الإمارات العربية المتحدة
وزارة التربية والتعليم

نحن الإمارات
WE THE UAE 2031

2025-2026

الدّراسات الاجتماعيّة والتّربية الوطنيّة

التربية الأخلاقية في العصر الرقمي

الصف
11

الدراسات الاجتماعية والتربية الوطنية

كتاب النشاط للطالب

الصف الحادي عشر

المجلد الثالث

رؤية وتحليل لكتاب

التّربيةُ الأخلاقيّةُ في العصرِ الرّقميِّ

1447-1446 هـ / 2026-2025 م

“

أَهَمِّيَّةُ تَوافُرِ ثَلاثَةِ أَشياءَ أَساسِيَّةٍ لِتَنافُسِيَّةِ الدُّوَلِ وَأَسْبَقِيَّتِها، وَهي: أَوّلًا: الحَجْمُ، وَثانيًا: سِلاحُ العِلْمِ، والاستِثمارُ فيهِ بِكُلِّ الإمكاناتِ، وَثالِثًا: القيادَةُ الواعِيَةُ الّتي لَدَيْها رُؤْيَةٌ واضِحَةٌ، وَخَريطَةُ طَريقٍ مُحَدَّدَةٌ.

”

صاحب السمو الشيخ محمد بن زايد آل نهيان

تعليمات:

- تخزين برنامج ماسح رمز الاستجابة السريعة (QR Code Reader) على الجهاز.
- مسح الرمز الوارد في الصفحة لمشاهدة (الفيديو).

الإمارات تسطر التاريخ بوصول مسبار الأمل إلى المريخ

نجح "مسبار الأمل الإماراتي" في الوصول إلى مدار كوكب المريخ مساء التاسع من فبراير 2021م بعد رحلة استمرت (7) أشهر قُطع خلالها مسافة (494) مليون كيلومتر، لتصبح بذلك دولة الإمارات أول دولة عربية، وخامس دولة في العالم تصل إلى كوكب المريخ، وذلك بهدف تقديم أول صورة متكاملة للغلاف الجوي للمريخ، وفهم أعمق للتغيرات المناخية على سطح الكوكب الأحمر.

وتزامنًا معَ الذكرى الخمسين لقيامِ دولة الإمارات العربية المتحدة أطلقت الدولة في العشرين من يوليو2020م مسبار الأمل الذي بُني في مركز محمد بن راشد للفضاء وصنع بأيدي إماراتية.

ونشر صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي -رعاه الله- أول صورة للمريخ سجلها "مسبار الأمل" قائلًا سموه:

"من ارتفاع 25 ألف كم عن سطح الكوكب الأحمر ..
أول صورة للمريخ بأول مسبار عربي في التاريخ".

السلام عليكم، الإمارات تحيكم من كوكب المريخ

"أبناء الإمارات حولوا الحلم إلى واقع، وحققوا طموحات أجيال من العرب، ظل يراودها أمل وضع قدم راسخة في سباق الفضاء، الذي ظل حكرًا على عدد محدود من الدول".

الشيخ خليفة بن زايد آل نهيان – رحمه الله

”وصول مسبار الأمل إلى المريخ، هو موعد مع التاريخ، الذي سيكتب أن إرادة التقدم الإماراتية انتصرت على كل التحديات، وأن الرهان على شبابنا المسلح بالمعرفة حقق أهم إنجاز علمي عربي في العصر الحديث، وإننا نستطيع تحقيق كل طموحاتنا، مهما بدت صعبة أو حتى مستحيلة“

صاحب السمو الشيخ محمد بن زايد آل نهيان رئيس الدولة –حفظه الله.

”بدأت مرحلة جديدة من التاريخ العلمي العربي.. أبارك لشعب الإمارات، ونبارك لجميع الشعوب العربية و الإسلامية.. نبارك للبشرية وصول أولى بعثاتها في 2021 لكوكب المريخ“.. اليوم بدأت مرحلة جديدة من التاريخ العلمي العربي. مرحلة عنوانها الثقة.. الثقة بأنفسنا وبشبابنا وبشعوبنا العربية.. الثقة بأننا نستطيع أن ننافس بقية الأمم والشعوب“.

صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس دولة الإمارات رئيس مجلس الوزراء حاكم دبي -رعاه الله.

مسبار الأمل

المقدِّمة

يعد البعد الأخلاقي ركنًا أساسيًّا في العملية التربوية، وأحد ثوابتها، حيث يعجز أي كان عن الفصل بين الأخلاق والتربية، ولا يستقيم حال أحدهما دون الآخر، ويتجلى هذا التصور للعلاقة بين الأخلاق والتربية في مقولة (هربرت سبنسر) الأخلاقية: "إن الغرض الجزئي والكلي من التربية يتمثل في فكرة واحدة هي (الفضيلة)".

واعتمادًا على هذه المقولة لا يمكن للأخلاق أن تنفك عن التربية جوهريًّا، ويكاد يستحيل إيجاد الحدود الفاصلة بين الأخلاق والتربية، إنهما عنصران متكاملان في بناء شخصية الفرد وسلوكه، والنهوض به إلى أعلى المراتب الإنسانية والأخلاقية.

وفي عالم اليوم الذي يعج بأشكال التقنيات الحديثة،والتحولات التكنولوجية والعلمية، فرضت هذه التقنيات نفسها كأحد المستحدثات التربوية والتعليمية التي أثرت على مصادر المعرفة التي يمكن للطالب أن ينهل منها، وتغير دور المعلم من كونه المصدر الوحيد للمعلومة، وتبدل الاهتمام من التعليم المباشر والتلقين إلى التعلم الذاتي الذي بات يلقي بمسؤولية أكبر على الطالب للتعلم من خلال الاستكشاف والبحث والتجريب، ولم يعد هناك مفر لأي كان من الخوض في أسبار التقنية.

