامج لجدار الحماية على الحاسب الآلي الخاص بك لتعقب المتسللين.
4. ثبّت التحديثات الأمنية تمكن معظم أنظمة تشغيل الحاسب الآلي المستخدمين من تحديث أنظمة أمان الأجهزة الخاصة بهم لحماية البيانات من البرامج الضارة والفيروسات والتهديدات الأخرى.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

التعرف على القضايا المتعلقة بممارسة المعاملات عبر (الإنترنت)

الاحتيال المتعلق بالبطاقات الائتمانية

اليوم، يستخدم معظم الناس بطاقات الائتمان والمدين للشراء. فهذه البطاقات لا تساعد فقط على جعل المعاملات أكثر سهولة وأسرع، بل إنها تحل محل الحاجة إلى حمل الأموال. وبالإضافة إلى ذلك، تعتبر بطاقات الائتمان والمدين أفضل وسائل الدفع لعمليات الشراء عبر (الإنترنت).

على الرغم من ميزات الأمان المتنوعة التي توفرها شركات بطاقات الائتمان، إلا أن مستخدمي بطاقات الائتمان لا يزالون معرضين لخطر الاحتيال المتعلق ببطاقات الائتمان. وفي الواقع، فإن حتى أولئك الذين لا يمتلكون بطاقات ائتمان يصبحون ضحايا، لأن المعلومات الشخصية الخاصة بهم يمكن أن يتم استخدامها للتقدم لشراء بطاقات الائتمان من قِبَل المحتالين.

دراسة حالة (18): حكم بالحبس على رجل بتهمة التسوق لفترة قصيرة مستخدمًا (15) بطاقة ائتمان مزيفة

دبي – تم الحكم على رجل يبلغ من العمر (42) عامًا بتهمة استخدام وثائق تتعلق بأشخاص آخرين، وبتهمة التزوير والغش ومحاولة الغش وانتحال صفة الآخرين.

تم العثور على (15) بطاقة ائتمان من خلال بطاقتان من بطاقات العمل المفقودة، في حوزة المتهم بالإضافة على عنصر آخر مشتبه به. وكما هو مزعوم، حصل هؤلاء المتهمين على (61,000) درهم إماراتي من المصرف المحلي باستخدام بطاقات ائتمان مزورة في المتاجر.

قام المتهم أيضًا بجولة تسويقية صغيرة، اشترى خلالها مجوهرات تساوى (58,000) درهم إماراتي، وبضائع أخرى تبغ قيمتها (16,500) درهم. وحاول هذا المتهم إجراء عمليات شراء أخرى لكنه فشل في ذلك بسبب رفض العديد من المتاجر بطاقات الائتمان التي بحوزته.

كان أحد المسئولين الرسميين من قسم المخاطر ومكافحة الغش التابع للمصرف المحلي موجودًا في العمل عند إخباره بشأن الاستخدام المريب لبطاقات الائتمان من قبل المدعى عليه. وعند فحص البطاقات من قبل المسئول، تبين له أن هذه البطاقات لم تصدر من هذا المصرف. هذه الأرقام المسلسلة للبطاقات مدرجة في مصرف في دولة أخرى، وتخص عملاء هذا المصرف.

في الثاني من يناير، تم اعتقال شخص عاطل بعد أن أثار الشبهات حوله في محل للمجوهرات في مدينة النايف.

أخبر البائع المدعى العام أنه كان في نوبته بالعمل عندما اشترى المدعى عليه سبع أساور ذهبية. قام المتهم بدفع المبلغ باستخدام بطاقة ائتمان أخرى بعد رفض ماكينة الصرف للبطاقة الأولى.

تظاهر البائع بأنه يغلف المجوهرات، واستدعى قسم التحقيقات الجنائي أثناء توقيع المدعى عليه إيصال الشراء.

Khaleej Times Online, 15 September, 2011, http://bit.ly/vESq4c

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

عمليات الخداع الشائعة المتعلقة بالبطاقات الائتمانية

توجد عدة أنواع من عمليات الاحتيال المتعلقة ببطاقات الائتمان الشهيرة للغاية حاليًا، مثل:

- سرقة بطاقة الائتمان: عندما يستولي شخص على بطاقة ائتمان شخص آخر ويستخدمها بدون الحصول على إذن منه.
- التزييف: عندما يستولي شخص على تفاصيل بطاقة ائتمان شخص آخر ويستخدمها لتحقيق مصالحه. يمكن أن تفيد تفاصيل بطاقة الائتمان للآخرين، خصوصًا فيما يتعلق بالمعاملات التي تتم على (الإنترنت).
- عمليات الاحتيال المتعلقة بعدم وجود البطاقات: يمكن الحصول على التفاصيل من بطاقة مسروقة، أو من خلال فحص أو الاطلاع على لإيصالات الخاصة بشخص ما، أو من خلال نسخ البيانات أثناء المعاملات.

نصائح: كيفية تتجنب تزييف بطاقة الائتمان

من الضروري للغاية لملاك بطاقات الائتمان الحفاظ على أمان البطاقات الخاصة بهم. فكل معاملة يتم تسجيلها. وإليكم بعض الإرشادات الخاصة بكيفية تجنب عمليات الاحتيال الخاصة ببطاقات الائتمان:

1. احتفظ ببطاقة الائتمان الخاصة بك في مكان آمن لا تحمل أكثر من بطاقة واحدة أو بطاقتين معك. ليس من الآمن حمل أكثر من بطاقتي ائتمان في حافظة النقود، لأنه من المحتمل فقدها أو نسيانها في مكان ما.
2. قم بتقطيع كافة الوثائق المتعلقة بتفاصيل بطاقة الائتمان الخاصة بك إلى قطع صغيرة قم بالتخلص من كل المستندات، والمراسلات البريدية، والفواتير التي تتم طباعة تفاصيل بطاقات الائتمان الخاصة بك عليها.
3. لا تقم بالتوقيع على أي إيصالات بطاقات ائتمان خالية دائمًا تحقق من المبلغ المذكور في الإيصالات قبل التوقيع عليها.
4. تجنب الإعلان عن معلومات بطاقة الائتمان الخاصة بك إذا طلب منك شخص ما تفاصيل بطاقات الائتمان الخاصة بك، فلا تقم بإعطائها لهم بسهولة.
5. كن حذرًا عند استخدام هذه البطاقات عبر (الإنترنت)، لا تسترسل في متابعة أية معاملات تجارية عبر (الإنترنت) حتى وإن جاءك إعلام (بريد إلكتروني/اتصال هاتفي) من شخص ما يدعي أنه مسئول بطاقات ائتمان.
6. الإبلاغ على الفور عند فقدان أو سرقة بطاقات الائتمان الخاصة بك. في حالة فقد بطاقات الائتمان الخاصة بك، فقم بإبلاغ البنك وشركة بطاقات الائتمان على الفور.
7. لا تعط بطاقة الائتمان الخاصة بك مطلقًا لأي شخص آخر.
8. تحل بالذكاء عند دفع الفواتير باستخدام بطاقات الائتمان تحل بالذكاء أثناء دفع الفواتير عبر بطاقات الائتمان. ألق نظرة ثاقبة على كل معاملة يتم إجراؤها وافحص المعاملة بشكل شامل.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة (19): تم الاعتقال عند محاولة شراء الآلات باستخدام بطاقات ائتمان مزورة

الشارقة – ألقت الشرطة القبض على ثلاثة رجال وسيدة ممن يستخدمون بطاقات ائتمان مزيفة للتسوق المزعوم للحصول على أدوات إلكترونية من منافذ في عدة أماكن.

ووفقًا لكلام مسئول قسم التحقيق الجنائي، تلقت الشرطة معلومات سرية من مصدر ما حول هذه العصابة، وكون هذا المسئول فريق من رجال الشرطة للتعرف على المشتبه بهم وتحديد أماكنهم خلال وقت قصير.

أخبر أحد مديري منافذ البيع الشرطة عن وصول المشتبه بهم وأوقعهم فريق الشرطة في الفخ. تم القبض على العصابة الثلاثية.

وعند استجوابهم، أقر هؤلاء بأنهم حصلوا على بطاقات الائتمان من دولة أجنبية تحت إشراف شخص ما. ثم تعاونوا بعد ذلك مع رجال الشرطة للقبض على المشتبه الرابع.

Khaleej Times Online, 14 September, 2011, http://bit.ly/vgQy2A

الشراء المندفع

يتم تعريف الشراء المندفع على أنه الشراء غير المخطط له أو العفوي. ويشار إلى الشخص الذي يميل إلى فعل ذلك باسم المشتري المندفع.

معرفة النفس: هل أنت مندفع عند الشراء

لا يدرك الكثيرون أنهم مشترون مندفعون. إذًا، كيف يمكن معرفة ما إذا كنت مشترٍ مندفع أم لا؟

بداية، يمكنك الإجابة على الأسئلة الخمسة التالية.

أسئلة معرفة النفس
هل تقوم بالتسوق وترك مكان التسوق بدون شراء أي شي أو مع شراء شيء واحد فقط؟ أ. لم يحدث ذلك من قبل تقريبًا. ب. نادرًا ما حدث ذلك. ج. في بعض الأوقات. د. دائمًا. أعرف بالضبط ما أنوي شرائه قبل التوجه إلى مكان التسوق.
عندما تقوم بالتسوق مع الأصدقاء، هل تشعر بالحاجة إلى شراء المزيد من الأشياء؟ أ. نعم، أشعر بمتعة أكبر عند إنفاق الأموال أثناء التواجد مع مجموعات. ب. في بعض الأحيان، إذا أقنعني صديق بشراء شيء ما. ج. نادرًا، إلا إذا رأيت شيئًا يباع بثمن منخفض. د. لا مطلقًا. أنا أعرف ما أبحث عنه، ولم أنحرف مطلقًا عن نواياي.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أسئلة معرفة النفس

هل تقوم بإنفاق الأموال التي لا تخصك؟

أ. نعم، بصفة دائمة. أدرك ذلك عندما تصل فواتير بطاقة الائتمان، وسوف أتمكن من دفع ثمن الفواتير بطريقة أو بأخرى.

ب. في بعض الأوقات عندما أحتاج إلى شيء ما احتياجًا شديدًا. أرى أن أقترض من الأصدقاء أو من أحد أفراد الأسرة إذا اضطررت إلى ذلك.

ج. نادرًا، إلا إذا كان الأمر طارئًا، مما يعني أنني لا يمكنني دفع الإيجار.

د. لا مطلقًا. لدي ميزانية التزم بها ودائمًا أقوم بتوفير راتب ستة أشهر للطوارئ.

هل تقوم بدفع الحد الأدنى لبطاقة الائتمان الخاصة بك؟

أ. دائمًا.

ب. في بعض الأحيان.

ج. نادرًا ما يحدث ذلك.

د. لا مطلقًا.

هل تقوم بالبحث عن المشتريات غالية الثمن (الأكثر من 100 دولار) أو أنك تقوم بشراء أول شيء تقع عينك عليه؟

أ. إذا لفت نظري شيء، فإني أشتريه.

ب. يمكن أن ألقي نظرة للمراجعة قبل التوجه إلى المتجر، ثم أقوم بالشراء. أبحث عن الأسعار قبل مغادرة المنزل، إلا أنه إذا جذب شيء ما نظري، فإنني أقوم بشرائه دون تردد.

ج. أقوم بعمل بحث مكثف مع مقارنة الأسعار، والتصفيات، والمتاجر المتاحة على (الإنترنت) والمتاجر الفعلية بالإضافة إلى القسائم والتخفيضات قبل أن أضع قدمي في متجر. ثم أقوم بفحص السلعة فحصًا شاملاً وأقوم بقراءة كل المطبوعات الدقيقة قبل الشراء.

1. إذا كانت إجابتك بالحرف "د" على كل إجابة، فتقبل تهانينا! فأنت من المستهلكين الأذكياء، الذين يعرفون كيف ينفقون بحكمة ويبذلون كل قرش في موضعه الصحيح.

2. إذا كانت إجابتك بالحرف "أ" على كل سؤال، فأنت بحاجة إلى مساعدة! ابحث عن أخصائي لمساعدتك على عمل ميزانية وتعلم كيفية الالتزام بها. وأنت بحاجة لمعالجة مشكلة الإنفاق قبل أن تخرج عن السيطرة بالكلية.

3. إن كانت إجابتك "ب" أو "ج" على أربعة أسئلة من أصل خمسة، فقد تكون ممن لا يعانون من مشكلة كبيرة حتى الآن، لكنه ينبغي عليك التريث والتأني في إنفاق كل قرش. وبعد البدء في تتبع النفقات الخاصة بك، ستبدأ تدرك حجم الأموال التي أهدرتها دون أن تعرف ذلك.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

نصائح: كيف تتجنب أن تكون مشتر مندفع

1. كن على بينة من حجم الأموال الذي تنفقه وفكر مليًا في كل قرش تنفقه. قد تريد ألا تنفق الكثير على الأمور غير الضرورية. وأفضل شيء تفعله هو وضع ميزانية خاصة بك والالتزام بها.

2. التفكير مرتين قبل الشراء، فإذا كان لديك ميل للاندفاع بالشراء، فكن على حذر من أي إعلان قد يؤثر عليك.

3. يلزم أن يكون لديك أهداف واضحة أثناء التسوق حدد أهدافك في كل مرة تذهب فيها للتسوق والتزم بها. قد تحتاج إلى ما يذكرك كأن تصطحب معك دفتر ملاحظات يمكنك أن تدون فيه جميع المنتجات التي تحتاج إليها قبل الذهاب.

دراسة حالة (20): هل أنا مشترٍ مندفع؟ - حالة كاتي كالمسكي

(كاتي كالمسكي) طالبة بالمرحلة الثانوية (17)عامًا فازت بجائزة قيمتها (5,000) دولار في مسابقة كتابة المقالات بأسبوع التعليم الائتماني. وعنوان الموضوع هو أغبى شيء على الإطلاق فعلته بأموالي، وماذا تعلمت منه.

وتدور قصتها عندما ذهبت لسحب أموال من أحد المصارف واكتشفت أن رصيد حسابها يقل حوالي (1,100) دولار أمريكي عما كان متوقعًا. في البداية، ظنت أنها كانت ضحية للاحتيال، فعزمت بالفعل على الاتصال بالشرطة. وكان ذلك حتى سلمها مدير المصرف قائمة بالمعاملات التي أجرتها على مدى الأشهر السبعة الماضية حتى تتأكد منها. وحينئذ علمت أنها هي التي أنفقت المال باندفاع على المشتريات التي لم تكن بحاجة إليها.

وبعد أن أصيبت بالصدمة وخيبة الأمل الكبيرة في نفسها، فتحت حسابًا مصرفيًا على (الإنترنت) حتى تتابع إنفاقها. وعلى الرغم من كل ذلك، فإنها تشعر بالامتنان أنها تعلمت الدرس وهي في عمر الـ (17) وليس بعد (15) عامًا عندما أصبح لديها أطفال تطعمهم وعليها قرض عقاري تدفعه. فقد تعلمت الآن أن تتابع معاملات بطاقة الخصم الخاصة بها وأصبحت مسؤولة عن الشؤون المالية لنفسها. وكتبت كاتي قائلة، "على الرغم من أن الأمر بدا لي وكأنه نهاية العالم، إلا أن ذلك كان في نهاية المطاف هو أفضل خطأ ارتكبته في حياتي".

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تمرين

1. **وجدت متجرًا على (الإنترنت) يعرض خصمًا ممتازًا على المنتجات الجلدية. كيف يمكن أن تتحقق من مصداقية موقع ويب التجزئة هذا لإجراء عمليات الشراء ودفع الأموال؟**
   - أ. الاتصال بالشركة مباشرة للتحقق من موقع (الويب).
   - ب. البحث عن تقرير مصداقية من هيئة تجارية محلية.
   - ج. الاطلاع على عنوان موقع (الويب) لمعرفة ما إذا كان يبدأ بالبادئة(https:).
   - د. قراءة مراجعات وملاحظات العملاء حول المتجر.

2. **ما هي أفضل طريقة لحماية نفسك من عمليات الاحتيال المتعلقة ببطاقات الائتمان؟**
   - أ. إقراض بطاقة الائتمان الخاصة بك للأشخاص الذين تعرفهم فقط.
   - ب. تخزين رقم التعريف الشخصي (PIN) على الهاتف الخلوي الخاص بك.
   - ج. إرسال معلومات بطاقة الائتمان الخاصة بك إلى الآخرين عبر رسائل البريد الإلكتروني.
   - د. توفير معلومات بطاقة الائتمان الخاصة بك إلى مواقع (الويب) الآمنة فقط.

3. **ما الخياران اللذان يوضحان طرق حماية نفسك من سرقة الهوية عبر (الإنترنت)؟ (اختر إجابتين)**
   - أ. إبلاغ السلطات المحلية بكل عمليات الشراء المتعلقة ببطاقة الائتمان الخاصة بك.
   - ب. الاهتمام الشديد بما تشاركه أثناء استخدام برامج مشاركة الملفات.
   - ج. مشاركة المعلومات الخاصة بك مع أفراد الأسرة والأصدقاء المقربين فقط.
   - د. لا تقم بإعطاء معلوماتك الشخصية عبر البريد الإلكتروني أو عبر شبكة (الإنترنت).
   - ه. تقطيع المستندات وأوراق العمل التي تحتوي على معلومات شخصية قبل التخلص منها.

4. **ما هي النتيجة المحتملة للشراء المندفع على (الإنترنت)؟**
   - أ. إدارة الميزانية الشهرية بشكل أفضل.
   - ب. الميل لشراء السلع غير الضرورية.
   - ج. صنع القرار بحكمة عند شراء.
   - د. الحصول على قسائم الخصم من المتجر.

الإجابة: 1. ج، 2. د، 3. ب ود، 4. ب

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

07 الرعاية الإلكترونيّة

حول هذه الوحدة:

يجب علينا فهم الرفاهية المادية والنفسية في عالم التقنيات الرقمي ولكن ينبغي علينا في ذات الوقت الانتباه للمخاطر المختلفة المرتبطة باستخدام هذه التقنيات.