لقد جاءت الحاجة إلى استحداث كتاب التربية الأخلاقية في عصر التكنولوجيا بسبب الإيمان العميق بأهمية تعزيز الفضيلة لدى المتعلمين، ولأن المجتمعات الإنسانية لا يستقيم حالها دون الأخلاق كما التقنية.

ولأن التعامل مع أفراد المجتمع في العالم الحقيقي لا يختلف في جوهره عن التعامل معهم من خلف شاشات مضيئة.

المحتويات

1	**الحقوق والواجبات الإلكترونية**	**12**
	الفائدة من استخدام المعلومات الرقمية على الصعيد الإجتماعي	14
	الوصول العادل للمعلومات والتغلب على الفجوة الرقمية	15
	تكافؤ فرص المشاركة الإلكترونية لأصحاب الهمم	17
	المسؤوليات التي يجب إدراكها عند مشاركة المعلومات والمعرفة	19
2	**الثورة الرقمية**	**22**
	تطور التقنيات الرقمية	24
	أدوات الثقافة الرقمية	24
	تطبيقات الثقافة الرقمية	26
	التطبيقات عبر الإنترنت	28
3	**التسوق عبر (الإنترنت)**	**32**
	أنواع التعاملات عبر (الإنترنت)	34
4	**التقنية والجريمة**	**40**
	الجرائم الإلكترونية	42
	المحتوى غير الأخلاقي	46
	أسباب الجرائم الإلكترونية	50
	كيف تحمي نفسك من الوقوع كضحية لجريمة إلكترونية؟	51
	مصداقية المصادر المتوفرة عبر (الإنترنت)	52

5 الاستخدام الآمن والأخلاقي للتقنيات	**56**
الأنماط الشائعة للانتهاكات الرقمية	58
الحوسبة السحابية	64
مواقع التواصل الاجتماعي	66
الاستخدام الملائم والأخلاقي لأدوات التواصل والتعاون الرقمية	74
استخدام أدوات التواصل الاجتماعي للأسباب الجيدة	76
تبادل ومشاركة المعلومات عبر أنظمة الشبكات بشكل أخلاقي	76
اتخاذ القرارات الأخلاقية	79
الوقاية على الإنترنت	80
(بروتوكولات) الحماية المستخدمة في تأمين الشبكات اللاسلكية	85
6 الصحة والسلامة	**90**
فهم مبدأ قوانين بيئة العمل الصحية وأهميتها	92
وضعية الجسم والبيئة المحيطة في أثناء استخدام لوحة المفاتيح	95
استخدامات الحاسوب التي تؤثر على الصحة الجسدية	95
المشاكل الاجتماعية المرتبطة باستخدام الحاسوب و(الإنترنت)	98
التخلص من معدات الحاسوب وتدويرها بالشكل الملائم	103
كيف يمكنك مسح البيانات نهائيًّا من حاسوبك القديم؟	104

الحقوق والواجبات الإلكترونية

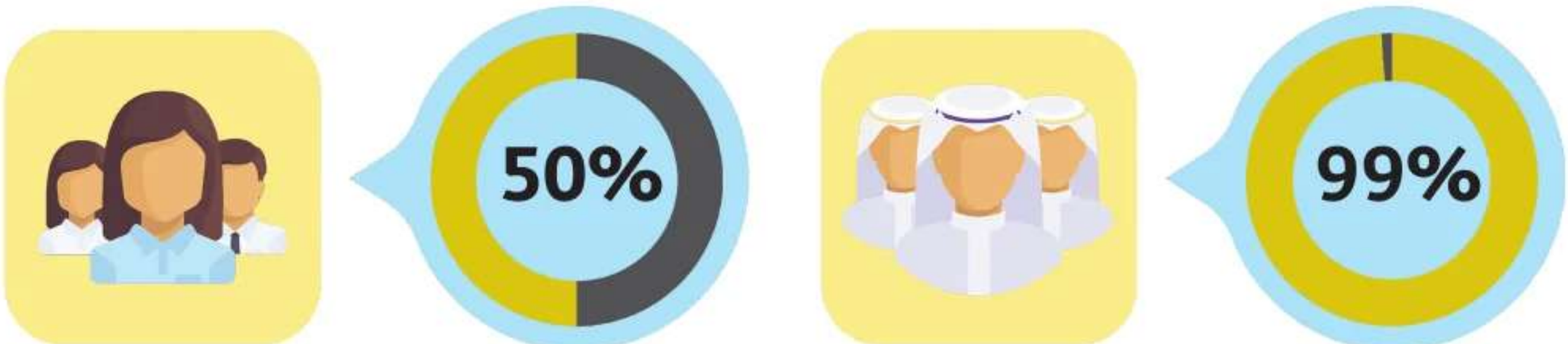
الفائدة من استخدام المعلومات الرقمية على الصعيد الإجتماعي:

مع التّطور الحاصل في مجال المعلوماتية على الصعيد الاجتماعي يتزايد الإقبال على استخدام تقنيات الاتصال والمعلومات كأداة لنشر المعلومات في وقتنا الحاضر، حيث تمكن تقنيات المعلومات والاتصال من نشر المعلومات بشكل متزامن أو غير متزامن، كما تمكن الأفراد من الحصول على المعلومات في أي زمان ومكان وحول أي موضوع يمكنهم استغلاله لتطوير أنفسهم اجتماعيًّا وثقافيًّا واقتصاديًّا.

الوصول يعني (القدرة على الدخول) أو (النفاذ من أو إلى مكان ما) أو (التواصل مع شخص أو شيء ما).

عملت (الإنترنت) على جعل المعلومات متوفرة بطريقة سهلة وسريعة متاحة للعامة، وفي متناول اليد، كما قامت بإحداث ثورة في مجال الاتصالات والتواصل الاجتماعي من خلال إنشاء نطاق عالمي، يستطيع الأفراد من خلاله التواصل مع بعضهم، ومشاركة البيانات والعمل من خلال (الإنترنت)، كما يلعب (الإنترنت) دورًا كبيرًا في إزالة الحدود بين الأمم.

- يبلغ العدد الإجمالي لمستخدمي (الإنترنت) لعام 2020م في دولة الإمارات العربية المتحدة (99) مستخدمًا لكل (100) نسمة.
- يبلغ العدد الإجمالي لمستخدمي (الإنترنت) لعام 2017م على الصعيد العالمي (50) مستخدمًا لكل (100) نسمة.



قد يشير عدد مستخدمي (الإنترنت) إلى المستخدمين من مرحلة عمرية ما.

ارتفع عدد مستخدمي (الإنترنت) في جميع أرجاء العالم عام 2020م إلى (4.8)مليار مستخدم بحوالي (62 %) من إجمالي سكان العالم المقدر بأكثر من (7.7) مليار إنسان.

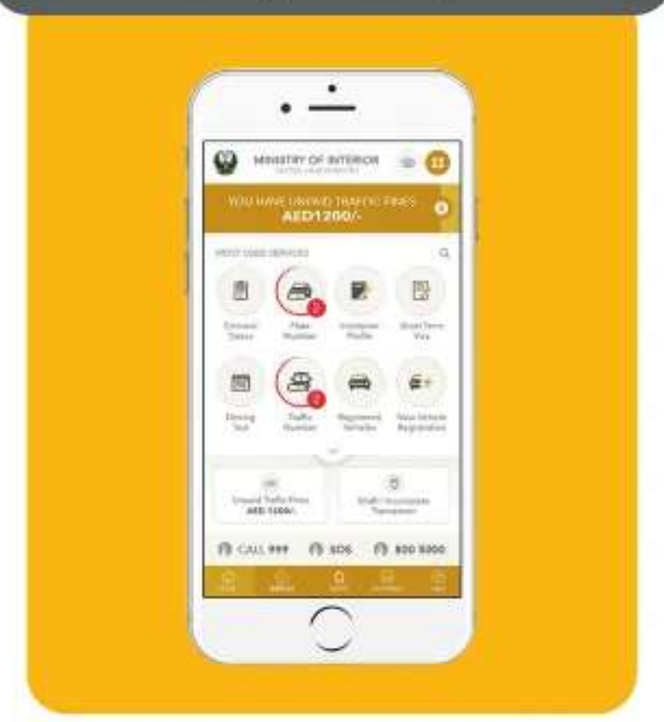
الوصول العادل للمعلومات والتغلب على الفجوة الرقمية:

على النقيض من سابقًا كان الناس يعتمدون وبشكل أساسي على الجرائد والمجلات والكتب والمواد المطبوعة الأخرى للحصول على المعلومات، فإننا في الوقت الحاضر نعتمد على وسائط أكثر تطورًا وعلى (الإنترنت)، والجيد حول هذا الأمر هو توفر العديد من الطرائق للوصول إلى (الإنترنت).

تعد دولة الإمارات العربية المتحدة من الدول الرائدة على الصعيد الإقليمي في التغلب على الفجوة الرقمية من خلال عدة مشاريع ريادية مثل:

المدينة الذكية
دبي **2014**

حكومة أبوظبي المتنقلة
وخدمات الهاتف



توجد عدة طرائق للوصول إلى (الإنترنت)، ولكل طريقة خصائصها وعيوبها، وحتى تكون قادرًا على اختيار أمثل طريقة تناسب احتياجاتك فإنه يتعين عليك تقييم الخيارات المتاحة.

نشاط

ماذا تعرف عن تطبيق الهاتف لوزارة الداخلية، استفسر من والديك أو معلمك عن الخدمات التي يوفرها التطبيق، وناقشه مع زملائك في الصف.

(المودم):

يعد استخدام (المودم) الطريقة الأقدم للوصول إلى (الإنترنت)، كما يقوم مصنعو الحاسوب في الوقت الحالي بتزويد منتجاتهم بـ (مودم) مدمج بها.

خدمات (الإنترنت) العامة:

في الوقت الحاضر يمكنك الاتصال بـ (الإنترنت) بسهولة؛ نظرًا لوجود العديد من المؤسسات التي بدأت بتوفير شبكات النطاق العريض، عالية السرعة والتي يسهل استخدامها، ولكن قد يتعين عليك دفع مبلغ بسيط في مقابل الحصول على هذه الخدمة بناء على السرعة التي تحصل عليها. تعد المكتبات العامة والمرافق الحكومية مثالًا على الأماكن التي يمكنك الحصول فيها على اتصال مجاني بـ (الإنترنت).

بالإضافة إلى ما سبق، يمكنك الحصول -عادة- على اتصال بـ (الإنترنت) في الأماكن الآتية:

- الكليات والجامعات.
- المرافق التجارية، مثل الفنادق والمراكز التجارية، ومراكز الاجتماعات والمطارات.
- مقاهي (الإنترنت).