في هذه الوحدة، سوف نلقي نظرة على أكثر المشاكل انتشارًا والمتعلقة بالصحة والأمان أثناء استخدام هذه التقنيات ومن ثم الخطوات التي يمكن اتخاذها لتقليل المخاطر. كما سنتطرق إلى بعض مصطلحات مثل "إدمان (الكمبيوتر) وشبكة (الإنترنت) " و "بيئة العمل الصحية"، بالإضافة إلى التأثير البيئي لاستخدام أجهزة (الكمبيوتر).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أهداف التعلُّم

أهداف هذه الوحدة هي:

- تزويد القارئ بالمعلومات اللازمة حول بيئة العمل الصحية المناسبة أثناء استخدام (الكمبيوتر).
- بيان المخاطر الصحية المتعلقة باستخدام أجهزة (الكمبيوتر).
- توضيح المشاكل الاجتماعية المقترنة بشبكة (الإنترنت) والإدمان على استخدام أجهزة (الكمبيوتر).
- التعريف بطرق إعادة تدوير أجهزة (الكمبيوتر) والتخلص منها بالشكل الصحيح.

نواتج التعلُّم

في نهاية هذه الوحدة، سوف تكون قادرًا على:

- شرح ظروف بيئة العمل الصحية التي تساعد في تحسين الأداء وزيادة الإنتاجية.
- توضيح طرق منع الاضطرابات البدنية عند استخدام أجهزة (الكمبيوتر).
- شرح أعراض إدمان (الإنترنت).
- توضيح طرق إعادة تدوير والتخلص السليم من أجهزة (الكمبيوتر).

قائمة المراجعة

البنود	التحصيل العلمي	قبل	بعد
1	أنا أدرك كيف تساعد بيئة العمل الصحية في تحسين أدائي و إنتاجيتي.		
2	أنا أدرك المشاكل الصحية التي يعاني منها مستخدمو أجهزة (الكمبيوتر).		
3	أنا أدرك كيفية ولماذا يدمن الناس استخدام أجهزة (الكمبيوتر) وشبكة (الإنترنت).		
4	أنا أعلم أي من استخدامات التقنية تعتبر أخلاقية أوغير أخلاقية.		

التعليمات:

بناءً على معرفتك السابقة والمعارف التي ستكتسبها بعد الانتهاء من قراءة هذهالوحدة،

يُرجى إكمال الاستبيان باستخدام المقياس التالي:

المقياس:

1. ليس لدي أدنى معرفة.
2. لدي معرفة محدودة.
3. لدي معرفة جيدة وأفهم ما قرأته.
4. كفؤ وأستطيع تطبيق كل ما تعلمته.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الرعاية الإلكترونية - الرفاهية المادية والنفسية في عالم رقمي

إذا ألقيت نظرة على العالم اليوم، فسوف تدرك أن الناس يعيشون أسلوب حياة صحية أفضل مما اعتادوا عليه في الماضي، والسبب في ذلك يرجع إلى تقدم العلوم الطبية التي تطورت بشكل سريع في الآونة الأخيرة من حيث توفير الخدمات ووسائل العلاج الصحية عالية الجودة.

لقد ساعدت التقنيات الحديثة الأطباء والعلماء في العثور على الوسائل العلاجية وتطوير الأدوية للكثيرمن الأمراض الخطيرة، كما تم توفير تنوع جيد من المكملات الغذائية والفيتامينات التي يمكن أن تساعد في الحيلولة دون وقوع الأمراض. نتيجة لذلك، انخفضت معدلات الوفيات وأصبح الناس يعيشون لفترة أطول وبشكل أفضل. بشكل عام أصبح معظم الناس يتمتعون بحياة أكثرصحية.

ومع ذلك، ما لا يمكننا رؤيته هو أنه وسط كل هذه التطورات في التقنية والعلوم الطبية التي ساعدت في السيطرة على عدد كبير من الأمراض، ظهر جيل جديد من الأمراض بدلاً منها. وبالرغم من أنها لا تكون ظاهرة للعيان، لكنها ليست أقل خطرًا. والأهم من ذلك، فإن الكثير منها يتعلق باستخدام التقنيات الرقمية.

إذًا، فما المقصود بالرعاية الإلكترونية؟ ما علاقتها بالأمراض وكل ما سبق؟

الرعاية الإلكترونية عبارة عن مصطلح يستخدم للإشارة إلى إرشادات الأمان المستخدمة للاعتناء بالرفاهية النفسية والجسدية لمستخدمي التقنيات الرقمية. ولقد تم إنجاز الكثير من الأعمال في العصر الحديث بشكل أسرع بسبب استخدام أجهزة (الكمبيوتر). فالمدرسون، والطلبة، والعاملون في المكاتب، والمسئولون الحكوميون، وغيرهم الكثير، يستخدمون أجهزة (الكمبيوتر) في أعمالهم وحياتهم اليومية. ولكن مع الأسف لا ندرك أنه على الرغم من أن أجهزة (الكمبيوتر) قد جعلت حياتنا أسرع وأسهل، إلا أننا نميل إلى قضاء عدة ساعات أمام التطبيقات لدرجة أننا في بعض الأحيان ننسى أن نتناول الطعام أو الاستحمام. كما أننا أصبحنا نتجاهل صحتنا أثناء العمل.

لذا، فإن الرعاية الإلكترونية تساعدك في إدراك مخاطر هذه التهديدات، وما يمكنك القيام به لتقليل المخاطر المتعلقة باستخدام التقنيات الرقمية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

إدراك مفهوم بيئة العمل الصحية وأهميتها (قاعة الدرس/مختبر الحاسوب)

في هذه الوحدة، ستتعرف على مصطلح جديد، ألا وهو بيئة العمل الصحية (ergonomics). وهو مصطلح مشتق من اللغة اليونانية ومكون من كلمتين (ergon) وتعني العمل و(nomos) وتعني القوانين. وبالتالي يصبح المعنى الكامل للمصطلح هو (القوانين الطبيعية).

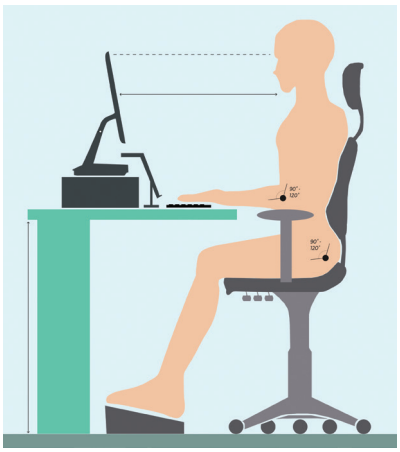
هل تتذكر كيف تطرقنا للتهديدات التي يمكن أن تتعرض لها نتيجة قضاء ساعات طويلة، غير مريحة، أمام شاشة (الكمبيوتر)؟

إن بيئة العمل الصحية هي علم يساعد الناس في صنع وتصميم آلات أو أدوات تتسم بالراحة وسهولة الاستخدام. وبمعنى آخر، بدلاً من جعل مستخدمي أجهزة الحاسوب يتكيفون مع الطريقة التي يتم تصميم الأجهزة بها، فإنه يحاول تصميم الأجهزة والآلات بطريقة تتناسب مع المستخدم كالأثاث والملحقات المريحة، مثل مقعد الحاسوب، الفأرة ولوحة المفاتيح بشكل يقلل من التعب والإجهاد الذي يعاني منه مستخدمو الحاسوب.

بالنسبة لجمعية بيئة العمل الصحية العالمية فهي تُعرّف مصطلح (ergonomics) على أنه "العلم الذي يُعنى بتوضيح التفاعل بين العنصر البشري والبيئة المحيطة به وبين المهنة التي يمارسها لاستخدام المعلومات المتوفرة، المبادئ، البيانات وطرق التصميم المعروفة من أجل تحسين رفاهية الإنسان في بيئة عمله وتحسين أداء المنظومة بشكل عام ومتكامل".

قم بإلقاء نظرة على بعض أمثلة الأثاث والملحقات التي يتم تصميمها بشكل صحي أدناه:

مقعد صحي



محطة عمل صحية

ماوس صحي

لوحة مفاتيح صحية

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تطبيق مفهوم بيئة العمل الصحية في حياتنا

والآن، وبعد أن تعرفت ماهي بيئة العمل الصحية، مالذي يمكن أن تفعله لتحقيق تلك البيئة؟

توفر بيئة العمل الصحية طريقة للناس للعمل والحياة بشكل يتسم بالتناسق مع البيئة المحيطة بهم. فهي تساعد الناس على الاستمتاع بالأشياء المحيطة بهم، والشعور بالتكيف معها، سواء أثناء العمل أو أثناء الاسترخاء في المنزل. فعندما يشعر الناس بالراحة والاسترخاء، فإن الأعمال التي يقومون بها سوف تؤدي هي الأخرى إلى الحصول على نتائج أفضل مع تزايد قدرتهم على العمل بمزيد من الراحة والتفكير بشكل أكثر صفاء.

ويوفر المكتب الصحي مكان عمل أفضل، بينما يوفر المنزل المصمم بشكل صحي مكانًا أكثر راحة للإقامة به. ولكي تتمكن من تحقيق ذلك، يجب أن تتعرف على كيفية تصميم محطة عمل صحية. توفر الإرشادات التالية لك المعلومات اللازمة حول كيفية القيام بذلك بالشكل الصحيح.

ارتفاع سطح العمل

طاولة كمبيوتر قابلة للتعديل

1. بدايةً، يجب أن تقوم بضبط ارتفاع سطح العمل أو المنضدة التي تعمل عليها.
2. تحقق من أن مرفقك فوق السطح بما يساوي طول إصبع حتى لا تضطر إلى الانثناء كثيرًا أو إجهاد نفسك للوصول إليه.
3. تذكر أن تقوم بضبط المقعد بناءً على ذلك أيضًا. وفي الحقيقة، قد تحتاج إلى تعديل المقعد والمنضدة معًا، أو أحدهما فقط.

المقعد

مقعد مريح

1. من الضروري أيضًا اختيار مقعد مصمم بشكل جيد يدعم ظهرك ويسمح لك بالعمل بكل راحة.
2. اختر مقعدًا يمكن تعديل ارتفاعه ودرجة ميله. تحقق من كون المقعد أفقيًا إلى حد ما، ولكن يجب أن يكون مائلاً قليلاً حتى تتمكن من الوصول إلى لوحة المفاتيح وسطح العمل واستخدامهما بكل سهولة. استخدم مسندًا للقدم حتى تتجنب إجهاد عضلات الرجل أو لاستخدامه في حالة عدم وصول قدمك إلى الأرض.
3. لا تهبط أو تترهل في المقعد. قم بضبط المسند الخلفي حتى يمكنك إراحة الجزء السفلي من ظهرك عليه وتجنب الضغط الزائد عن الحد.
4. اختر مقعدًا به مسندين للذراع، وتحقق من إمكانية ضبط هذين المسندين. قم بضبط مسندي الذراع بحيث يكون الذراعين مرفوعين قليلاً من عند الكتفين. فبتلك الطريقة يمكنك تجنب وضع المزيد من الإجهاد على الرقبة والكتفين.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

وضع لوحة المفاتيح

1. قم بضبط موضع لوحة المفاتيح حتى تسمح بأن يكون ذراعاك متوازيين مع يديك. يجب أن يتم وضع ذراعيك بشكل أفقي، بحيث أن يكون المعصمين مفرودين.
2. وتحقق أن ذلك لا يؤدي إلى إبعاد المرفق كثيرًا عن جانبك، فإذا حدث ذلك، فاضبط ارتفاع المنضدة بناءً على ذلك.

وضع الشاشة

1. قم بضبط المقعد بحيث يسمح لعينيك بأن تكونا في مستوى مريح فيما يتعلق بالشاشة. تحقق من أن تسمح لك المسافة بين عينيك وبين الشاشة بالتركيز بأفضل شكل ممكن على ما تشاهده.
2. اضبط ارتفاع الشاشة بحيث تكون عيناك فوق مستوى أعلى الشاشة، وتحقق من قدرتك على النظر إلى الجزء السفلي من الشاشة بدون الاضطرار إلى إمالة رأسك إلى أسفل. وهذا يعني أن مركز الشاشة يكون قريبًا إلى حد ما من ارتفاع كتفك، وأنك لا تحتاج إلى تحريك عينيك إلى أعلى وإلى أسفل دون تحريك رأسك.

حامل المستندات

1. من الأفكار الجيدة شراء حامل مستندات، حيث يساعد ذلك على تقليل حركة رأسك عند تغيير تركيزك من على الشاشة إلى المستندات التي تتعامل معها.
2. ضع حامل المستندات بالقرب من شاشة (الكمبيوتر). واضبطه بحيث لا تحتاج إلى ثني أو إمالة رأسك كثيرًا تجاه الشاشة أو تجاه المستندات.

تصميم سطح المكتب

تحقق من القدرة على الوصول إلى كل المستندات وإلى كل وسائل التحكم بكلا اليدين بحيث لا تكون هناك حاجة إلى ثني وإدارة أي جزء من جسمك بدون ضرورة.

الوضع والبيئة أثناء استخدام لوحة المفاتيح

1. من الضروري تعلم كيفية الجلوس بشكل جيد أثناء القيام بالأعمال الخاصة بك. ويمكن أن يشتمل ذلك على الجلوس بطريقة طبيعية ومسترخية، بحيث تتاح لك حرية الحركة واتخاذ مواضع بديلة أخرى. لا تجعل بطريقة متجمدة ومتصلبة.
2. تجنب الإجهاد من خلال تغيير وضع جسمك بشكل متكرر. حاول تجنب الأوضاع الصعبة التي يمكن أن تسبب الإجهاد للمفاصل، خصوصًا المعصمين.
3. تحقق من الراحة لفترات قصيرة متقاربة بدلاً من الحصول على فترات راحة أطول ولكنها غير متقاربة. راقب حمل العمل الخاص بك – وتحقق من عدم إجراء تغييرات سريعة أو حادة فيما يتعلق بزيادة معدل العمل الخاص بك. وبدلاً من ذلك، قم بالوصول إلى تلك الزيادة بشكل متدرج وببطء لتجنب الإجهاد.
4. ويمكن زيادة العدد الإجمالي لفترات العمل التي تشتمل على استخدام لوحات المفاتيح بعد الحصول على راحة طويلة، وفقط إذا كانت الظروف تسمح لك بذلك.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

إضاءة وحدات شاشات العرض المرئي (Lighting for Visual Display Units – VDUs)

1. يجب أن يكون مصدر الإضاءة الخاص بك منير بما فيه الكفاية عند عملك على جهاز (الكمبيوتر) الخاص بك.
2. تجنب وضع الشاشات بالقرب من النوافذ.
3. إذا كانت هناك مستويات مختلفة للإضاءة يمكن أن تتناقض بشدة مع بعضها البعض، فاستخدم مستوى إضاءة معتدل، إلا أنك قد تحتاج إلى استخدام شاشة عالية الجودة ومقاومة للوهج.

استخدام الماوس

1. اختر ماوس مصمم تصميمًا جيدًا بحيث يجنبك الضغط على الساعدين والمعصمين.

2. لا تستخدم ماوس كبير وضخم لأنه يجبر معصميك على الانحناء بشكل مستمر في زاوية غير مريحة.
3. اترك الماوس على فترات متقاربة بحيث تتجنب الضغط على الرسغين.
4. ضع الماوس واستخدمه على مسافة مناسبة من (الكمبيوتر).

التعرف على استخدامات الحاسوب التي تؤثر على الصحة البدنية

الآن، دعونا نلقي نظرة على بعض الإصابات البدنية التي يمكن أن تحدث بسبب الاستخدام الطائش لأجهزة (الكمبيوتر) ولفترات طويلة. تعرف على هذه الإصابات حتى تكون على دراية بكيفية حدوثها وكيفية تجنبها

الإصابات الناجمة عن الإجهاد المتكرر

يمكن أن تحدث الإصابات الناجمة عن الاستخدام المتكرر، والتي يشار إليها اختصارًا ب (RSI)، بسبب استخدام اليدين لفترة طويلة. ويمكن أن يؤدي ذلك إلى عدد من الأعراض، مثل الألم، والالتهاب، والانتفاخ، والوخز، والخدر، وفقد الليونة والضعف.

ويطلق على الإصابات الناجمة عن الضغط المتكرر (RSI) أيضًا عدة أسماء أخرى، مثل متلازمة الإفراط المهني (OOS)، ومرض الصدمة التراكمية (CTD) ومتلازمة الحركة المتكررة(RMS).

ويعرف هذا المرض الذي ينجم عن الحركة المتكررة لليدين بشكل أكثر تحديدًا باسم متلازمة النفق الرسغي (CTS). وينجم هذا المرض عن تكرار تحريك اليدين، والناجم عن الاستمرار في الكتابة على لوحة المفاتيح والاستمرار في استخدام الماوس. ويمكن أن تتعرف على أعراض هذا المرض من خلال الخدر في اليدين، ووجود ألم في المعصمين. وينجم كلا هذين العرضين عن انضغاط العصب المتوسط، والذي يتواجد في الذراع، بدءًا من الأصابع. ويمكن أن يكون هذا الألم شديدًا للغاية، كما يمكن أن يمتد إلى الرقبة أيضًا.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

آلام الظهر

يمكن أن تكون قد عانيت من آلام أسفل الظهر بسبب الجلوس والعمل في مقعد كمبيوتر لفترة زمنية طويلة. وفي الواقع، يمكن أن تكون قد تعرضت لمضاعفات لمشكلة موجودة بالفعل في الظهر أو الرقبة. فلماذا يحدث ذلك؟ يحدث ذلك لأنك تجلس أمام.

جهاز (الكمبيوتر)، أو في أي مكان آخر، وتكون في حالة من الثبات. ويساعد ذلك على تزايد الضغط على الظهر والرقبة والكتفين والذراعين والقدمين. وبشكل خاص، يمكن أن يزيد ذلك من مقادير الضغط الناجمة على عضلات الظهر وديسك العمود الفقري.

وبالإضافة إلى ذلك، يميل الناس بطبيعتهم إلى السقوط في الكرسي عند الجلوس فيه لفترة طويلة ويمكن أن يؤدي ذلك إلى تمديد أربطة العمود الفقري. كما يمكن أن يزيد أيضًا الضغط على الديسك والمناطق المحيطة بالعمود الفقري. ومع مرور الوقت، إذا تركت نفسك تجلس بشكل مستمر في أوضاع غير صحيحة، فقد تكون تعرض تكوينات العمود الفقري للضرر كما تكون تعرض نفسك لنوبات متكررة من آلام الظهر.

يعاني معظم مستخدمي أجهزة (الكمبيوتر) الذين يعمدون إلى العمل لساعات طويلة أثناء الجلوس في مقعد كمبيوتر من مشاكل عنيفة في الظهر. وغالبًا ما يحدث ذلك بسبب الوضع السيئ أو الجلوس بشكل غريب أو متصلب في المقعد مع النظر بشكل مستمر إلى شاشة (الكمبيوتر).

نصائح: كيف تتجنب آلام الظهر

1. اختر مقعدًا يمكن تعديله بسهولة وبشكل تام. وتحقق من القدرة على تغيير ارتفاعه ووضع الجلوس به.
2. حاول العثور على مقعد يحتوي على مسند للقدم، أو قم بشراء مسند قدم منفصل، بحيث يمكنك وضع قدمك عليه بزاوية طبيعية.
3. استخدم شاشة يمكن تعديل وضعها. وضعها في موضع ملائم بحيث لا تضطر إلى ثني رقبتك للنظر إليها.
4. تذكر أن تأخذ فترات راحة قصيرة ولكن متكررة. انهض من المقعد وتحرك. قم بفرد عنقك وذراعيك وقدميك لزيادة المرونة.
5. اجلس بحيث يكون ظهرك مفرودًا وبحيث يكون رأسك لأعلى. لا تهبط في المقعد، وإذا وجدت نفسك تهبط في المقعد بعد مرور بعض الوقت، فقم بتعديل وضعك.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

إجهاد العين

هل تعلم أن ما يزيد على (50%) من مستخدمي أجهزة (الكمبيوتر) يعانون من إجهاد شديد في العين؟ كما أنهم يعانون أيضًا من صداع متكرر، وعدم وضوح الرؤية، بالإضافة إلى أعراض أخرى في الرؤية والتي يمكن أن تنجم عن النظر أو التحديق المستمر في شاشة (الكمبيوتر). ويمكن أن يسبب إجهاد جهاز الرؤية في حقيقة الأمر إجهادًا للجسم، ويمكن أن يقلل من كفائتك في العمل.

كما يمكن أن تتعرض عينيك للإجهاد أيضًا، أثناء العمل في مكان ظروف الإضاءة به سيئة، أو به الكثير من الوهج، أو إذا كانت الشاشة مهتزة. إلا أنه لا يوجد داعٍ للقلق، فإجهاد العين غالبًا ما يكون مؤقتًا، ويختفي بعد فترة من الزمن.

وفيما يلي بعض أعراض إجهاد العين:

- جفاف العينين أو التهابهما، أو الشعور بالحكة بهما.
- عدم وضوح الرؤية أو رؤية الصور مزدوجة.
- الصداع.
- الغثيان.
- الإجهاد.

نصائح: كيف تتجنب إجهاد العين

1. تحقق من استخدام شاشات غير مهتزة، لأن هذا النوع من الشاشات يؤدي إلى إجهاد العينين بسبب عدم القدرة على النظر إلى الشاشة بشكل مريح.
2. قم بضبط الستائر التي يمكن تعديلها في النافذة الخاصة بك للحيلولة دون سقوط أشعة الشمس المباشرة على الشاشة.
3. استخدم مصابيح تؤدي إلى تفريق الضوء بشكل متساوٍ، وتحقق من أن ضوء هذه المصابيح لا يسقط على الشاشة مباشرة.
4. استخدام فلتر للشاشة.
5. تحقق من بعد عينيك عن الشاشة بمسافة لا تقل عن (18) بوصة.
6. امنح عينيك بعض الوقت للراحة من خلال الحصول على فترات راحة بشكل منتظم والابتعاد عن الشاشة وتركيز النظر على شيء بعيد.
7. تأكد من حصولك على فترات راحة منتظمة لمدة 5 دقائق في كل ساعة.
8. قم بإجراء فحص دوري للعيون. استخدم دائمًا النظارات الخاصة بك أثناء استخدام جهاز (الكمبيوتر) إذا كانت تلك النظارات بوصفة من الطبيب.

الاضطرابات العضلية والهيكلية (Musculoskeletal Disorders – MSDs)

تعرف الاضطرابات العضلية والهيكلية (MSDs) بأنها ضعف الهيكل الجسديّ مثل: العضلات والمفاصل والأوتار والأربطة والأعصاب والعظام ونظام الدورة الدموية الموضعية التي تنتج من أو تتفاقم بسبب العمل وبيئة العمل.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المشكلات الاجتماعية المقترنة باستخدام أجهزة (الكمبيوتر) و(الإنترنت)

ما المقصود بالاستخدام الصحي لشبكة (الإنترنت)، وما هو الاستخدام غير الصحي لها؟ كيف يمكن أن تتعرف عليهما، وأن تفرق بينهما؟ ليس من السهل الإجابة على هذا السؤال، لأن الأفراد المختلفون يستخدمون شبكة (الإنترنت) بطرق مختلفة، ولأغراض مختلفة.

قد يحتاج البعض إلى قضاء فترات زمنية طويلة على شبكة (الإنترنت)، لأنهم يقومون بأعمالهم من خلالها. وبالتالي فإن شبكة (الإنترنت) تكون بمثابة المكان أو المنصة الرئيسية لعملهم. والبعض يمكن أن يستخدم شبكة (الإنترنت) بشكل منتظم لأغراض الأعمال التجارية، مثل الإعلان عن البضائع الخاصة بهم والاطلاع على أوامر الشراء. يمكن أن يقضي الطلبة الكثير من الوقت على شبكة (الإنترنت) للعثور على المعلومات من مجموعة مكثفة من المعلومات المتاحة عليها. وفي نفس الوقت، يمكن أن يعتمد الآخرون بشكل كبير على مواقع الشبكات الاجتماعية للتواصل مع أفراد الأسرة والأصدقاء.

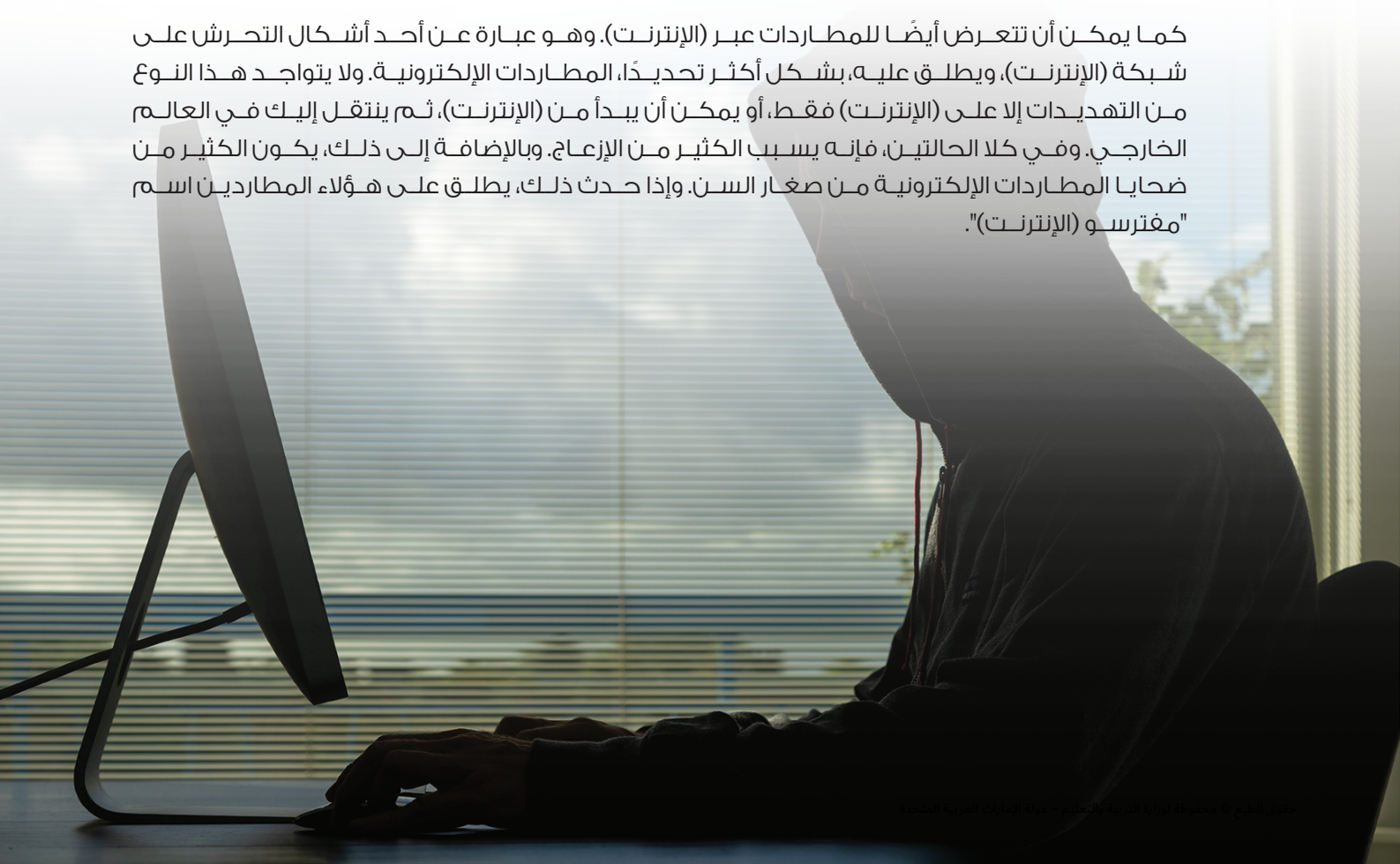
المشكلات الاجتماعية المقترنة بالاستخدام المفرط لأجهزة (الكمبيوتر) و(الإنترنت)

دعونا نلقي نظرة على بعض المشكلات الاجتماعية المقترنة بالاستخدام المفرط لأجهزة (الكمبيوتر) و(الإنترنت) أدناه:

مفترسو (الإنترنت)

يعتمد الكثيرون اعتمادًا كبيرًا على مواقع الشبكات الاجتماعية، حيث يمكنهم لقاء الآخرين لمشاركة المعلومات والتواصل معهم. كما أنهم حتى يكونون صداقات جديدة، وفي بعض الأحيان يقابلون أصدقائهم في الحياة عبر (الإنترنت). لكن يجب توخي الحذر! يمكن أن يكون مشاركة الكثير من المعلومات الشخصية مع شخص صادقته عبر شبكة (الإنترنت) أمرًا خطيرًا للغاية.

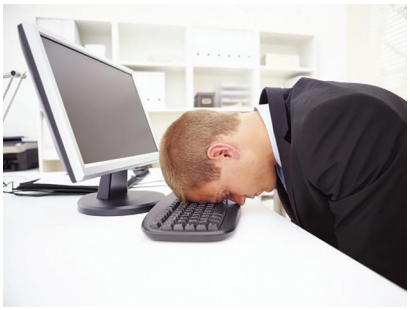
كما يمكن أن تتعرض أيضًا للمطاردات عبر (الإنترنت). وهو عبارة عن أحد أشكال التحرش على شبكة (الإنترنت)، ويطلق عليه، بشكل أكثر تحديدًا، المطاردات الإلكترونية. ولا يتواجد هذا النوع من التهديدات إلا على (الإنترنت) فقط، أو يمكن أن يبدأ من (الإنترنت)، ثم ينتقل إليك في العالم الخارجي. وفي كلا الحالتين، فإنه يسبب الكثير من الإزعاج. وبالإضافة إلى ذلك، يكون الكثير من ضحايا المطاردات الإلكترونية من صغار السن. وإذا حدث ذلك، يطلق على هؤلاء المطاردين اسم "مفترسو (الإنترنت)".



إهمال الأسرة والأصدقاء

يميل الأشخاص الذين يقضون ساعات طويلة في عزلة أثناء استخدام أجهزة (الكمبيوتر) إلى إهمال علاقاتهم مع الأشخاص الآخرين، خصوصًا الأسرة والأصدقاء. ومن خلال القيام بذلك، فإنهم أيضًا يهملون تطوير المهارات الهامة لديهم، وعند اللقاء مع الآخرين والحديث معهم، فإنهم غالبًا ما يعانون من صعوبات وعدم راحة.

الاضطراب في النوم



كما يمكن أن يعاني مستخدمي (الإنترنت) المندفعين من اضطرابات في النوم. وهي حالة دائمة تنجم عن مقاطعة دورة النوم الطبيعية. وهذا يعني أن الشخص يبقى مستيقظًا عندما يفترض به الخلود للنوم، وينام عندما يفترض به الاستيقاظ، أو قد لا ينام على الإطلاق. ويؤدي ذلك إلى خلق سلوكيات سلبية، وضعف الأداء في الدراسة أو العمل، وضعف الإنتاجية، والخلود للنوم في أوقات غير ملائمة.

التسوق القهري عبر (الإنترنت)

يُعد التسوق القهري عبر (الإنترنت) عادة أخرى سيئة تُكتسب من خلال قضاء وقت طويل على شبكة (الإنترنت). يقوم المتسوقون عبر (الإنترنت) بشراء الأشياء باندفاع أو بشكل عفوي. يجد هؤلاء الأشخاص أنفسهم يقدمون طلبات شراء لأشياء لم يخططوا لشرائها مسبقاً أو لم يفكروا إذا ما كانت ضرورية.

لذلك يجب علينا أن نكون على بينة من هذا الخطر حيث من الممكن أن يصبح شكلاً من أشكال الإدمان التي يمكن أن تؤدى إلى إضاعة المال وإنفاق مزيد من الوقت في تصفح (الإنترنت) لشراء أرخص السلع. كما قد يكون لديك صعوبة في إيجاد على راحة البال إذا ما صدفت تعاملات الإلكترونية سيئة التي قد تؤدى إلى فقدانك التركيز في مجالات حياتك الأخرى.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

إدمان ممارسة الألعاب على (الإنترنت)

تعد ممارسة الألعاب على (الإنترنت) شكلاً آخر من أشكال إدمان (الإنترنت). ويمكن أن يصل هذا الإدمان أيضًا إلى الأطفال صغار السن خصوصًا أولئك الذين لا تتم متابعتهم في المنزل وبدون أية متابعة من الوالدين أو أولياء الأمور.

وحسب بعض الدراسات، يمكن للألعاب التي يتم اتخاذ أدوار فيه أن تكون مفيدة نوعاً ما حيث يُطلب من اللاعبين التفكير بشكل نشط لحل الألغاز، أو للعثور على طرق لاتخاذ القرارات في مواقف صعبة.

في نفس الوقت، يمكن أن يتعلم المستخدمون أيضًا الانتباه، النشاط، والتعامل مع الإستراتيجية لحل المشكلات أو المواقف الصعبة. وعلى الرغم من هذه الفوائد، قد يكون للألعاب على (الإنترنت) تأثيرات سلبية يمكن أن تنجم من إنفاق الكثير من الوقت في اللعب، مثل:

- التحول إلى شخص غير اجتماعي. غالبًا ما يقضي اللاعبون على (الإنترنت) الكثير من الأوقات وهم "ملتصقون" للغاية بالألعاب. حيث يجدون صعوبة في التوقف لأنهم يكونون يرغبون في رؤية نتيجة الاستراتيجية الخاصة بهم، أو بسبب رغبتهم في الفوز بالمباراة. ويؤدي ذلك إلى قضاء الكثير من الوقت على (الإنترنت) مما يؤدي إلى فقد الرغبة بشكل تدريجي في الأشياء المحيطة وفي العلاقات مع الآخرين.
- في معظم الحالات، يستخدم اللاعبون – مثلهم في ذلك مثل الآخرين الذين يقضون الكثير من الوقت على (الإنترنت) – صناديق المحادثة أو أنظمة الرسائل الفورية للتواصل مع أصدقائهم على شبكة (الإنترنت). ونادرًا ما يقومون بإجراء المحادثات باستخدام المهارات الشفوية، ومع الوقت، يمكن أن تتدهور مهارات الاتصال الخاصة بهم.
- يمكن أن يواجه اللاعبون الذين لا يمتلكون المهارات الشفوية بسبب المشكلات المذكورة أعلاه مشكلات أخرى كما هو الحال عندما يتوجهون لإجراء مقابلات شخصية للحصول على وظائف أو عندما يقومون بإتمام مهمة في موقع العمل تتطلب منهم التعامل بشكل شفهي مع العملاء. فلن يكونوا مقنعين للغاية إذا استمروا في التلعثم والتأتأة في الكلمات بحثًا عن الأشياء التي يريدون قولها.
- غالبًا ما يميل الناس الذين يقضون الكثير من الوقت في المحادثات عبر (الإنترنت) إلى الاندفاع، وبالتالي يمكن أن يستجيبوا بسرعة لنظرائهم على شبكة (الإنترنت). ويمكن أن يؤدي ذلك بهم إلى الكتابة بسرعة، مما يؤدي إلى حدوث أخطاء في الهجاء واستخدام صيغ نحوية خاطئة، مثل استخدام الكلمة (your) مكان الكلمة (you're). ويمكن أن يمتد ذلك ليشمل الحياة الفعلية، ويمكن أن يؤدي إلى مشكلات عند كتابة أو الرد على أسئلة الاختبارات.
- يكون اللاعبون على (الإنترنت) عرضة للارتباك والحساسية الاجتماعية. ويصبحون عرضة لاستخدام لغة بذيئة عند الخسارة في الألعاب، أو عند الوقوع في مواقف يصعب حلها. هذا يشمل اللاعبين الكبار والصغار على حد سواء بسبب عدم معرفة/ظهور الهوية أثناء اللعب على (الإنترنت). وهذا الأمر ليس جيدًا، لأنه على الرغم من عدم القدرة على رؤية الشخص الذي نتفاعل معه، إلا أنهم مازالوا موجودين (أمام أجهزة (الكمبيوتر) الخاصة بهم) لذا يجب التعامل معهم كما لو كنا نتعامل معهم وجهًا لوجه في الحياة الفعلية.
- أخيرًا، فإن ممارسة ألعاب (الإنترنت) باستمرار يمكن أن يؤدي إلى الإضرار بالعلاقة الموجودة بينك وبين أفراد أسرتك أو أصدقائك. فقد تشعر أنه لا توجد هناك ضرورة لتقوية مهاراتك الاجتماعية، لأنك لن تحتاجها، بل سوف تعتمد على جهاز (الكمبيوتر) الخاص بك ليكون مصدر الاهتمام الوحيد في حياتك، مما يؤدي بك إلى نسيان أهمية إتمام أعمالك المدرسية والتوجه إلى أنشطة أخرى.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أعراض إدمان (الإنترنت)

هناك عدة علامات أو أعراض على إدمان (الإنترنت)، وقد تختلف من شخص لآخر حسب الظروف. إلا أنه لايمكننا تشخيص إدمان (الإنترنت) فقط من خلال معرفة عدد الساعات التي يقضيها الشخص أمام الحاسوب أو من خلال عدد الكلمات التي يكتبها لأن معظم ذلك قد يكون من أجل العمل.