الوصول إلى (الإنترنت) من خلال شبكات (الواي فاي) المفتوحة أو المدفوعة:

بدأت العديد من الدول ببناء نقاط لاسلكية للاتصال بـ (الإنترنت) سواء أكانت مجانية أم برسوم قليلة، حيث تعد المطارات والمكتبات والمراكز التجارية والأماكن المعروفة والمقاهي من الأمثلة على الأماكن التي توفر هذه الخدمة في دولة الإمارات العربية المتحدة، ولكن قد يتحتم عليك التسجيل في خدمة (الواي فاي) من أجل الحصول على الاتصال في المواقع المختلفة.

الهواتف الخلوية والمساعدات الرقمية الشخصية:

عرفت الهواتف الخلوية والمساعدات الرقمية الشخصية باستخدامها للحصول على خدمات (الإنترنت) لبعض الوقت. إن ميزة استخدام الهواتف المحمولة للاتصال بـ (الإنترنت) هي أنها ملائمة، وتتوفر بتكاليف زهيدة، وإن شراء هاتف محمول يعد أقل تكلفة بالطبع من شراء حاسوب محمول، كما أن حمل الهاتف المحمول في الأوقات كافّة أكثر سهولة إذا ما قارناه بالحاسوب المحمول.

تكافؤ فرص المشاركة الإلكترونية لأصحاب الهمم:

يعاني أصحاب الهمم من صعوبات متعددة عند محاولتهم الوصول إلى المعلومات من خلال استخدام (الإنترنت)، ولكن وزارة تمكين المجتمع في دولة الإمارات العربية المتحدة تعمل على وضع إستراتيجيات وخطط سياسات محددة لتمكين أصحاب الهمم من الحصول على المعرفة وصولًا إلى تمكينهم من استخدام مواقع (الإنترنت) وتطبيقات الهواتف الذكية.

تهدف هذه المبادرة إلى تمكين الأشخاص الذين يحتاجون إلى الوصول إلى المعلومات، بغض النظر عن مصادرها المختلفة، خاصة من خلال تعزيز مبادئ وممارسات الحكومة الذكية التي تهدف إليها وزارة تمكين المجتمع من أجل ضمان أن أصحاب الهمم قادرون على الحصول على المواد المرئية والسمعية والمكتوبة بشكل يتوافق مع المحتوى الرقمي، وقد بدأت بعض الهيئات بإدراك أهمية هذا الوصول، وخصوصًا في دبي، حيث بدأت الهيئة العامة للطيران المدني والتي تعد من أهم القطاعات بالبحث عن المواقع التي يتم تصميمها لتلائم احتياجات أصحاب الهمم، ولا سيما أصحاب التحديات البصرية، والتي تبين كيفية التواصل معهم بشكل سهل وميسر.

يعاني أصحاب الهمم من بعض العوائق عند محاولة الوصول إلى المعلومات عبر (الإنترنت)، لكنه توجد حلول عديدة للتغلب على هذه العوائق، وخصوصًا تلك التي تتعلق بإيجاد مزايا خاصة.

لتمكين الوصول لأصحاب الهمم، يمكن تقسيمهم إلى أربع فئات رئيسة على النحو الآتي:

1. أصحاب التحديات الحركية.
2. أصحاب التحديات البصرية.
3. أصحاب الصعوبات الإدراكية واللغوية.
4. أصحاب الصعوبات السمعية والصّم.

تظهر المعلومات التالية التفاصيل المتعلقة بالمشاكل التي يواجهها أصحاب الهمم، بالإضافة إلى ما يمكن فعله، أو ما تمّ فعله لمساعدتهم للوصول إلى (الإنترنت) واستخدامه.

نوع الإعاقة	الحلول
التحديات الحركية، صعوبة استخدام الفأرة، وصعوبة الضغط على الأزرار الصغيرة	استخدام اختصارات لوحة المفاتيح بدلًا من الفأرة. مثال: استخدام أمر (Tab) للتنقل أو استخدام اختصار لوحة المفاتيح (Ctrl+C) للنسخ.
التحديات البصرية أو عمى الألوان	◦ تكبير أو تحسين المنطقة التي يتم التركيز عليها. ◦ ضبط إعدادت الخط والألوان ومؤشر الفأرة حتى يتمكن المستخدمون من استخدام البرامج بسهولة. ◦ استخدام قارئ الشاشة التي تحول النص المكتوب إلى صوت مسموع. ◦ تحسين جودة الألوان، مع استخدام وسائل إيصال المعلومات في البرامج. ◦ يتعين على البرامج أن تكون متوافقة مع النمط الأحادي اللون. ◦ استخدام ألوان متمايزة في الظلام.
الصعوبات الإداركية واللغوية	◦ نماذج بسيطة ملائمة مصممة بشكل سهل ومباشر. ◦ استخدام برامج قراءة الشاشة التي تحول النص المكتوب إلى صوت مسموع.
الصعوبات السمعية والصّم عدم القدرة على سماع الأصوات	◦ إدراج أشكال مرئية للمعلومات المسموعة كافّة.

ولتقدير المرافق الرقمية يجب علينا عدم:

- إساءة استخدام المرافق الرقمية في تصفح المحتويات غير الأخلاقية أو نشرها، أو الانخراط في المقامرات غير المشروعة أو غيرها من الأنشطة اللا أخلاقية.
- تخريب مرافق (الإنترنت).
- الإضرار بسرعات (الإنترنت) من خلال تحميل ملفات ضخمة خلال ساعات الذروة.
- اختراق الشبكات.

المسؤوليات التي يجب إدراكها عند مشاركة المعلومات والمعرفة:

- عدم نشر المعلومات والأخبار المضللة وغير الصحيحة.
- عدم إطلاق الأحكام على الآخرين من خلال المدونات ومواقع (الإنترنت) والبوابات الاجتماعية؛ لأن هذا من شأنه إثارة المشاعر السلبية.
- التعامل برفق مع الأشخاص من المجموعات العرقية أو المعتقدات الدينية المختلفة، وبحسب الاحتياجات الوطنية.

مراجعة

1. اذكر ثلاث طرائق للاتصال بـ (الإنترنت)، وما الطريقة الأنسب لك؟ ولماذا؟

   - _____
   - _____
   - _____

2. أي من الخيارات التالية تعبر عن التقدير المناسب للتقنيات الحديثة؟

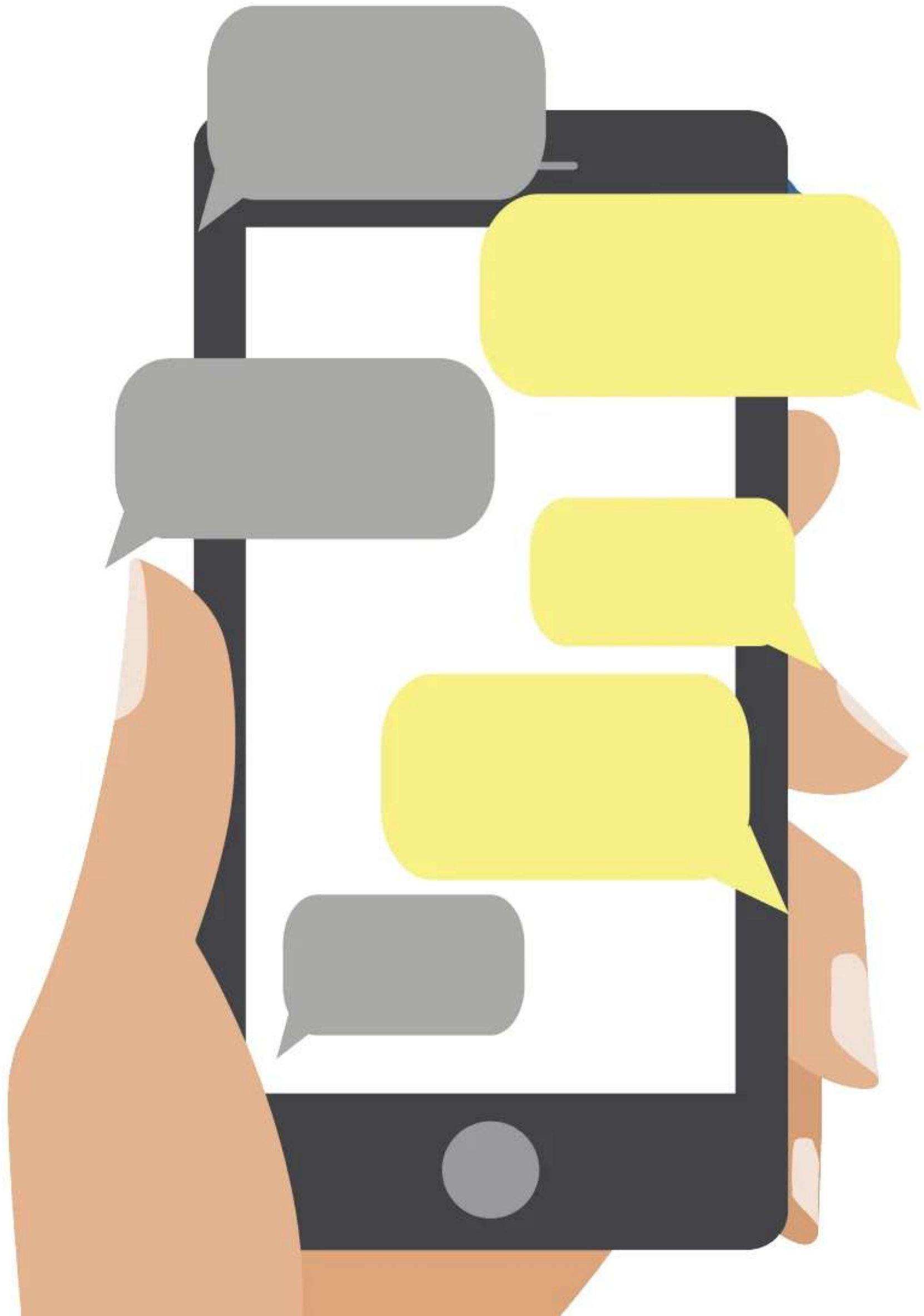
   - تصفح أو نشر المحتويات غير الأخلاقية.
   - الانخراط في مقامرات غير مشروعة أو أنشطة غير أخلاقية.
   - اختراق الشبكات.
   - الالتزام بالأخلاقيات الحسنة، وعدم الاشتراك في مقامرات غير مشروعة، وعدم تصفح أو نشر المحتويات غير الأخلاقية.

3. سجّل أبرز الصعوبات التي قد تواجه أصحاب الهمم في أثناء استخدام التقنيات الحديثة، وما الحلول المناسبة لمساعدتهم؟

   _____
   _____
   _____

4. وضح المسؤوليات التي تترتب عليك عند مشاركتك المعلومات والمعرفة.

   _____
   _____




02

الثورة الرقمية

تطور التقنيات الرقمية:

تتوفر العديد من الأجهزة الرقمية في الأسواق في وقتنا الحاضر، وقد تطورت هذه التقنيات من الأجهزة التقليدية إلى أجهزة رقمية ذات استخدامات متعددة، وعلى سبيل المثال، فقد تطورت الهواتف التقليدية إلى الهواتف المحمولة، كما تطور البريد التقليدي إلى البريد الإلكتروني، وتطورت الكتب والمراجع لتصبح محركات للبحث عبر (الإنترنت)، وهذه التطورات الرقمية المختلفة موضحة كما في الشكل.