ولكن بشكل عام يمكننا تحديد ما إذا كان شخصاً ما قد أدمن (الإنترنت) من خلال ملاحظة الأعراض التالية:

1. **إضاعة الكثير من الوقت عبر (الإنترنت) حتى لا يدرك الشخص الوقت الذي أمضاه**

هل اكتشفت بشكل متكرر أنك تمضي الكثير من الوقت أكثر مما خططت عبر (الإنترنت)؟ هل تحولت الدقائق العشر إلى ساعتين ؟ هل سبب لك إضاعة الكثير من الوقت عبر (الإنترنت) التأخر عن مواعيد المدرسة أو العمل؟ هل يزعجك كثيرًا إذا قاطعك أحد عندما تكون منهمكًا في الأنشطة الخاصة بك على (الإنترنت)؟

2. **إيجاد مشكلات عند إنجاز المهام بالعمل أو المنزل**

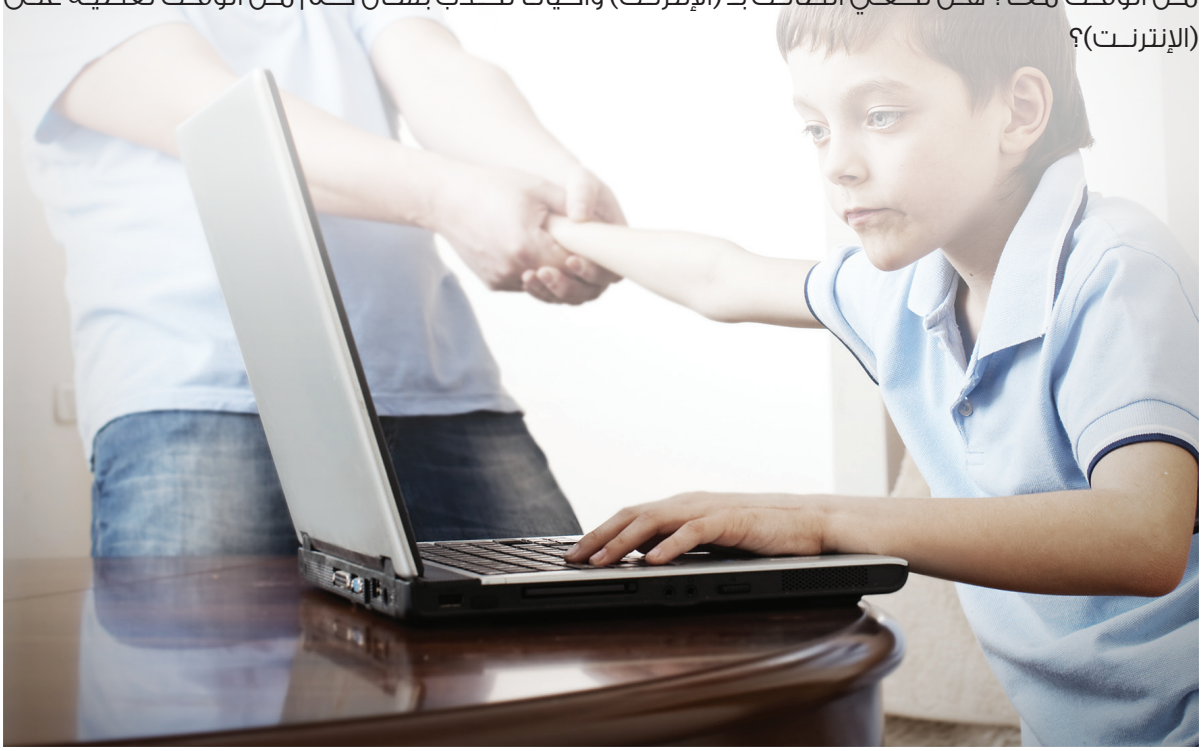
هل اكتشفت فجأة أنه لا يوجد طعام لتناول العشاء أو ربما أن الغسيل تراكم بكثرة وأنه ليس لديك سوى القليل من الملابس لترتديه؟ ربما بدون أن تشعر، بدأت في المكوث في المكتب لساعات طويلة لكي تنهي عملك لأنك كنت مشغولاً على (الإنترنت). أحياناً تبقى لمدة أطول لكي تتصفح (الإنترنت) بحرية.

3. **العزلة عن العائلة والأصدقاء**

هل تجاهلت حياتك الاجتماعية ولا تشعر بالذنب حيال ذلك؟ أو ربما لم تلحظ أن أصدقائك وأسرتك بدأوا في الانسحاب بعيداً عن حياتك؟ هل تشعر بأنه ربما لا يفهمك أحد في حياتك الحقيقية مثلما يفهمك أصدقائك في الحياة الإلكترونية ؟ هل بدأت في التفكير بأنه لا أهمية لأحد إذا كان «غير متصل» بقدر أهميته وهو «متصل»؟

4. **إخفاء الإحساس بالذنب والمشاعر الدفاعية حول استخدام (الإنترنت).**

هل تشعر بالتعب من إزعاج زوجتك لك بسبب قضاءك المزيد من الوقت على (الإنترنت) والقليل من الوقت معًا؟ هل تخفي اتصالك بـ (الإنترنت) وأحيانًا تكذب بشأن كم من الوقت تقضيه على (الإنترنت)؟



حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة (21): ارتفاع عدد مدمني التكنولوجيا من بين الشباب في الإمارات

أبو ظبي – لقد أصبح من الضروري البقاء متصلاً بشبكة (الإنترنت) طوال الوقت في ظل الوجود المتزايد للتقنية. يلاحظ السكان بأنه في الوقت الي تعود به التقنية بمجموعة من الفوائد، فإنها لا تأتي مع المشكلات الخاصة بها فقط. يتفق بعض الآباء على أن ممارسة الألعاب الإلكترونية مفيد لتنمية وتحسين قدرات أبنائهم التفكيرية. مثل تطوير القدرة على الهجاء، إثراء مهارات التفكير وتوسيع نطاق مفرداتهم.

يمكن لألعاب الحاسوب و(الإنترنت) أن يصل إلى حد الإدمان نتيجة قضاء الأطفال وقت أطول أمام (الكمبيوتر) على حساب الدراسة.

الشباب «المدمن»

في دراسة حديثة أجرتها مؤسسة الإمارات للأعمال الخيرية بعنوان «مستوى إدمان الشباب الإماراتي على تقنية المعلومات الحديثة، فرص، تحديات/المخاطر والحلول الممكنة لمستقبل أفضل» أوضحت أن ما يقرب من أربعة أشخاص ممن شملتهم الدراسة إما يتفقون أو يتفقون بشدة أنهم كانوا مدمنين باستخدام أدوات المعلومات الحديثة. أبرزت هذه النسبة الحاجة إلى مزيد من التدخل من المربين والوالدين، لضمان عمل الشباب على تطوير العادات الصحية عند استخدام وسائل التقنية الحديثة.

وتشير النتائج أنه ينبغي على القيادات التعليمية والوالدين إعطاء اهتماما كبيرا لتقنية المعلومات الحديثة، ليس من حيث استخداماتها المتعددة، بل من حيث امكانية سوء استخدامها أيضًا. لذا، ينبغي مساعدة الشباب في دولة الإمارات في تطوير عادات صحية عند تصفح (الإنترنت) أو استخدام هواتفهم المحمولة. قد يضطر البالغون إلى وضع حدود من خلال تعليم الشباب التحكم في وسائل تقنية المعلومات الحديثة وتطبيقاتها المتنوعة.

إعادة تدوير معدات أجهزة (الكمبيوتر) والتخلص منها بشكل صحيح

من الضروري أن تعرف كيف تتم إعادة تدوير الفضلات الناجمة عن جهاز (الكمبيوتر) الخاص بك بشكل صحيح. والسبب في ذلك هو أن جهاز (الكمبيوتر)، بما في ذلك إنتاجه، واستخدامه، والتخلص منه، يتسبب في تأثيرات كبيرة على البيئة.

إن إنتاج أجهزة (الكمبيوتر) يستلزم استخدام معادن نادرة وغيرها من المواد الخطرة المضرة بالصحة مثل الفضلات السامة التي يمكن أن تمثل خطرًا على صحتك. في حين أن أجهزة (الكمبيوتر) المستعملة يمكن أن توفر بعض العناصر المفيدة مثل: النحاس والرصاص، إلا أنها تحتوي أيضًا على مواد ضارة يمكن أن تضر بالبيئة وأن تمثل تهديدًا لها في حالة التخلص منها بشكل غير ملائم. من هذه الأجزاء الضارة:

- الزئبق الموجود في أنابيب (الفلورسنت).
- (الكادميوم) والسموم الأخرى المحتملة في بطاريات (الكمبيوتر) المحمول ومصادر الطاقة.
- الرصاص الموجود في الدوائر الكهرومغناطيسية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

يساعد استخدام أجهزة (الكمبيوتر) في خلق امتيازات بيئية، حيث إنها تتيح خلق مكاتب "لا تعتمد على الأوراق"، مما يقلل من عدد الأشجار التي يتوجب قطعها. كما أنها تسمح أيضًا بدراسة الأنظمة البيئية المعقدة وإتاحة التعليم البيئي بشكل أسهل. ومع ذلك، فمع نهاية عمر تلك الأجهزة، يمكن أن يصبح جهاز (الكمبيوتر) خطرًا بسبب المكونات الضارة التي يحتوي عليها.

وبالتالي، يجب أن تعلم ما يتوجب عليك القيام به لتقليل تأثير فضلات أجهزة (الكمبيوتر) على البيئة الخاصة بنا. وإليكم بعض الأشياء التي يمكن القيام بها:

استخدم (الكمبيوتر) فقط عند الحاجة

1. قم بشراء شاشة لا تستهلك الكثير من الطاقة أثناء عدم نشاطها.
2. لا تطبع المستندات إلا في حالة الضرورة فقط. اقرأ المستندات الخاصة بك على الشاشة، وإذا لزم الأمر، قم بتمريرها إلى الآخرين في شكل نسخ برمجية، وبدون طباعتها.
3. قم بإيقاف تشغيل جهاز (الكمبيوتر) بدلاً من تركه في حالة الاستعداد إذا كنت ستتركه لفترة زمنية طويلة.

التبرع

1. إذا كنت ترغب في شراء جهاز كمبيوتر شخصي أو جهاز كمبيوتر محمول جديد، فلا تحتفظ بجهاز (الكمبيوتر) القديم إذا كنت لا تنوي استخدامه.
2. وبدلاً من ذلك، يمكن تمرير جهاز (الكمبيوتر) إلى شخص آخر يمكن أن يستفيد منه، أو التبرع به لجمعية خيرية محلية. وتذكر تدمير محرك الأقراص الصلبة بشكل مادي حتى لا يتمكن الملاك الجدد من استعادة المحتويات الحساسة الموجودة عليه.

إعادة التدوير

1. يجب أن يتم تجميع الأوراق المستعملة التي لم تعد هناك حاجة إليها وإرسالها إلى مراكز إعادة التدوير. إذا كنت تقوم بطباعة صفحة اختبار، فاستخدم ظهر ورقة مستعملة.
2. قم بإعادة تدوير أجهزة (الكمبيوتر) القديمة، وكذلك خراطيش وحبر الطابعات.
3. ومع ذلك، إذا تعرض جهاز (الكمبيوتر) الخاص بك للضرر الذي لا يمكن إصلاحه، أو إذا لم يصبح ملائمًا للاستخدام، فيمكن إرساله إلى مركز إعادة التدوير المحلي. تحقق من إرساله إلى مركز إعادة التدوير مباشرة، إذا أمكن.

مشاريع مقترحة:

1. قم بعمل صور متحركة/(فيديو)/رسوم أو جداول بيانية لتوضيح فوائد/أضرار إعادة التدوير.
2. قم بعمل صور متحركة/(فيديو)/ رسوم أو جداول بيانية لتوضيح كيفية التخلص من القطع الإلكترونية بشكل صحيح.
3. قم بعمل صور متحركة/(فيديو)/ رسوم أو جداول بيانية لتوضيح كيفية حماية نفسك من الإدمان على (الإنترنت).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تمرين

1. **ما هما الخياران المتعلقان ببيئة العمل الصحية؟ (اختر خيارين)**

أ. تحسين الصحة والإنتاجية.

ب. فهم القدرات البشرية.

ج. فهم تدفق الهواء حول المكونات الصلبة.

د. خطر التعرض للإصابات المؤلمة والتي يمكن أن تسبب إعاقات.

ه. تحسين التفاعل البشري مع بيئة غرفة الدراسة.

2. **قم بتوصيل أنواع الإصابات المتعلقة بأجهزة (الكمبيوتر) بالصور ذات الصلة.**

متلازمة النفق الرسغي	متلازمة رؤية جهاز (الكمبيوتر)	أمراض العضلات والعظام
		

3. **يعاني إحسان من تصلب الظهر والرقبة والكتف. أي من عادات (الكمبيوتر) التالية تسببت في هذه المشكلات؟**

أ. النظر بعيدًا عن الشاشة لمدة عشر ثوان.

ب. ضبط وضعية الجلوس بين الحين والآخر.

ج. الهبوط/الترهل على مقعد (الكمبيوتر) لمدة (6) ساعات متواصلة.

د. الاستيقاظ أو القيام بأعمال بديلة مثل: عمل ملفات كل (30) دقيقة.

4. **قم بتحديد مشكلتين من مشاكل الإدمان المتعلقة بأجهزة (الكمبيوتر) (اختر خيارين).**

أ. المشاركة بشكل دائم في المنتديات المتعلقة بإدمان المخدرات.

ب. البحث بشكل مستمر عن رسائل البريد الإلكترونيّ الشخصيّ الواردة والصادرة.

ج. المشاركة بشكل مندفع في الشراء والبيع عبر العطاءات على (الإنترنت).

د. البحث بانتظام عن الصحف والمقالات من مواقع ويب مختلفة.

هـ. تكرار سرقة الأعمال لتقليدها في المهام باستخدام المقالات التي يمكن تنزيلها من شبكة (الإنترنت).

5. ما الطريقة المثلى للتخلص من بطارية جهازك القديمة؟

أ. إلقاءها بالبحر.

ب. إلقائها بمكان النفايات.

ج. إرسالها إلى موقع النفايات الإلكترونية.

د. حرقها بأي مكان في الصحراء.

الإجابة: 1. أ و 2. صورة 1 – متلازمة رؤية (الكمبيوتر)، صورة 2 – اضطراب العضلات والعظام، صورة 3 – متلازمة النفق الرسغي3 ج 4. ب و ج 5. ج

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

08 المحاسبة الإلكترونيّة

تناقش هذه الوحدة موضوع "إمكانية المحاسبة" عند استخدام التقنيات الرقمية في حياتنا اليومية. فهي تغطي حقوق وامتيازات مستخدمي شبكة (الإنترنت) والسلوكيات التي يجب التحلي بها.

وتعد المحاسبة مفهومًا معقدًا فيما يتعلق بالأخلاقيات والحوكمة. وهناك مصطلحات أخرى تحمل نفس المعنى مثل المسئولية وتحمل المسئولية واستحقاق اللوم وتحمل المسئولية، وهي جميعها مرتبطة ببعضها من خلال توقع تحمل المسئولية. ولتوفير الحوكمة، يجب أن تتوافر قواعد وسياسات للإجراءات أو الأنشطة المقبولة وغيرالمقبولة لصالح المستخدمين. وبالتالي فإن هذه الوحدة سوف تطلعك على مفهوم سياسة الاستخدام المقبول (AUP) في المنظمات والمؤسسات.

كما تلقي هذه الوحدة الضوء على أهمية الشعور بالمسئولية كمستخدم للتقنيات الرقمية. وهي مصممة لإعلام المشاركين بالمعضلات الأخلاقية فيما يتعلق بتبعات انتهاكات السياسات والقواعد المقبولة لنشر المحتويات على (الإنترنت)، خصوصًا في ضوء إطلاق (Web 2.0).

- اسياسة الإستخدام المقبول
- الملكية الفكرية
- التعدي على حقوق الملكية
- السرقة الأدبية
- البرامج المقرصنة

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أهداف التعلُّم

أهداف هذه الوحدة هي:

- تعزيز أهمية "تحمل المسؤولية" عند استخدام التكنولوجيا الرقمية.
- تقديم صور مختلفة من التعدى على حقوق الطبع والنشر.
- وصف تأثيرات التعدى على حقوق الطبع والنشر على الحياة.
- الإرشاد إلى الطرق الصحيحة لطلب التراخيص المحددة قبل استخدام الموارد الإلكترونية.

نواتج التعلُّم

في نهاية هذه الوحدة، سوف تكون قادرًا على:

- شرح أسباب أهمية المحاسبة والمساءلة في العالم الرقمي.
- توضيح الملكية الفكرية وحقوق النشر والاستخدام العادل والملكية العامة.
- شرح كيفية طلب أذونات محددة قبل استخدام الموارد الإلكترونية.
- شرح عواقب التعدي على الملكية الفكرية.
- وصف البرامج المقرصنة وكيفية تحمل المسؤولية على (الإنترنت).