لقد أدت هذه الأجهزة الرقمية ذات الاستعمالات المتعددة إلى تسهيل أنشطتنا اليومية، كما أنها مكنتنا من الوصول إلى (الإنترنت) في أي مكان وزمان، ولكن دون الإرشادات الملائمة، فقد تتم إساءة استخدام هذه الأجهزة من قبل أصحابها.

أدوات الثقافة الرقمية:

توجد أدناه العديد من التقنيات الرقمية الحالية التي تستخدم على نطاق واسع، فكم جزءًا منها يمثل من حياتك اليومية؟

الهواتف المحمولة:

بدءًا من الهواتف التقليدية القديمة، مكننا التطور الرقمي من استغلال التقنيات الرقمية بشكل كامل في تطوير الهواتف المحمولة، وتمتلك الهواتف الذكية التأثير الأساسي المرتبط بكيفية إنشاء واستخدام المعلومات الرقمية، فأصبحت جهاز التحكم الشخصي في حياتنا.

يمكننا القيام بالعديد من الأمور باستخدام هواتفنا المحمولة كالتقاط الصور و(الفيديوهات) ذات الوضوح العالي، وإرسالها، وإجراء الاتصالات المرئية باستخدام تطبيقات الجيل الثالث، وحتى العثور على إرشادات الطريق للوصول إلى منازل أصدقائنا وأقاربنا باستخدام نظام تحديد المواقع العالمي (GPS) المدمج في هواتفنا.

إضافة إلى ذلك، تمتلك الهواتف الذكية في وقتنا الحاضر القدرة على الوصول إلى (الإنترنت)، حيث يمكننا تصفح المواقع، وإرسال رسائل البريد الإلكتروني، أو حتى متابعة أسواق الأسهم طوال الوقت، كما يمكننا نقل وتخزين الصور و(الفيديوهات) والملفات بسهولة على حواسيبنا.

المكونات الذكية:

تمكننا التقنيات الحديثة من تطوير تطبيقات رقمية صغيرة تعتمد على الحاسوب، وتعرف باسم (المكونات الذكية).

تتضمن استخدامات المكونات الذكية في الوقت الحاضر بطاقات الهوية الشخصية، وبطاقات الائتمان، والبطاقات البنكية، وجوازات السفر وغيرها.

تمكن تقنيات المكونات الذكية من تخزين برامج ومعلومات بسيطة في مكون ما.

كما يمكن استخدام المكونات الذكية في تتبع الحيوانات والطيور، ويستطيع العلماء مثلًا استخدام مكونات ذكية لتتبع حركة الحيتان في المحيطات لتحليل سلوكاتها والمجتمعات التي تعيش فيها.

بطاقة الهوية الإماراتية:

بطاقة الهوية الإماراتية عبارة عن بطاقة بلاستيكية تستخدم كوثيقة سفر للتنقل بين دول مجلس التعاون الخليجي، وكبديل عن جواز السفر، إضافة إلى استخدامات أخرى لهذه الهوية.

تلفاز الأقمار الصناعية:

توفر أجهزة التلفاز التقليدية عددًا محدودًا من القنوات، ولكن في وقتنا الحاضر يمكننا متابعة عدد كبير من القنوات التلفزيونية، وبالاعتماد على البث الرقمي للقنوات فقد أصبح بإمكان كل من يمتلك جهاز استقبال رقمي التمتع بالعديد من القنوات التلفزيونية بغض النظر عن موقعه، وعادة ما يتم تقديم هذه الخدمات من قبل موفري خدمات التلفاز المحليين بمقابل مادي بسيط.

منصات الألعاب:

مكن التطور الذي طرأ على منصات الألعاب من تغلب الألعاب ثلاثية الأبعاد على الألعاب ذات الأبعاد الثنائية، حيث تمكن الصور ذات الوضوح الأعلى والأكثر واقعية المستخدمين من الاستمتاع بشكل أكبر بهذه الألعاب، كما غدا العديد من هذه المنصات أكثر تفاعلية، وسمحت للاعبين بتجربة ألعاب أكثر واقعية من ذي قبل.

تطبيقات الثقافة الرقمية:

يتواصل الأشخاص حول العالم من خلال (الإنترنت) باستخدام البريد الإلكتروني والرسائل الفورية ومواقع التواصل الاجتماعي وغيرها من التطبيقات.

(ويب 2.0):

(ويب 2.0) هو الجيل الثاني من (الإنترنت)، وبدلًا عن صفحات (الويب) الثابتة، فقد أصبحت صفحات (الويب) مفعمة بالحيوية، وتتيح مشاركة المحتويات والتواصل الاجتماعي، كما أصبح المستخدمون هم من يقومون بإنشاء المحتوى بدلًا من مجرد متصفحين له، حيث يستطيع أي شخص كان من إنشاء الموقع الخاص به لتحميل المقاطع الصوتية والمرئية ونشر الصور والمعلومات وتنفيذ العديد من الأمور والمهام الأخرى.

الرسائل الفورية:

الرسائل الفورية، والتي تعرف غالبًا باختصار (IM)، هي نوع من خدمات الاتصال التي تتيح لك إنشاء ما يشبه غرف المحادثة الخاصة نوعًا ما مع شخص آخر من أجل التواصل معه في الوقت نفسه عبر (الإنترنت).

عادة ما يقوم نظام الرسائل الفورية بإرسال تنبيهات لك في حال تواجد أحد من معارفك في حال اتصال، وبعد ذلك يمكنك البدء بجلسة محادثة مع الشخص المعني.

توفر غالبية برامج المحادثة إمكانية التواصل الصوتي والمرئي، ومع هذه الميزات، فقد أصبح المستخدمون جميعهم في أنحاء العالم كافّة قادرين على التواصل إلكترونيًّا مع بعضهم.

مواقع التواصل الاجتماعي:

مواقع التواصل الاجتماعي هي عبارة عن مجتمعات افتراضية تضم أشخاصًا لهم اهتمامات متشابهة، وتمكنهم من التواصل مع بعضهم لتبادل الآراء ومشاركة المعرفة، كما يمكن اعتبارها على أنها خدمة تركز على بناء شبكات أو علاقات اجتماعية بين الناس، وعادة ما يكون التسجيل مجانيًّا، ومن الأمثلة على بعض مواقع التواصل الاجتماعي (فيسبوك) و(تويتر) وغيرها.

وفي معزل عن الاستخدام الواضح كوسيلة للتواصل مع زملاء الدراسة، والبقاء على اتصال مع الأصدقاء، فقد استخدمت مواقع التواصل الاجتماعي كوسيلة لنشر المعلومات المتعلقة بأسباب بعض الأحداث على الصعيد العالمي، مثل: الأحداث التي وقعت في عدد من الدول مؤخرًا.

http://www.facebook.com

https://www.linkedin.com

http://www.twitter.com

http://www.instagram.com

مواقع (الفيديوهات) الاجتماعية:

توفر مواقع (الفيديوهات) الاجتماعية إمكانية الوصول إلى (الفيديوهات) التي يقوم بنشرها المستخدمون الآخرون حول العالم، ومن الأمثلة على هذه المواقع:

http://blip.tv

http://www.youtube.com

نشاط

1. اذكر ثلاث تقنيات حديثة تطورت في آخر 5 سنوات؟
2. استخدم أحد أصدقائك تقنية الرسائل الفورية لنشر الشائعات، فبماذا تنصحه؟

التطبيقات عبر الإنترنت:

الحكومة الإلكترونية:

يستخدم مصطلح الحكومة الإلكترونية لوصف استخدام التقنيات لتسهيل عمل الحكومة وتوفير المعلومات والخدمات الحكومية.

توفر الحكومات حول العالم في الوقت الحاضر بوابات عبر (الإنترنت) للجمهور لتمكينهم من الوصول إلى البرامج والخدمات الحكومية. حيث تساعد هذه التقنية المسؤولين الحكومين من البقاء قريبين من العامة وبالتالي تعزيز الفهم لديهم حول المخططات والمبادرات الحكومية المجتمعية.

إضافة إلى ذلك، يستطيع المستخدمون الاطلاع على نشاطات الهيئات والمؤسسات الحكومية وأحدث الأخبار المتعلقة بها، كما يستطيع المستخدمون تحميل النماذج والتقديم على الوظائف وارسال الشكاوى وحتى دفع الرسوم والضرائب عبر (الإنترنت)، تاليًا بعض الأمثلة على البوابات الحكومية عبر (الإنترنت).

التعلم الإلكتروني:

التعلم الإلكتروني أو التعلم عبر (الإنترنت) هو طريقة جديدة للحصول على المعلومات والمعرفة باستخدام تقنيات المعلومات والاتصال، تتيح هذه الطريقة إعادة صياغة عملية التعليم والتعلم ضمن عالم رقمي، وهي تعني باختصار إتاحة القدرة على التعلم من خلال الشبكات أو من خلال الإنترنت. يتيح التحول من صفوف الدراسة التقليدية إلى التعلم الإلكتروني تجربة تعليمية ممتعة تمكن الطالب والمعلم على حد سواء من الاستفادة من الأدوات والمهارات الجديدة من أجل تحقيق نمو وازدهار في مجتمع المعلومات.

أطلقت العديد من المؤسسات التعليمية حول العالم أنظمة لاتاحة التعلم الإلكتروني مثل (مودل) و(بلاك بورد) و(إدمودو)،

حيث يتمكن الطلاب من التفاعل مع معلميهم من خلال بوابات رقمية عبر (الإنترنت)، ومن الأمثلة على هذه البوابات التعليمية:

- جامعة حمدان بن محمد. (https://www.hbmsu.ac.ae)
- جامعة أبوظبي. (http://www.adu.ac.ae/prospects.html#cstudents)
- جامعة خليفة. (https://elearn.kustar.ac.ae)

- ناقش مع زملائك التكنولوجيا التي يمكن أن تختفي خلال السنوات القادمة.

مراجعة

1. سجل ثلاثًا من التقنيات الرقمية التي تستخدم عالميًّا في الوقت الحالي، وما استخداماتك لها؟
   - _____
   - _____
   - _____
2. (تعد الرسائل الفورية واحدة من تطبيقات الاتصال الحديثة التي نستخدمها بشكل يومي)، ما تطبيقات الرسائل الفورية التي تستخدمها؟ وما الطريقة الأخلاقية لاستخدامها؟
   - _____
   - _____
3. تعد الحكومة الإلكترونية واحدة من تطبيقات (الإنترنت)؟ (صحيح - خطأ).
4. وضح المقصود بالمفاهيم والمصطلحات الآتية:
   - التعلم الإلكتروني: _____
   - المكونات الذكية: _____
5. وضح أهميتين اثنتين لكل مما يأتي:
   - مواقع التواصل الاجتماعي:

_____

_____

- توفير الحكومات البوابات الإلكترونية عبر (الإنترنت) للجمهور:

- الأجهزة الرقمية:

التسوق عبر (الإنترنت)

أنواع التعاملات عبر (الإنترنت):

التجارة الرقمية (التسوق الإلكتروني):

تعني التجارة الرقمية أو التسوق عبر (الإنترنت) تنفيذ الأعمال التجارية التي تتضمن بيع وشراء المنتجات والخدمات عبر (الإنترنت).