قائمة المراجعة

البنود	التحصيل العلمي	قبل	بعد
1	أنا أدرك المقصود بالمحاسبة الإلكترونية.		
2	يمكنني التعرّف على سياسة الاستخدام المقبول.		
3	أنا أدرك ما هو المقصود بحقوق الطبع والنشر وتبعات انتهاك تلك الحقوق.		
4	أنا أدرك ما الذي يعتبر استخدامًا أخلاقيًا وما الذي لا يعتبر استخدامًا أخلاقيا للتقنيات.		

التعليمات:

بناءً على معرفتك السابقة والمعارف التي ستكتسبها بعد الانتهاء من قراءة هذهالوحدة.

يُرجى إكمال الاستبيان باستخدام المقياس التالي:

المقياس:

1. ليس لدي أدنى معرفة.
2. لدي معرفة محدودة.
3. لدي معرفة جيدة وأفهم ما قرأته.
4. كفؤ وأستطيع تطبيق كل ما تعلمته.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المحاسبة الإلكترونية - مسئوليات مستخدمي (الإنترنت) والسلوكيات المتوقعة منهم

تدور التقنيات في إطار مساعدة البشر. ويحتاج المجتمع إلى المزيد من التقنيات المتطورة لحل المشكلات اليومية في عالم يتسم بالعولمة، يتضائل فيه الوقت والمساحات، والموارد بشكل دائم، في نفس الوقت الذي تتزايد فيه الفرص.

وتعد التقنيات الرقمية هي الصفة المشتركة لتحقيق النجاح في القرن الحادي والعشرين. ويستخدم المزيد والمزيد من الأشخاص شبكة (الإنترنت) في الأنشطة اليومية الخاصة بهم، بل أصبح بعض الناس يعتمدون عليها بشكل زائد عن الحد حاليًا. إن تبني التقنيات أمر حتمي، ويحتاج الأطفال إلى معرفة كيفية استخدامها، كما يجب على الكبار التكيف مع الانتشار الكثيف لها. وكما يقول ستيوارت براند.

> "عندما تمر عليك تقنية جديدة، فإما أن تكون جزءًا يساعد على مرور تلك التقنية، وإما أن تكون جزءًا من الطريق".

إلا أن القليل للغاية منا يدركون امتيازات وحقوق مستخدمي شبكة (الإنترنت)، والسلوكيات المتوقعة منهم. وتتعلق الحقوق والامتيازات بشدة بأن تكون جزءًا من مجموعة. وتخضع السلوكيات المتوقعة من مجتمع عادي أو من مجتمع رقمي لسيطرة قواعد ولوائح يجب أن يلتزم بها كل عضو.

فَهم المحاسبة الإلكترونيّة

تعد المحاسبة مفهومًا معقدًا مرتبط بالأخلاقيات والإدارة. إنها مرادفة لمصطلحات مثل المسؤولية والملائمة التي تكون مصحوبة بتوقع المسؤولية حيال كل إجراءات نتخذها.

بعض تعريفات للمحاسبة الإلكترونية:

- مفهوم يتعلق بالأخلاقيات والحوكمة لاستخدام التقنيات الرقمية.
- حمل نفس معنى المسؤولية، وتحمل المسئولية، واستحقاق اللوم، وتوقع إعطاء الحساب إلى المستخدمين.

> "الامتيازات والحرية الممنوحة لكل مستخدمي التقنيات الرقمية، والتوقعات السلوكية التي تأتي معها".
>
> إم ريبل وجي بايلي – المواطنة الرقمية في المدارس، ISTE 2007.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

ظهور تقنيات (الويب 2) يخلق الحاجة إلى سياسة

شبكة (الإنترنت). على سبيل المثال، تتيح تقنية (Web 2.0) أن تكون الاتصالات أكثر تفاعلية، وأكثر مزامنة، وأن تكون في الوقت الفعلي، من خلال تفعيل إمكانية إنشاء ومشاركة المحتويات للجماهير. كما أثرت الوسائط الرقمية وتطبيقات الهواتف المحمولة الشاملة بشكل عميق على توصيل ومشاركة المعلومات بيننا.

خلافًا لتكنولوجيا الموقع القديم الذي كان به الكثير من القيود، يسمح (ويب 2.0) لتوليد وتوزيع المحتوى (بيانات أو نصوص أو صور أو تسجيلات صوتية) بحرية تبادلها وإعادة استخدامها.

أدى انتشار الوصول إلى الوسائط الرقميّة والمنتديات والمدونات والشبكات الاجتماعية والهاتف المحمول وتكنولوجيا الأقمار الصناعية إلى خلق فرص عمل جديدة وتهديدات. كما أدّى هذا الانتشار لوسائل الإعلام الرقميّة على المستوى العالميّ أيضًا إلى خلق قضايا جديدة مثل الخداع الإلكترونيّ والتعدي الإلكترونيّ وسرقة الهُوية والتجسس والانتحال.

ويتطلب وضع القدرة على التعبير عن الأفكار والآراء في مختلف أرجاء العالم في يد المستخدمين وجود إرشادات تحكم "عمليات النشر التي تتسم بالمسؤولية". ويكون هذا الأمر صحيحًا بشكل خاص عندما توفر شبكة (الإنترنت) شعورًا بعدم الكشف عن الهوية يخلق تأثيرات نفسية تعرف باسم "التخلص من الكبت على (الإنترنت)".

وقد اقترح جون سولير، وهو عالم نفسي في جامعة (رايد) في (لورنسفي)، (نيو جيرسي)، أن العديد من العوامل النفسية يمكن أن تؤدي إلى التخلص من الكبت على (الإنترنت)، من بينها ما يلي:

- عدم الكشف عن الهوية والاسم المستعار على (الويب).
- عدم قدرة الآخرين على رؤيتك.
- الفترة الزمنية الفاصلة بين إرسال رسالة بريد إلكتروني والحصول على الرد.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة (22): الانتقاد ثم التفكير بعد ذلك : أدلة جديدة على سوء استخدام البريد الإلكتروني

اتهم اللندنى البالغ من العمر (47) عامًا بالاعتداء عندما هاجم هو وصديقه رجل أمطره بوابل من الشتائم بغرفة للدردشة باستخدام مقبض فأس وسكين. وصفت جريدة تايمز اللندنية الحادث بأنه: "هجوم الغضب الإلكتروني البريطانى الأول".

يدرس الحقل الناشئ من علم الأعصاب الاجتماعية ما يدور في العقول والأجسام عندما يتفاعل شخصان ويكتشفا كيف يحدث الغضب. وطبقًا لبحث قامت به (جنيفر بيير)، عالمة نفسانية بجامعة (كاليفورنيا) (بدافس)، تمنع تفاعلات وجهًا لوجه التسرع في اتخاذ الإجراءات التي من شأنها أن تزعج الطرف الآخر. يختار وينفذ العقل الدوافع استنادًا إلى المعلومات الاجتماعية التي يتلقاها، على سبيل المثال، تغير نبرة الصوت.

ومع ذلك، يوجد قلة في هذه المعلومات والكلمات في البريد الإلكتروني التي يمكن أن يُساء قراءتها كنتيجة لذلك. وعندما يكتب أحدهم عندما يكون ثائرًا، يكون هذا الشخص أكثر عرضة لكتابة رسائل غير مناسبة ويضغط على زر "إرسال" قبل أن يفكر أكثر وما يدفعه للضغط على "تجاهل". ويعرف هذا بالغضب.

قد يكون استبدال الرسائل المكتوبة بـ (الفيديو) حلاً فقد يساعد الحصول على رسالة كاملة بالمعلومات الاجتماعية اللازمة على تقليل دافع الغضب.

New York Times, 20 February, 2007

http://www.nytimes.com/2007/02/20/health/psychology/20essa.html

- الإحساس المبالغ فيه بالذات بسبب الوحدة وغياب أي شكل للسلطات على شبكة (الإنترنت).

وأفادت الأنباء الواردة من جميع أنحاء العالم بالعديد من الحالات ذات الصلة بالاستخدام غير الملائم للتكنولوجيا الرقمية وتطبيقاتها بين المستخدمين. لذا، هناك حالة تكون عرضة أكثر للمساءلة بشأن الاستخدام اليومى للتكنولوجيا الرقمية، لا سيما بين الشباب.

من أجل معالجة هذه القضايا، يجب أن تكون هناك قواعد وسياسات للأعمال المقبولة وغير المقبولة، أو الأنشطة التي تكون لصالح المستخدمين. وهكذا، فإن المساءلة تقدم لك مفهومًا لسياسة الاستخدام المقبول في المؤسسات والمعاهد.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

فهم سياسة الاستخدام المقبول (Acceptable Use Policy – AUP)

هل فكرت من قبل في إمكانية السماح بالهواتف المحمولة في غرف الدراسة أثناء ممارسة أنشطة التعليم والتعلم.

هل تعتقد أنه يجب السماح بالتسجيلات الصوتية أو تسجيلات (الفيديو) أثناء التعليم؟

هل يكون من المناسب توفير إمكانية الوصول عبر شبكة (Wi-Fi) للطلبة في غرف الدراسة، أم يفضل أن يتاح هذا الوصول في المناطق العامة مثل: المكتبة، أو منطقة الانتظار، أو ملعب ممارسة الرياضة، أو الردهة، أو المقصف، أو مجمع المدارس؟

ما الذي يجب أن نفكر فيه قبل اتخاذ قرار؟ يجب أن نقوم بتقييم المزايا والعيوب والتوصل إلى قرار حيال ما هو مقبول.

يجب أن تكون لدينا سياسة استخدام مقبول للتقنيات لمواجهة هذا الأمر.

لم تكن المشاركة في وضع سياسات تقنيات المعلومات والاتصالات (ICT) أولوية لمعظم الأشخاص، حتى أولئك الذين ربما قد شاركوا في السياسة العامة في المناطق الأخرى.

ومع ذلك، ومع تقديم التقنيات الحديثة تقريبًا كل يوم وتزايد استخدام تلك التقنيات في حياتنا اليومية، تتزايد ضرورة توافر نوع من أنواع السياسات التي تحكم استخدام تلك التقنيات في تعاملاتنا اليومية وفي أعمالنا.

من الضروري بالنسبة للمدرسين وأولياء الأمور وموفري الرعاية ألا يخلطوا بين استخدام التقنيات بمهارة مع القدرة على إدراك وتجنب المخاطر، فثقافة شبكة (الإنترنت) وتقنيات المعلومات والاتصالات، لسوء الحظ، لا تعتبر مرادفًا لأمان شبكة (الإنترنت) وتقنيات المعلومات والاتصالات..

وتهدف السياسات والإرشادات المتعلقة بالتقنيات إلى توفير هيكل وعمليات مترابطة لتحسين الفعالية من أجل تحقيق المزيد من الإنتاجية، إلا أنها غالبًا ما أصبحت مصدرًا للمراجع للإجراءات القانونية ولفرض القانون. يجب أن يتم تصميم السياسة بحيث تكون وسيلة تمكين، وليس لكي تكون وسيلة منع فيما يتعلق بتقنيات المعلومات والاتصالات. فكونها وسيلة تمكين، فإنها يجب أن توفر إرشادات تزيد من الفاعلية والإنتاجية من خلال الاستخدام الملائم للتقنيات.

وهذا هو السبب الذي يجعل لدينا سياسة الاستخدام المقبول (Acceptable Use Policy – AUP).

تعريف سياسة الاستخدام المقبول

هناك عدة تعريفات مختلفة مقبولة بشكل واسع الإنتشار لسياسة الاستخدام المقبول. وربما كان أكثر هذه التعريفات شهرة هو:

"مجموعة من القواعد التي يتم تطبيقها من قبل مالك أو مدير شبكة، أو موقع ويب، أو نظام أجهزة كمبيوتر كبير، تحد من الطرق التي يمكن استخدام الموقع أو الشبكة بها".

وتتم كتابتها للشركات والمنظمات والمؤسسات والجامعات والمدارس وموفري خدمات (الإنترنت) (ISP) ومسؤولي مواقع (الويب) لتوفير الحماية ضد الإجراءات القانونية التي يقوم بها المستخدمون ولإتاحة فرض القانون.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

عناصر سياسة الاستخدام المقبول

ما يستلزم وجود سياسة استخدام مقبول جيدة؟ ينبغي أن تتكون سياسة الاستخدام المقبول الجيدة من العناصر التالية:

1. **بيان الفلسفة.**
2. **بيان استخدامات ومزايا مرفق الخدمة.**
3. **مدونة السلوكيات.**
4. **تبعات الانتهاكات.**
   - التحذيرات المتعلقة بالمشكلات، سواء المكتوبة أو الشفوية.
   - تعليق امتيازات النشر الخاصة بمجموعة الأخبار للعضو.
   - تعليق حساب المستخدم.
   - إنهاء حساب المستخدم.
   - فرض تكاليف إدارية و/أو تكاليف إعادة التنشيط على الأعضاء.
   - فرض الإجراءات القانونية لمنع ارتكاب الانتهاكات.
5. **خطابات الموافقة.**
6. **إخلاء المسئولية.**

تطوير سياسة الاستخدام المقبول

يعتبر تطوير سياسة أمرًا ضروريًا لأية منظمة، إلا أنك لا يجب أن تبدأ من الصفر. فهناك الكثير من السياسات المتاحة التي يمكن الرجوع إليها والاختيار من بينها. إليكم أدناه بعض الخطوات البسيطة التي يمكن استخدامها لتطوير سياسات الاستخدام المقبول الخاصة بالمنظمة أو المؤسسة أو الشركة أو المدرسة التي تتبعها.

1. قم بتشكيل فريق يتكون من كل الوحدات أو الإدارات في المنظمة، وحدد الحاجة وراء امتلاك سياسة الاستخدام المقبول والهدف منها.
2. ابحث على (الويب) عن عينات لسياسات الاستخدام المقبول للمنظمات المشابهة.
3. قم بمقارنة سياسات الاستخدام المقبول من خلال تحديد العناصر الأكثر عدلاً والأكثر ملائمة لأهداف منظمتك/مؤسستك.
4. قم بتطوير سياسة استخدام مقبول جديدة من أفضل المميزات المتاحة في سياسات الاستخدام المقبول الموجودة.
5. قم بتوضيح كل تبعات عدم الالتزام بسياسة الاستخدام المقبول التي يتم تبنيها.
6. احصل على آراء الخبراء من المحترفين، مثل: المحامين.
7. اطلب من كل المساهمين التصديق على السياسة. قم بالإعلان عن السياسة لكل من في المنظمة، ثم ابدأ في فرضها.
8. إعلان ذلك للجميع في المؤسسة ومن ثم تطبيقه.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

مثال لسياسة استخدام مقبول

سياسة استخدام مقبول للجامعات

حقوق الطبع والنشر والتراخيص

جامعة (ستانفورد)

سياسة استخدام (الكمبيوتر) والشبكة

- يجب على مستخدمي (الكمبيوتر) احترام حقوق الطبع والنشر وتراخيص البرمجيات ومواد الترفيه والوثائق المنشورة وغير المنشورة وغيرها من المعلومات الرقمية المحمية بصفة قانونية.
- نسخ أية مادة محمية بموجب حقوق الطبع والنشر لا يمكن نسخها باستثناء ما هو منصوص عليه تحديدًا من جانب صاحب حقوق الطبع والنشر أو بخلاف ذلك ما يسمح قانون حقوق الطبع والنشر به. قد لا يتم نسخ المواد المحمية في أو من أو من جانب أية منشأة أو نظام جامعي إلا بناءً على ترخيص ساري المفعول أو ما هو مسموح به بموجب قانون حقوق الطبع والنشر.
- عدد المستخدمين المتزامنين يجب أن تعالج مسألة عدد وتوزيع نسخ مواد حقوق الطبع والنشر بالطريقة التي لا يتجاوز فيها عدد المستخدمين في وقت واحد بقسم ما عدد النسخ الأصلية المشتراة من قِبَل هذه الإدارة، ما لم ينص على خلاف ذلك بعقد الشراء أو ما يسمح به بخلاف ذلك بموجب قانون حقوق الطبع والنشر.
- حقوق الطبع والنشر – ويجب استخدام كل المعلومات حقوق الطبع والنشر (النصوص والصور والرموز والبرامج و(الفيديو) والصوت،... الخ) التي تم استردادها من موارد (الكمبيوتر) أو الشبكة بالتوافق مع حقوق الطبع والنشر المعمول بها والقوانين الأخرى. يجب أن تعزى المواد المنسوخة بشكل صحيح. الانتحال (السرقة الأدبية) من المعلومات الرقمية يخضع لنفس العقوبات التي تطبق على الانتحال في أي وسيلة أخرى.

سياسة الاستخدام المقبول لجامعة (براون)

- ملزمة بموجب كافة القوانين المحلية والخارجية والاتحادية.
- ملزمة بموجب كافة قوانين حقوق الطبع والنشر والتراخيص المعمول بها. حررت جامعة (براون) اتفاقيات أو عقود قانونية لعدد من مواردنا في الشبكة والبرامج الذي يتطلب استخدام كل فرد لها الامتثال لتلك الاتفاقيات.
- يراعى قانون حقوق الطبع والنشر باعتباره ينطبق على الموسيقى و(الفيديو) والألعاب والصور والنصوص ووسائل الإعلام الأخرى سواء في الاستخدام الشخصي وفي انتاج المعلومات الإلكترونية. السهولة التي يمكن نسخ المواد الإلكترونية بها، وتعديلها وإرسالها عبر (الإنترنت) يجعل من المواد الإلكترونية عُرضة لدخول غير مصرح به، وغزو التعدي على الخصوصية وحقوق النشر.
- لا تستخدم، أو تنسخ، أو توزع أعمال محمية بحقوق الطبع والنشر (بما في ذلك على سبيل المثال لا الحصر على رسومات صفحة ويب، وملفات الصوت ومقاطع الأفلام، والعلامات التجارية والرسوم والبرامج والشعارات) إلا إذا كان لديك الحق القانوني في استخدام ونسخ وتوزيع، أو خلاف ذلك الاستفادة من العمل المحمي بحقوق الطبع والنشر. وبذلك يمكن أن توفر أساسًا لاتخاذ إجراءات تأديبية، التقاضي المدني والمقاضاة الجنائية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الخصوصية والحقوق الشخصية

جامعة (ستانفورد)

سياسة استخدام (الكمبيوتر) والشبكة

- الاستخدام – يجب على مستخدمي (الكمبيوتر) احترام حقوق مستخدمي (الكمبيوتر) الآخرين. توفر معظم أنظمة الجامعة آليات لحماية خصوصية المعلومات من فحصها من قِبَل الآخرين. تعتبر محاولات الالتفاف حول هذه الآليات من أجل الوصول غير المصرح به إلى نظام أو معلومات شخص آخر انتهاكًا لسياسة الجامعة وقد يشكل انتهاكًا للقانون الواجب التطبيق. يسمح لمسئولي النظام المفوضين بالوصول إلى ملفات مستخدمي (الكمبيوتر) في أي وقت من أجل أغراض الصيانة. يقوم مسئولو النظام بالإبلاغ عن الأنشطة المشتبه فيها وغير المشروعة أو غير اللائقة إلى السلطات المختصة.
- الاستخدام المحظور – يحظر الاستخدام – استخدام الحاسب الآلي في الجامعة، شبكة أو مرافق الاتصالات الإلكترونية مثل: البريد الإلكتروني أو الرسائل الفورية، أو أنظمة ذات وظائف مماثلة لإرسال أو عرض أو تحميل المواد الاحتيالية أو مواد التحرش او رسائل تهديد أو الرسائل أو المواد الأخرى التي تشكل انتهاكًا للقانون أو لسياسة الجامعة، ويحظر مثل هذه الحالات التي قد تتسبب في خلق بيئة عدائية داخل البيئة الأكاديمية أو العملية.
- القوائم البريدية يجب على المستخدمين احترام غرض ومواثيق القوائم البريدية (للكمبيوتر) (بما في ذلك مجموعات الأخبار المحلية وأخبار الشبكة والنشرة الإخبارية اللوحات). مستخدم القائمة البريدية الإلكترونية مسئول عن تحديد الهدف من القائمة قبل إرسال رسائل إلى أو تلقي رسائل من القائمة. سيتم عرض المشتركين في القائمة البريدية الإلكترونية باعتبارهم طالبين أي مواد تم تسليمها بالقائمة طالما أن المواد تتفق والغرض من القائمة. سيتم عرض الأشخاص الذين يرسلون إلى القائمة البريدية أية مواد لا تتفق مع غرض القائمة باعتبارهم قاموا بإرسال مواد غير مرغوب فيها.
- الإعلانات – بصفة عامة، يجب ألا تستخدم مرافق الاتصال الإلكتروني بالجامعة لنقل الإعلانات التجارية أو الشخصية أو الالتماسات أو العروض الترويجية (انظر الاستخدام التجاري أدناه). وقد تم تعيين بعض لوحات الإعلانات العامة لبيع سلع من قِبَل أعضاء مجتمع (ستانفورد)، ويمكن استخدامها على النحو الملائم، وفقًا للغرض المعلن للقوائم.
- المعلومات الخاصة بالآخرين – يجب على المستخدمين عدم طلب أو تقديم معلومات أو الحصول على نسخ أو تعديل ملفات بيانات أو البرامج أو كلمات السر أو المواد الرقمية الأخرى الخاصة بالآخرين عن عمد دون الحصول على إذن خاص من هؤلاء المستخدمين الآخرين.
- الخصوصية – قانون قابلية التأمين الصحي والمحاسبة لعام 1996م، ويتضمن المعايير والقواعد المنظمة لمعالجة أنشطة المعلومات الصحية التي يمكن تحديدها بشكل فردي (لمزيد من المعلومات الرجوع إلى المسئول عن خصوصية الجامعة).

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الخصوصية والحقوق الشخصية

سياسة الاستخدام المقبول لجامعة(براون)

- من المتوقع احترام جميع مستخدمي موارد (الكمبيوتر) والشبكة بالجامعة للخصوصية والحقوق الشخصية للآخرين.
- ممنوع الوصول إلى أو نسخ البريد الإلكتروني أو البيانات، أو البرامج، أو الملفات الأخرى الخاصة بمستخدم آخر، دون إذن خطي من رئيس مسئولي أمن المعلومات بجامعة براون، الذي يلتزم بالإجراءات المذكورة في الوصول إلى الحسابات والمعلومات في حالة الطوارئ.
- عليك بالمهنية والاحترام عند استخدام أنظمة الحاسب الآلي للتواصل مع الآخرين، فلا يُسمح باستخدام الموارد الحاسوبية للتشهير أو قذف أو التحرش بشخص آخر وقد يؤدي مثل هذا إلى التأديب الجامعي إضافة إلى الإجراء القانوني من قِبَل هؤلاء المستفيدين بهذه الإجراءات.

سياسة الاستخدام المقبول لمؤسسة

التعليمات التالية تم تصميمها لحماية مصالح خدمات شركة اتصالات (للإنترنت) وعملائها. قد يؤدي انتهاك هذه التعليمات إلى إيقاف أو فصل خدمات اتصالات (للإنترنت). تحتفظ شركة الإمارات للاتصالات أيضاً بالحق في إقامة دعوى قضائية في حالة حدوث مثل هذه الانتهاكات.

يمتنع جميع عملاء انترنت اتصالات عن المشاركة أو المساعدة أو المساهمة في كافة أو أى من الأنشطة المحظورة التالية :

- نشر أى إعلان أو إغراءات تجارية إلى أية مجموعة أخبار أو قائمة بريدية إلكترونية أو منتدى.
- نشر المقالات للمجموعة الإخبارية دون الامتثال بميثاق مكتوب لتلك المجموعات الإخبارية.
- نشر أية مواد حقوق طبع ونشر لأية مجموعة إخبارية أو منتدى أو قائمة بريدية دون الحصول على إذن صريح من صاحب حقوق الطبع.
- تزوير معلومات العنوان أو انتحال صفة مستخدم آخر أو تزوير معلومات المستخدم (مثل استخدام أسماء وهمية أو غير مكتملة) في البريد الإلكتروني أو بالنشر لأى مجموعة إخبارية، أو منتدى أو قائمة بريدية بريدية.
- إرسال رسائل بريد جماعية غير مرغوب فيها (رسائل بريد غير مرغوب فيها) لمستخدمي (الإنترنت) سواء كان ذلك على شبكة إنترنت اتصالات أو أى مزود آخر لخدمة (الإنترنت).
- نشر رسالة بريد إلكتروني خاصة لأية مجموعة إخبارية أو منتدى أو قائمة بريدية دون إذن صريح من تلك الجهة.
- نشر أو إرسال بريد إلكتروني لأى شخص لا يرغب في تلقيه في حالة إذا ما طلب المستقبِل التوقف عن تلقى البريد الإلكتروني.

الانخراط في أى من الأنشطة سالفة الذكر باستخدام الخدمة من مزود آخر، دون توجيه مثل هذه الأنشطة من خلال حساب انترنت اتصالات باعتباره بريد منسدل للاستجابات.

هذه المبادئ التوجيهية جزأ لا يتجزأ من أى عقد اتصالات لتوفير خدمات (الإنترنت). التأخير او الفشل في تطبيق أى من المذكور أعلاه، لا يعتبر تناز عن هذه المبادئ التوجيهية كما لا يؤثر على صحتها أو حق اتصالات فيما بعد في تنفيذ كافة أو أى من هذه المبادئ التوجيهية المذكورة أعلاه.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

دراسة حالة (23): تستخدم إحدى المدارس الكاميرات في أجهزة (الكمبيوتر) المحمول للطلاب للتجسس عليهم في المدرسة والمنزل

قد تم رفع دعوى قضائية ضد إحدى المدارس التي كانت تعمل على تشغيل الكاميرات في أجهزة (الكمبيوتر) المحمولة للطلاب المسلّمة لهم للتجسس عليهم وعلى عائلاتهم.

عرضت هذه المسألة عندما تم تأديب أحد الطلاب لقيامه بسلوك "غير لائق في منزله". استخدم النائب الأساسي الصورة عن طريق كاميرا (ويب) باعتبارها دليل. أظهرت معلومات تم تحديثها حول هذه الحالة أن المنطقة التعليمية تقر بأن أجهزة (لاب توب) الطلاب تحتوي على برنامج لتفعيل كاميرات (الويب) الخاصة بهم سرًا، إلا أنه نفى الجريمة.

بوينج بوينج: الثقافة والعلوم التكنولوجية، 17 فبراير 2010

http://boingboing.net/2010/02/17/school-used-student.html

أهمية الحصول على سياسة الاستخدام المقبول

سياسة الاستخدام المقبول مهمة حيث أنها بيان للسياسة العامة حول الاستخدام المناسب للتكنولوجيا داخل المنظمة. والمقصود بها أن توفر المبادئ التوجيهية التي تعزز الاستخدام العادل للموارد المشتركة. وهي لا تحمي المؤسسات ومزودي التكنولوجيا بوضع قواعد للسلوك فحسب، بل تحميهم أيضاً من الإجراءات القانونية. بالحصول على سياسة الاستخدام المقبول في مكان ما، يمكن تنفيذ إجراءات إذا ما وُجدت أية انتهاكات لتلك السياسة.

باختصار، تُعتبر سياسة الاستخدام المقبول طريقة لتعليم طاقم العمل والأعضاء والكلية والطلاب بأن يكونوا مسؤولين عن جميع الأعمال الرقمية. إنها مسئولية، من خلال احترام حقوق الملكية الفكرية، عن تقدير حقوق الطبع والمساواة في استخدام المواد من المجالات العامة.

إنها وثيقة حية يمكن تحسينها مع مرور الوقت. وينبغي على الجميع معرفة سياسة الاستخدام المقبول خاصة من خلال خطاب الشكر وخطاب الموافقة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

احترام أصحاب الملكية الفكرية وحقوقهم

غالبًا ما تعني الحقوق الامتيازات التي يحصل عليها الشخص نظير المشاركة في مجموعة. وهي تشتمل على استخدام الموارد المشتركة التي تحكم القواعد واللوائح الخاصة بالمشاركة في المجموعة. فإذا كنت طالبًا في مدرسة أو في إحدى كليات الجامعة، فأنت تخضع لحقوق وامتيازات عضوية المدرسة أو الكلية والجامعة. ومن الافتراضات العامة العمل بما يتوافق مع قواعد المدرسة أو الكلية والجامعة. وفي حالة عدم التزامك بسياسة الاستخدام المقبولة في المجموعة، تمتلك المدرسة أو الكلية والجامعة الحق في توجيه اللوم إليك.

نظرًا لأن الجميع لهم حقوق، فمن الضروري احترام حقوق الجميع طالما أنها تتوافق مع سياسة الاستخدام المقبول للمجموعة. ويشتمل ذلك على حقوق حماية الإبداعات والأفكار، وهو ما يعرف بصفة عامة باسم حقوق الملكية الفكرية.

فهم الملكية الفكرية (Intellectual Property - IP)

يغطي مصطلح الملكية الفكرية (IP) مجموعة من وسائل الحماية القانونية لإبداعات العقل البشري. وتوفر الملكية الفكرية حافزًا للإبداع، حيث يمكن أن يستفيد مالك تلك الحقوق منها للحصول على فوائد تجارية من الجهات المهتمة بالأمر والذين يرغبون في استخدام هذا العمل الذي أبدعه صاحب الحقوق.

ونحن قد نرغب بالقطع في الحصول على نفس تلك الحقوق ووسائل الحماية عند الإبداع والابتكار، وبما يؤدي إلى امتلاكنا لحقوق الملكية الفكرية. كما أننا نقدر أن يقر الآخرون بحقوق الملكية الفكرية الخاصة بنا، كما سنقدر بشكل أكبر أن يتم منحنا تعويضات مقابل استخدام هذا الإبداع. ويمكن أن تكفي معظم الإبداعات في العالم الأكاديمي في حالة الاعتراف بالعمل الأصلي وتقديره بالشكل الملائم.

تتزايد التطورات فيما يتعلق بالتقنيات الرقمية وهناك العديد من نقاط الالتقاء التقنية التي يتم التوصل إليها. على سبيل المثال، كان من المعتاد أن تكون الكاميرا الرقمية والهواتف المحمولة منتجين مختلفين، إلا أنهما الآن تم دمجهما في منتج واحد. فتقريبًا كل الهواتف المحمولة حاليًا تحتوي على كاميرات مدمجة بها. وتتيح الوسائط الاجتماعية للمستخدمين أن يقوموا بعمل المحتويات على شبكة (الإنترنت). ويستخدم المستخدمون بشكل مكثف الآن تطبيقات الشبكات الاجتماعية، ويمكن الآن نسخ المواد الرقمية من صور وصوت ومقاطع فيديو، ونقل تلك المواد وتعديلها ولصقها بكل سهولة في مستند جديد وادعاء أنها إبداع فكري جديد.

إن استخدام التقنيات الرقمية سواء في العمل أو أثناء وقت الفراغ بسهولة يجعلك تدخل ضمن إطار المواطنين الرقميين. وكونك مواطنًا رقميًا، يكون لديك أنت أيضًا حقوق ومسئوليات تجاه المجموعة الرقمية الخاصة بك. ومع الأخذ في الاعتبار أن كل احتياجات البنية التحتية الخاصة بك الآن تتاح من قبل المجتمع، أو المدرسة، أو الكلية، أو الجامعة، أو الولاية ، أو الحكومة، أو الدولة التي تنتمي إليها، يمتلك كل منا الحقوق والمسئوليات تجاه المجتمع بشكل عام.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

حقوق الطبع والنشر

أهداف امتلاك حقوق الطبع والنشر هي:

- توضيح أشكال انتهاكات حقوق الطبع والنشر.
- توضيح كيفية تأثير الانتهاكات على كل فرد وعلى الأوجه المختلفة للحياة (على سبيل المثال الاقتصاد).
- طلب إذن محدد قبل استخدام الموارد الإلكترونية.

وقبل أن يتسنى لنا مناقشة انتهاكات حقوق الطبع والنشر، يجب أن نفهم ماهية حقوق الطبع والنشر أولاً. وما هي الحقوق التي توفرها حقوق الطبع والنشر؟

تدوم مدة حماية حقوق الطبع والنشر مدى حياة المؤلف بالإضافة إلى 70 عامًا أخرى. أما الأعمال الأخرى التي لم تعد تخضع لحماية حقوق الطبع والنشر فتعتبر "في إطار النطاق العام".

وفي حالة الأعمال "التي يتم تأجير أشخاص لإتمامها"، حيث يتم تنفيذ الأعمال الإبداعية أثناء العمل كموظف، يعتبر صاحب العمل وليس الموظف هو المؤلف لتلك الأعمال وصاحب حقوق الطبع والنشر لها. ويمكن نقل الحقوق الحصرية للمالك إلى جهة أخرى من خلال موافقة مكتوبة وموقعة من مالك حقوق الطبع والنشر.

تعد حماية الأعمال الخاصة بك من خلال حقوق الطبع والنشر الجزء الأسهل فيما يتعلق بالكتابة، حيث تتم حماية أعمالك من اللحظة التي تبدأ في تسجيلها وكتابتها فيها. ولا يجب أن تقوم بتسجيل حقوق الطبع والنشر كي تسري تلك الحقوق. فيكفي كتابة إشعار بحقوق الطبع والنشر على المستند الخاص بك. فعلى سبيل المثال، يكفي كتابة العبارة "حقوق الطبع والنشر © محفوظة لـ (اسمك).

التعدي على حق الطبع والنّشر

ما الذي يمكن اعتباره انتهاكًا؟ يعرف ذلك أيضًا باسم انتهاك حقوق الطبع والنشر. وهو عبارة عن استخدام غير مرخص به أو محظور لأعمال تخضع لملكية حصرية لحقوق الطبع والنشر، مثل إعادة إنتاج، أو توزيع، أو تعديل تلك الأعمال لإنتاج أعمال مشتقة منها.

وبالنسبة للوسائط الرقمية والمرئية، يشار إلى إعادة الإنتاج والتوزيع غير المرخص بهما أيضًا بشكل عام باسم القرصنة. ومن أول الحالات التي تمت فيها الإشارة إلى القرصنة في سياق انتهاك حقوق الطبع والنشر كانت من قبل (دانيال ديفو) في عام 1703م، عندما قال في روايته (تروبورن إنجليش مان) "تتم طباعتها الآن مرات ومرات، من قبل القراصنة".

أمثلة شائعة

تعد إعادة إنتاج الأعمال الموسيقية بدون الحصول على إذن أحد أشكال التعدي على حقوق الطبع والنشر. ويمكن أن تأخذ إعادة الإنتاج الأشكال التالية:

- نسخ الأعمال أو المستندات من أحد المواقع أو الملقمات أو المجلدات أو الأدلة أو وسائط التخزين أو المستودعات.
- التنزيل غير المعتمد للمواد المحفوظة بحقوق الطبع والنشر.
- تعد مشاركة الموسيقى المسجلة غالبًا بتنسيق ملفات (MP3) أحد أشكال الانتهاكات الشائعة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الاستخدام العادل

ما المقصود بالاستخدام العادل؟ لماذا يتاح الاستخدام العادل؟ ما الذي يمكن اعتباره استخدامًا عادلاً بموجب قوانين حقوق الطبع والنشر؟

يمكن أن يعتبر تحديد الحماية أمرًا معقدًا. وغالبًا ما يثار الجدل حول الاستخدام العادل، ومن الصعب للممارسين القانونيين فهمه، كما يكون من الصعب بشكل أكبر على الناشرين فك شفرته. عند تحديد الاستخدام العادل، هناك بعض الأسئلة التي يمكن أن تساعد في تحديد ما إذا كان قد حدث انتهاكًا لحقوق الطبع والنشر أم لا.

وإليك الأسئلة التي يجب طرحها:

- هل العمل خاضع لحقوق الطبع والنشر؟
- ما مقدار المواد التي تم نسخها؟
- ما هي طبيعة العمل الذي تم نسخه؟
- هل يحقق الشخص الذي يقوم بإعادة إنتاج العمل أرباحًا؟
- كيف يتأثر العمل الأصلي بالنسخ؟

ويكون الاستخدام العادل عندما يتم استخدام المواد الخاضعة لحقوق الطبع والنشر لأغراض محدودة وتحويلية مثل التعليق عليها أو انتقادها، أو السخرية منها. ويمكن أن تتم مثل تلك الاستخدامات بدون الحصول على إذن من مالك حقوق الطبع والنشر.

إذًا، فما المقصود بالاستخدام (التحويلي)؟ إذا كان هذا التعريف يبدو غامضًا أو غير واضح، فيجب ملاحظة أن ملايين الدولارات قد تم إنفاقها في شكل رسوم قانونية لتحديد ما يمكن اعتباره استخدامًا عادلاً. فلا توجد قواعد ثابتة وسريعة، بل توجد قواعد عامة وقرارات متنوعة من المحاكم.

والسبب وراء ذلك هو أن القضاة وصناع القوانين الذين قاموا بوضع استثناء الاستخدام العادل لم يكونوا يرغبون في قصر تعريفه. فقد أرادوا له أن يكون مثل الحوار الحر، وأن يكون له معنى شاملاً، مفتوحًا على كل التفسيرات.

قياس الاستخدام العادل: العوامل الأربعة:

تعد هذه العوامل الأربعة هي الإرشادات الخاصة بقياس الاستخدام العادل:

1. السبب المنطقي وراء الاستخدام.
2. طبيعة المواد المحفوظة بحقوق الطبع والنشر.
3. الجزء الذي يتم استخدامه.
4. التبعات المحتملة على الأسواق.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

المعايير الخمسة التي يجب الوفاء بها للاستخدام العادل الأكاديمي

1. يجب أن تكون الأبحاث أو الأوراق المشار إليها من بين الأعمال الأكاديمية المشروعة.
2. يجب أن تكون المواد المستخدمة ذات صلة مباشرة بالموضوع.
3. يجب أن يتم ذكر المصدر وحقوق الطبع والنشر المحتملة.
4. يجب أن تكون الأوراق لأغراض تعليمية غير هادفة إلى الربح.
5. لا يجب الاستخدام المفرط لمادة المؤلف حتى تؤثر على القيمة السوقية للعمل الأصلي.

ما الذي يمكن اعتباره استخدامًا عادلاً؟

توجد بعض الإرشادات العامة يمكن استخدام جزء محدود من الموارد أو المواد من خلالها في فصول الدراسة بموجب الاستخدام العادل، وإليك تلك الإرشادات:

- أجزاء أو جمل من كتاب.
- مقالات من نشرة أو صحيفة.
- مخطط أو رسم بياني أو شكل توضيحي أو رسم أو رسوم كرتونية أو صور من كتاب، أو نشرة أو صحيفة.
- الشعر – نسخ متعددة من قصيدة عدد كلماتها (250) كلمة أو أقل تظهر في صفحتين أو أقل أو(250) كلمة من قصيدة أطول من ذلك.
- النثر – نسخ متعددة من مقال أو قصة أو بحث عدد كلماته (2,500) كلمة أو أقل أو اقتباس (1,000) كلمة أو (10%) من العمل الإجمالي، أيهما أقل.

إليكم بعض الأسئلة التي يجب أن يتم توجيهها للمساعدة في تحديد ما إذا كان قد حدث انتهاكًا لحقوق الطبع والنشر أم لا:

- هل العمل خاضع لحقوق الطبع والنشر؟
- ما مقدار المواد التي تم نسخها؟
- ما هي طبيعة العمل الذي تم نسخه؟
- هل يحقق الشخص الذي يقوم بإعادة إنتاج العمل أرباحًا؟
- كيف يتأثر العمل الأصلي بالنسخ؟

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

النطاق العام

لقد بدأ النطاق العام في القرن الثامن عشر لوصف الأعمال التي لم تكن تخضع لقانون حقوق الطبع والنشر. كما يستخدم أيضًا للإشارة إلى نهاية فترات حقوق الطبع والنشر عند انتهاء صلاحية حقوق الملكية الفكرية، مثل: حقوق الطبع والنشر، وبراءات الاختراع، والعلامات التجارية، أو عندما يتم هجرها أو التنازل عنها. ونظرًا لأن قانون حقوق الطبع والنشر يختلف من دولة لأخرى، فقد وصفت (باميلا ساموليسون)، وهي مدرسة القانون وإدارة المعلومات في جامعة (بيركلي)، النطاق العام على أنه "أحجام مختلفة في أوقات مختلفة في دول مختلفة".

كما يمكن الإشارة إليه أيضًا على أنه تلك الأعمال التي لم تعد تحظى برعاية قانونية بموجب قانون الملكية الفكرية، وتشتمل على كل أوجه الأعمال التي لا تخضع لتغطية عقيدة الملكية الفكرية، مثل: الأجزاء التي لا قيمة لها في الأعمال الخاضعة لحقوق الطبع والنشر، أو الإجراءات أو الاستثناءات المعرفة والمحددة قانونيًا لحقوق الطبع والنشر.

وحسبما قالته البروفيسور (ساموليسون)، تشتمل القيم المحتملة للأعمال في النطاق العام ما يلي:

- اللبنات الأساسية لخلق معرفة جديدة، وتشتمل الأمثلة على ذلك البيانات والحقائق والأفكار والنظريات والمبادئ العلمية.
- الوصول إلى الإرث الثقافي من خلال موارد المعلومات مثل: النصوص اليونانية القديمة و(سيمفونيات موتزارت).
- الترويج للتعليم، من خلال نشر المعلومات والأفكار والمبادئ العلمية.
- تمكين الوصول قليل التكلفة إلى المعلومات بدون الحاجة إلى تحديد موقع المالك أو التفاوض على دفع رسوم الحقوق وحقوق المؤلفين، من خلال، على سبيل المثال، الأعمال أو براءات الاختراع التي انتهت صلاحية حقوق الطبع والنشر الخاصة بها، بالإضافة إلى تجميع البيانات غير الأصلية.
- الترويج للصحة العامة والأمان العام، من خلال المعلومات والمبادئ العلمية.
- الترويج للعملية والقيم الديمقراطية، من خلال الأخبار والقوانين والتشريعات والأفكار القضائية.
- تمكين التقليد التنافسي، من خلال، على سبيل المثال، براءات الاختراع وحقوق الطبع والنشر التي انتهت.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

أمثلة الأعمال الخاضعة للنطاق العام

تمثل الثقافات التقليدية والفلكلور الشعبي إلى أن تكون مؤثرة عبر الأجيال، وأن تكون موغلة في القدم، بالإضافة إلى أنها تكون "مملوكة" للمجموعات والمجتمعات. وبالتالي، فإنه ينظر إليها في أغلب الأمر على أنه مثال للنطاق العام. وغالبًا لا تكون خاضعة لحماية قوانين الملكية الفكرية الحالية، ويتم التعامل معها على أنها في إطار النطاق العام. وتعد مغامرة (مارك توين) (لتوم سوير) مثالاً كلاسيكيًا للنطاق العام مع مشتقات متعددة.

الإذن العام

من الصعب هذه الأيام العمل وإنتاج الأعمال الخاصة بك دون الإشارة إلى أعمال الآخرين والاستفادة منها.

ويصبح الأمر أكثر صعوبة لأن شبكة (الإنترنت) قد أتاحت لنا إمكانية الوصول تقريبًا إلى كل أنواع المعلومات، والمستندات،والتصميمات، والأفكار، والعمليات، وحتى يمكننا الاقتباس من المصادر الأصلية من خلالها. وتتمثل المسئولية أثناء القيام بالأعمال الخاصة بنا، على الرغم من ذلك، في الحصول على إذن عند الرغبة في استخدام المواد الخاصة بالآخرين.

اطرح الأسئلة التالية على نفسك:

1. متى يكون الإذن ضروريًا؟

- متى تنوي استخدام تلك المواد لأغراض تجارية.
- متى تنوي استخدام تلك المواد بشكل متكرر.
- متى تنوي استخدام عمل بمجمله، ويكون أكبر من (2,500) كلمة.

2. كيف يمكن الحصول على الإذن؟

- لكي يتسنى استخدام المواد خارج المؤسسة التي تتبعها، يجب أن تحصل على إذن أنت نفسك.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

نموذج خطاب مرسل إلى أحد ملاك حقوق الطبع والنشر يطلب المرسل فيه الإذن للحصول على نسخة من العمل

التاريخ.

إدارة أذون المواد.

شركة كتب افتراضية.

عمارة رقم 40 في أي شارع.

المدينة، والرمز البريدي للولاية.

سيدي العزيز/سيدتي العزيزة:

أرغب في الحصول على إذن لنسخ ما يلي للاستخدام المستمر في الفصول الدراسية التي أعمل بها خلال الأعوام الدراسية التالية.

العنوان:	التعليم في الكلية، الطبعة الثانية.
حقوق الطبع والنشر:	أي شركة كتب، 970ام, 1972م.
المؤلف:	(جون هميلتون).
المواد التي سيتم تكرارها:	الفصول (5، 6) و(15) (مرفق صورة منها).
عدد النسخ:	(500).
التوزيع:	يتم توزيع المواد إلى الطلبة في الفصول الدراسية التي أعمل بها ولن يدفعوا سوى تكلفة التصوير الضوئي.
نوع إعادة الطبع:	التصوير الضوئي.
الاستخدام:	سيتم استخدام هذه الفصول كمواد تعليمية تكميلية.

وقد أرفقت ظرفًا يحمل الطابع وعليه عنواني لاستخدامه للرد على طلبي.

مع خالص التقدير،

عضو هيئة التدريس.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تصريح خاص

يتم طلب الإذن الخاص للمواد الخاصة المحمية بحقوق الطبع والنشر. يتطلب إعادة إنتاج وتوزيع المواد المحمية بحقوق الطبع والنشر أو الأعمال مثل: الصوت والصور ومقاطع (الفيديو) الحصول على إذن خاص. إذا كنت ترغب في إعادة إنتاج المواد المحمية بحقوق الطبع والنشر، فيجب أن تحصل على إذن مكتوب لذلك. ويمكنك طلب الإذن من الناشر لاستخدام المواد بشكل كامل أو لاستخدام أجزاء منها. إذا كان إعادة إنتاج المواد يعتبر استخدامًا عادلاً، فلن تحتاج إلى الحصول على إذن.

كيف يمكن الحصول على الإذن الخاص؟

1. خطاب طلب الإذن.

2. حدد هل يعد استخدام المواد استخدامًا عادلاً أم أنك ستحتاج إلى الحصول على إذن مكتوب لإعادة إنتاجها. يسمح الاستخدام العادل بإعادة الإنتاج المحدود. على سبيل المثال، إذا كنت مدرسًا وكنت تقوم بإعادة إنتاج المعلومات من أجل درس تعليمي، فيمكن أن يعتبر ذلك استخدامًا عادلاً. أما إذا كنت ستجني أرباحًا من إعادة إنتاج المواد، فمن الأغلب ألا يعتبر ذلك استخدمًا عادلاً. ويمكن أن تساعدك قائمة فحص المواد التي يمكن اعتبار استخدامها عادلاً وتلك التي لا يعتبر استخدامها عادلاً.

3. ابحث عن ناشر المواد إذا قررت أنها لا تأتي ضمن قانون الاستخدام العادل.

4. اطلب الحصول على إذن لاستخدام المواد. ويمكنك استخدام عينة خطاب طلب الإذن.

قم بإرسال الطلب الخاص بك إلى الناشر مع إرسال ظرف مسجل عليه العنوان الخاص بك حتى يتمكن الناشر من إرسال الرد عليك سواء بمنح الإذن أم لا.

السرقة الأدبية

لا يعتبر مصطلح السرقة الأدبية مصطلحًا معتادًا بالنسبة لمعظمنا. ونظرًا لأنه مصطلح غير معتاد بالنسبة لنا، يعد عدم معرفة معناها وتبعات ارتكابها أمرًا خطيرًا للغاية. فالنسخ واللصق أمر معتاد وطبيعي لمعظمنا!

وبمعنى آخر، تعتبر السرقة الأدبية شكلاً من أشكال الاحتيال. وهي تشتمل على سرقة عمل شخص آخر والكذب حياله بعد ذلك. ويجعل ذلك السرقة الأدبية واحدة من أشهر السلوكيات غير الأخلاقية على شبكة (الإنترنت).

يعد كل ما يلي من أشكال السرقة الأدبية:

- انتحال أعمال الآخرين وادعاء أنها تخصك.
- نسخ الكلمات أو الأفكار من شخص آخر بدون ذكر مصدرها الأصلي.
- عدم وضع الأشياء المقتبسة بين علامتي اقتباس.
- إعطاء معلومات غير صحيحة حول مصدر الاقتباس.
- تغيير الكلمات ولكن نسخ هيكل الجمل في مصدر ما مع عدم ذكر المصدر الأصلي.
- نسخ الكثير من الكلمات أو الأفكار من مصدر بما يشكل أغلبية العمل، سواء قمت بذكر المصدر الأصلي أم لا (ارجع إلى القسم الخاص بقواعد «الاستخدام العادل).

ومع ذلك، يمكن تجنب معظم حالات السرقة الأدبية من خلال ذكر المصادر. ويعد الإقرار بأن بعض المواد قد تمت استعارتها، وتوفير المعلومات اللازمة للوصول إلى المصادر لمتابعيك، أمرًا كافيًا، للحيلولة دون حدوث السرقة الأدبية.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الأنشطة

نشاط: تبعات السرقة الأدبية

اذكر بعض التبعات المحتملة للسرقة الأدبية بين طلاب الجامعات أو المحترفين. قم بمناقشة الأمر وعمل قائمة بتلك التبعات.

المنظورات الثقافية حيال السرقة الأدبية

لا تنظر كل الثقافات بنفس الطريقة إلى السرقة الأدبية. ويمكن أن يبدو المفهوم العربي بأن "الأفكار " يمكن أن تكون ملكية للأفراد سخيفًا لأولئك الذين يمتلكون الآراء المختلفة حيال ما يمكن أن يمثل معلومات مشتركة أو أمور يمكن نشرها بين العامة. ويمكن أن يعاني الطلبة من الثقافات التي لديها شعورًا أكثر بالتعاونية فيما يتعلق بالهوية، على سبيل المثال، لفهم الفوارق التي تضعها بعض الثقافات بين الممتلكات الفردية والممتلكات العامة. ويمكن أن تقضي بعض الوقت الفعال للغاية في الفصل الدراسي في مناقشة وجهات نظر الطلبة حيال هذا الأمر.

البرامج التي تتعرض للقرصنة

البرامج التي تتعرض للقرصنة هي البرامج التي يتم نسخها ويتم توزيعها دون الحصول على تصريح بذلك. وتحدث القرصنة على البرامج عندما يقوم شخص ما بعمل نسخة غير مشروعة من برنامج أصلي ثم بيع تلك النسخة.

ولقد خلقت التطورات الحديثة في التقنيات المتقاربة المتطورة المزيد من قدرات المعالجة، والأدوات الجديدة، والتطبيقات المصغرة للهواتف المحمولة، والتطبيقات، والبرامج، وشبكات النظير إلى النظير، ومواقع المزادات، وغير ذلك من أنواع القنوات القائمة على شبكة (الإنترنت) للمستخدمين لتبنيها. ومع ذلك، فإن السلبية تتمثل في أنها جعلت القرصنة أكثر سهولة.

"تؤثر القرصنة على البرامج أكثر من مجرد صناعة البرامج حيث إنه لكل دولار من مبيعات برامج (الكمبيوتر) الشخصية، هناك (3) أو (4) دولارات أخرى تفقد من العائدات بسبب دعم تقنية المبيعات وخدمات التوزيع."

تقرير (BSA) الصادر في أكتوبر 2009م، قرصنة البرامج على شبكة (الإنترنت)، تهديد يواجه أمانك

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تحدث عمليات الاحتيال المعتمدة على شبكة (الإنترنت) من خلال قنوات متنوعة

تتسبب عمليات القرصنة والاحتيال على البرامج والمعتمدة على شبكة (الإنترنت) في الكثير من الأضرار للأشخاص وللصناعة. فبالإضافة إلى القرصنة، فإنها تربي أيضًا عمليات الاحتيال والهجمات بالفيروسات والخداع. وقبل إتاحة القرصنة عبر شبكة (الإنترنت)، كان النسخ غير المرخص به للبرامج غالبًا ما يتطلب التبادل المادي للأقراص. وتشير القرصنة على البرامج من خلال شبكة (الإنترنت) إلى استخدام شبكة (الإنترنت) للقيام بما يلي:

- توفير الوصول إلى نسخ يمكن تنزيلها من البرامج التي تعرضت للقرصنة.
- الإعلان عن البرامج التي تعرضت للقرصنة وتسويقها، وتوفيرها من خلال البريد، أو توفير أو نقل الأكواد أو التقنيات الأخرى اللازمة للتحايل على ميزات الأمان المضادة للنسخ ويمكن أن تنتقل عمليات الاحتيال تلك من خلال المواقع التالية:

- **مواقع المزادات**

تأتي ضمن أشهر المواقع التي يقوم الأشخاص بشراء وبيع المنتجات القانونية والمشروعة من خلالها، إلا أنها تكون عرضة لإساءة الاستخدام خصوصًا عندما يتعلق الأمر ببيع البرامج.

- **مواقع النظير للنظير (Peer-to-Peer - P2P)**

تهدف هذه التقنية إلى توصيل مستخدمي أجهزة (الكمبيوتر) ببعضهم البعض مباشرة بدون نقطة إدارة مركزية. ويجب على المستخدم تنزيل تطبيقات النظير إلى النظير الخاصة بالعميل للوصول إلى شبكة النظير إلى النظير. فهي تسمح بالعثور على الملفات التي يحتاج إليها المستخدمون ومشاركتها، بما في ذلك البرامج، والموسيقى، والأفلام، ونغمات الرنين، وبرامج التلفاز.

دراسة حالة (24): صرّح الكونجرس أن مشاركة الملفات يسرب بيانات فيدرالية حساسة

تسربت معلومات حكومية وشخصية حساسة من خلال استخدام تقنية معروفة لمشاركة البيانات عبر (الإنترنت). وقد اشتملت هذه المعلومات على صور رقابية لرجل مافيا مضروب، وقوائم من أفراد في برنامج الحكومة لحماية الشهود وقوائم من أفراد يعانون من مرض الإيدز وغيرهم. وعادة ما يتم الكشف هذا النوع من المعلومات دون قصد من قِبَل أفراد يقومون بتحميل تلك التقنية لمشاركة ملفات الموسيقى وغيرها من الملفات. فهم ليسوا على دراية بأن برنامج النظير للنظير ييسر كذلك للآخرين الحصول على المعلومات الموجودة على أجهزة (الكمبيوتر) الخاصة بهم. وقد أصبح هذا الأمر بالغ الخطورة لدرجة أن رئيس لجنة متابعة البرلمان والاصلاح الحكومي. عن ولاية نيويورك (Edolphus Towns) قدم مشروعًا قانون لمنع تداول مثل هذه البرامج في كافة أجهزة (الكمبيوتر) وشبكات الحكومة والمتعهدين.

Washington Post, 30 July, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/07/29/AR2009072902273.html

- **مواقع الشركات إلى الشركات (Business-to-Business - B2B)**

تستخدم لتوزيع المنتجات بين الشركات بأسعار منخفضة، وعلى نطاق واسع. وغالبًا ما يتم بيع البرامج المزيفة من قبل الموزعين على هذه المواقع.

- **مواقع الشبكات الاجتماعية**

ادعت شركة أمنية تتعامل مع أمان (الويب)، أنه في وقت قريب، ستصبح مواقع الشبكات الاجتماعية، تربة خصبة لعمليات الاحتيال والقرصنة.

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

الخضوع للمحاسبة أثناء الاتصال بـ (الإنترنت)

دقة المعلومات

تعني دقة المعلومات، بكل بساطة، تحديد مدى دقة المعلومات. ويتعلق الأمر بجودة ودقة المعلومات. وهناك علاقة متبادلة بين الرقم المتزايد للغاية للمستخدمين عبر شبكة (الإنترنت) في مختلف أرجاء العالم وبين مقدار المعلومات المتاحة.

ومع تزايد أعداد المستخدمين، يتزايد مقدار المحتويات والمعلومات المتاحة على شبكة (الإنترنت). لكن كيف نضمن أن المعلومات التي نصل إليها صحيحة ودقيقة. تمت مناقشة بعض الحقائق الأساسية في قسم الثقافة الإلكترونية حول كيفية التمييز بين المصادر التي يمكن الاعتماد عليها وتلك التي لا يمكن الاعتماد عليها على شبكة (الإنترنت).

ومن المعلومات المعروفة أن الوصول إلى مصدر (يمكن الاعتماد عليه) للمعلومات يوفر احتمالية كبيرة للحصول على "معلومات دقيقة".

إذًا، كيف يمكن الحصول على معلومات دقيقة؟

الحصول على المعلومات الدقيقة

1. **الوصول إلى المواقع ذات السمعة الحسنة**

يوفر لك الوصول إلى المواقع ذات السمعة الحسنة، مثل: (اليونسكو)، ومراكز الأبحاث، ومواقع الأعمال الشهيرة، والمكتبات العامة، والإدارات الحكومية، والوكالات الحكومية والجامعات الشهيرة، والمعاهد الموسيقية، والمنظمات الاحترافية، والأرشيفات، والبنوك المركزية، والجهات التنظيمية، والمتاحف، "المعلومات الدقيقة" التي تبحث عنها.

ويتم تصنيف معظم تلك المواقع تحت النطاقات (.gov) و(.org) و(.edu) و(.net) و(.com). فيمكن أن يؤدي البحث عن المواقع التي تنتمي إلى تلك النطاقات إلى المساعدة في الحصول على المعلومات الدقيقة. وتجنب مواقع الصحف الشعبية، والصحف العادية، وأعمدة القيل والقال، ومجلات الصحافة الصفراء.

2. **المراجع التبادلية**

تعد المراجع التبادلية، أو ما يطلق عليه أيضًا اسم (التثليث) عملية الهدف منها "التحقق" من المعلومات في مواقع مختلفة، أو من مصادر مختلفة، أو من خبراء مختلفين. ومن شأن ذلك أن يوفر لنا الفرصة للتحقق من المعلومات. وهي مهارة بحثية يمكن تعلمها وإتقانها للمساعدة في الحصول على "المعلومات الدقيقة".

"لقد خلقت الأجيال الأولى من التقنيات تحديات لقوانين حقوق الطبع والنشر الحالية، إلا أن أيًا منها لم يشكل نفس التهديد مثل: التحديات الرقمية."

جون في بافليك

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

تمرين

1. **تذكر سياسة المدرسة أن الطلبة يسمح لهم بتنزيل مقاطع (الفيديو) والصوت من المواد التعليمية والتي لا تتجاوز 5 ميجا بايت. ومع ذلك، يحتاج طالب إلى تنزيل ملف فيديو حجمه (7) ميجا بايت. لإتمام مشروع مدرسي. فما الذي يجب عليه فعله؟**

   أ. تنزيل مقطع (الفيديو) بعد الحصول على موافقة المدرس.

   ب. تنزيل مقطع (الفيديو) عندما لا يكون هناك أي شخص موجود.

   ج. تنزيل مقطع (الفيديو) بعد ساعات الدراسة.

   د. يسمح بتنزيل مقاطع (الفيديو) للمشروعات المدرسية.

2. **تشدد سياسة متبعة في مدرسة ثانوية تستخدم (الإنترنت) على أنه يجب ألا يقوم الطلبة بتنزيل مقاطع (الفيديو) والصوت من المواد التعليمية والتي تتجاوز (5) ميجا بايت مطلقًا. ما هو أفضل سبب يجعل المدرسة تفرض تلك السياسة؟**

   أ. للحد من مخاطر الإضرار بالبنية التحتية لشبكة المدرسة.

   ب. للحيلولة دون شغل الطلبة لعرض النطاق الترددي لشبكة (الإنترنت) بشكل كبير.

   ج. للحد من تنزيل الطلبة لمقاطع (الفيديو) والموسيقى التعليمية.

   د. لمنع الطلبة من تنزيل المواد غير ذات الصلة إلى شبكة المدرسة.

3. **أثناء إتمام الواجب المنزلي الخاص بك، قمت بنسخ صفحة كاملة من كتاب كتبه كاتب مشهور. ما الذي يمكن أن يحدث إذا تم كشف أنك لم تشر إلى الكاتب الأصلي؟**

   أ. يمكن أن تحصل على درجة سيئة في الواجب.

   ب. يمكن أن يقاضيك المؤلف والناشر.

   ج. لن يحدث شيء لأن ذلك لا يتجاوز حدود الواجب المنزلي.

   د. لن يحدث شيء لأن ذلك يعتبر استخدامًا عادلاً.

4. **ما هي الطريقة الصحيحة لطلب الإذن لاستخدام مقال منشور من شبكة (الإنترنت) لمجلة تعليمية تحقق أفضل المبيعات على الصعيد المحلي؟**

   أ. الكتابة إلى المؤلف لطلب الإذن.

   ب. استخدام المقال بشكل محدود دون طلب إذن.

   ج. تحرير المقال واستخدامه لأغراض تعليمية.

   د. الاتصال بالكاتب للحصول على إذن فوري.

5. **تلقيت اتصالاً هاتفيًا من رئيسك في العمل خلال الإجازة الأسبوعية أثناء تواجدك في السينما. ما الذي يجب عليك فعله؟**

   أ. توجيه المكالمة إلى البريد الصوتي.

   ب. الرد على المكالمة حيث إنها من رئيسك في العمل.

   ج. جعله ينتظر إلى أن تعثر على أقرب مخرج.

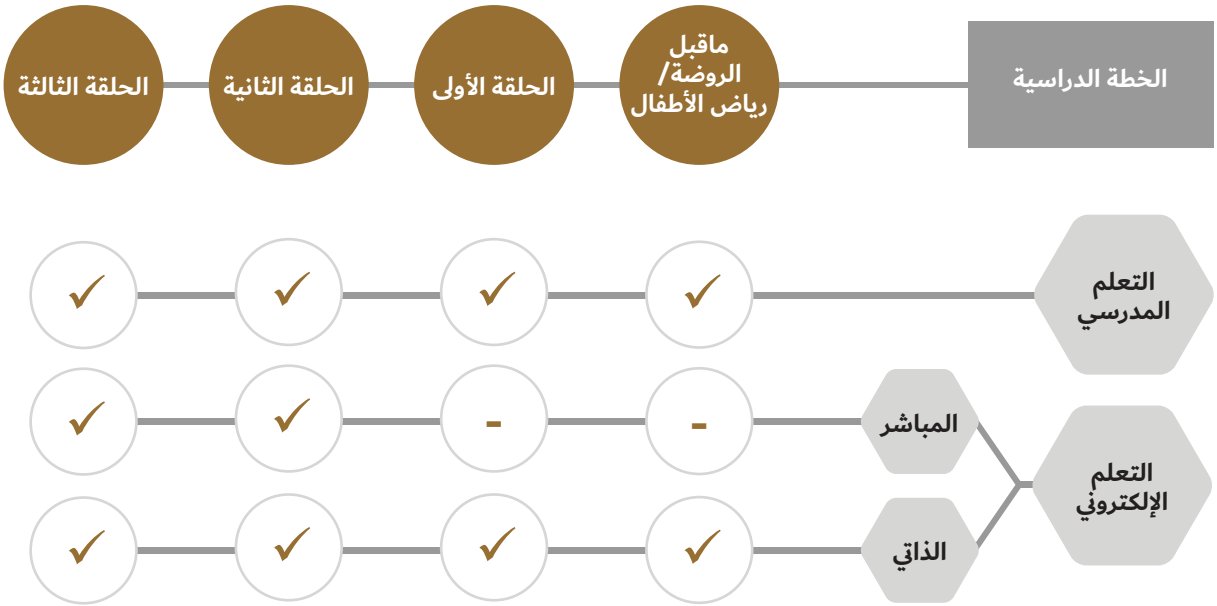
   د. تطلب منه الاتصال بك في وقت لاحق، حيث إنك لا يمكنك الحديث بحرية.

الإجابة: ١.أ ٢.ب ٣.أ ٤.أ ٥.ج

حقوق الطبع © محفوظة لوزارة التربية والتعليم – دولة الإمارات العربية المتحدة

التعليم الهجين في المدرسة الإماراتية

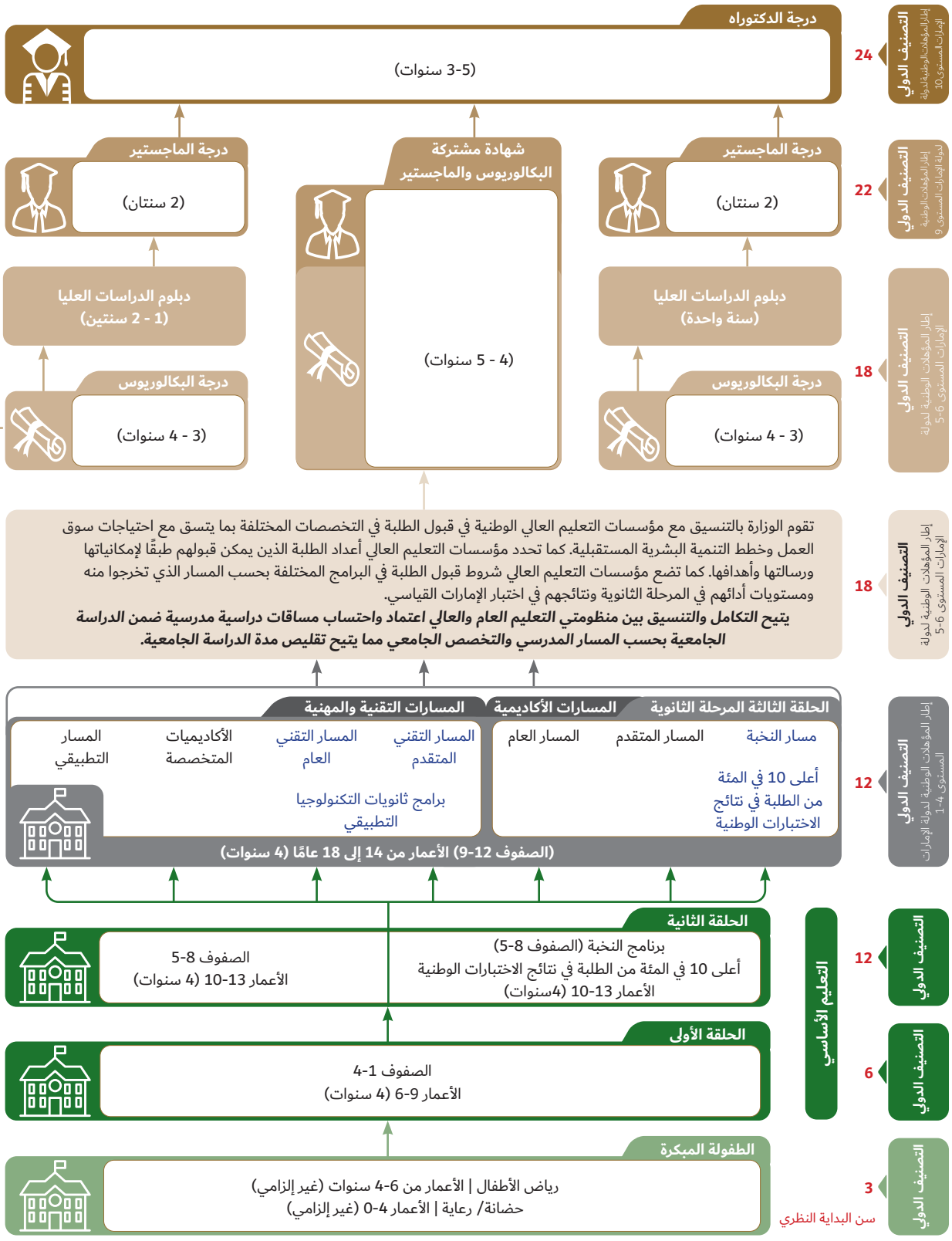
في إطار البعد الإستراتيجي لخطط التطوير في وزارة التربية والتعليم، وسعيها لتنويع قنوات التعليم وتجاوز كل التحديات التي قد تحول دونه، وضمان استمراره في جميع الظروف، فقد طبقت الوزارة خطة التعليم الهجين للطلبة جميعهم في المراحل الدراسيّة كافة.



قنوات الحصول على الكتاب المدرسي:

برنامج محمد بن راشد للتعلم الذكي
Mohammed Bin Rashid Smart Learning Program

الوحدات الإلكترونيّة


التصنيف الدولي
إطار المؤهلات الوطنية لدولة الإمارات المستوى 10
24
درجة الدكتوراه
(3-5 سنوات)
التصنيف الدولي
إطار المؤهلات الوطنية لدولة الإمارات المستوى 9
22
درجة الماجستير
(2 سنتان)
شهادة مشتركة
البكالوريوس والماجستير
(4 - 5 سنوات)
درجة الماجستير
(2 سنتان)
التصنيف الدولي
إطار المؤهلات الوطنية لدولة الإمارات المستوى 6-5
18
دبلوم الدراسات العليا
(1 - 2 سنتين)
دبلوم الدراسات العليا
(سنة واحدة)
درجة البكالوريوس
(3 - 4 سنوات)
درجة البكالوريوس
(3 - 4 سنوات)
التصنيف الدولي
إطار المؤهلات الوطنية لدولة الإمارات المستوى 6-5
18
تقوم الوزارة بالتنسيق مع مؤسسات التعليم العالي الوطنية في قبول الطلبة في التخصصات المختلفة بما يتسق مع احتياجات سوق العمل وخطط التنمية البشرية المستقبلية. كما تحدد مؤسسات التعليم العالي أعداد الطلبة الذين يمكن قبولهم طبقًا لإمكانياتها ورسالتها وأهدافها. كما تضع مؤسسات التعليم العالي شروط قبول الطلبة في البرامج المختلفة بحسب المسار الذي تخرجوا منه ومستويات أدائهم في المرحلة الثانوية ونتائجهم في اختبار الإمارات القياسي.
يتيح التكامل والتنسيق بين منظومتي التعليم العام والعالي اعتماد واحتساب مساقات دراسية مدرسية ضمن الدراسة الجامعية بحسب المسار المدرسي والتخصص الجامعي مما يتيح تقليص مدة الدراسة الجامعية.
التصنيف الدولي
إطار المؤهلات الوطنية لدولة الإمارات المستوى 4-1
12
الحلقة الثالثة المرحلة الثانوية
المسارات الأكاديمية
المسارات التقنية والمهنية
مسار النخبة
المسار المتقدم
المسار العام
المسار التقني المتقدم
المسار التقني العام
الأكاديميات المتخصصة
المسار التطبيقي
أعلى 10 في المئة من الطلبة في نتائج الاختبارات الوطنية
برامج ثانويات التكنولوجيا التطبيقي
(الصفوف 12-9) الأعمار من 14 إلى 18 عامًا (4 سنوات)
التعليم الأساسي
التصنيف الدولي
12
الحلقة الثانية
برنامج النخبة (الصفوف 8-5)
أعلى 10 في المئة من الطلبة في نتائج الاختبارات الوطنية
الأعمار 13-10 (4سنوات)
الصفوف 8-5
الأعمار 13-10 (4 سنوات)
التصنيف الدولي
6
الحلقة الأولى
الصفوف 1-4
الأعمار 9-6 (4 سنوات)
التصنيف الدولي
3
سن البداية النظري
الطفولة المبكرة
رياض الأطفال | الأعمار من 6-4 سنوات (غير إلزامي)
حضانة/ رعاية | الأعمار 4-0 (غير إلزامي)

الإمارات العربية المتحدة
وزارة التربية والتعليم

مركز اتصال وزارة التربية والتعليم
اقتراح - استفسار - شكوى

80051115

04-2176855

www.moe.gov.ae

ccc.moe@moe.gov.ae