تسعى العديد من المؤسسات الرائدة في الوقت الحاضر إلى تبنّي هذا النمط لتنفيذ الأعمال التجارية من أجل الحصول على حصة سوقية كبيرة.

توفر المواقع الرائدة للتسوق الإلكتروني لعملائها إمكانية تنفيذ التعاملات عبر (الإنترنت) بأمان، حيث يستطيع المشترون من خلال حواسيبهم تأكيد عمليات الشراء، وتنفيذ عمليات الدفع عبر (الإنترنت)، وبعدها يتم شحن المشتريات مباشرة وإرسالها إلى عنوان المشتري.

وللأسف، فقد تتسبب عمليات الشراء عبر (الإنترنت) أحيانًا في إقلاق المشتري حيال بعض الأمور، وخاصة في حال تأخر عملية توصيل المنتج، أو عدم توافق جودة المنتج مع المواصفات المعروضة على الموقع، أو حتى عدم وصول المنتج نهائيًّا.

ما الذي يتوجب عليك فعله قبل تنفيذ التعاملات المالية عبر (الإنترنت)؟

توفر المواقع الموجودة على (الإنترنت) مجموعة محددة من المعلومات الضرورية التي يجب مراعاتها قبل تنفيذ التعاملات عبر (الإنترنت) والتي تتضمن:

الشراء عبر (الإنترنت):

ابحث عن المواقع التي توفر عملية دفع آمنة.

احذر من استخدام الشبكات اللاسلكية العامة نظرًا لكونها غير آمنة.

تأكد من معرفة اسم التاجر وبياناته الكاملة، تساعدك هذه البيانات في الإبلاغ عن العمليات الاحتيالية.

احذر من العروض الوهمية أو الاحتيالية.

تأكد من أن الشركة تتبع سياسة لحماية الخصوصية والتي تمكنك من معرفة ما الذي يمكن للشركة فعله ببياناتك الشخصية.

لا تثق بنتائج محركات البحث.

حافظ على خصوصيتك، لا تقم بالإفصاح عن بياناتك الشخصية.

احذر من رسائل البريد الإلكتروني التي تحتوي على عروض مثل "احصل على عروض على رحلات العطلات" أو "هذا الموقع يقدم خصمًا لغاية 50%"، يمكن أن تعرضك هذه المواقع لبرمجيات خبيثة.

نصائح

ما الذي يمكنك القيام به لحماية نفسك؟

1. تأكد من المنتج من خلال الهاتف أو البريد الإلكتروني.
2. استخدم بطاقة ائتمان لإتمام عملية الدفع حتى تكون قادرًا على تتبع كافة تعاملاتك.
3. إذا كنت تجري عملية الدفع عبر (الإنترنت)، تأكد من كون الموقع آمنًا من خلال تفقد ختم أو سياسة الحماية الخاصة بالشركة.

نشاط

- ناقش مع زملائك كيفية حماية نفسك في أثناء استخدام (الإنترنت)، وما الطرائق التي ستتبعها لتنفيذ ذلك؟

نشاط

- حفظ بيانات بطاقة الائتمان عند التسوق على (الإنترنت) تساعدك على توفير الوقت في عملية الشراء في المستقبل من الموقع نفسه. ناقش ذلك.

مراجعة

1. يجب عليك مراعاة الأمور الآتية قبل تنفيذ أية تعاملات مصرفية عبر (الإنترنت). (اختر إجابتين).
   - إن الموقع يستخدم (بروتوكولًا) آمنًا للاتصال.
   - لا تقم بفتح رسائل البريد الإلكتروني ومرفقاتها.
   - استخدام كلمة مرور لا تقل عن ثمانية أحرف أو أرقام.
   - التأكد من مواصفات السلع أو الخدمات المقدمة.

2. سجل ثلاث طرائق يتعين عليك اتباعها حتى تحمي نفسك في أثناء التسوق عبر (الإنترنت).
   - _____
   - _____
   - _____

3. احذر من الرسائل الاحتيالية والعروض الوهمية، فقد يكون الموقع المعلن وهميًّا، ويقوم بتثبيت برامج غير ملائمة على جهازك.
   ما الإجراءات التي ستتخذها في حال وصول الرسائل الاحتيالية والعروض الوهمية إلى جهازك؟
   - _____
   - _____

5. صمم مخططًا ذهنيًّا يوضح أبرز مزايا وعيوب التجارة الرقمية.

04

التقنية والجريمة

الجرائم الإلكترونية:

مفهوم الجرائم الإلكترونية:

إذا كنت تعتقد أن الجرائم تقتصر على الأنواع التي ترتكب في العالم الحقيقي، فيجب عليك في هذه الحالة إعادة التفكير مرة أخرى.

هناك فعليًّا العديد من الجرائم التي ترتكب في العالم الافتراضي، ومنها ما تزيد خطورته عن تلك التي ترتكب في العالم الحقيقي، وهذا النوع من الجرائم التي ترتكب باستخدام التقنيات تُعرف باسم (الجرائم الإلكترونية).

تعرف الجرائم الإلكترونية أيضًا باسم جرائم (الكمبيوتر) أو الجرائم الرقمية، وتشترك هذه المسميات جميعها في أنها تشير إلى الجرائم التي ترتكب باستخدام التقنيات، وهذه الجرائم هي عبارة عن استخدام أجهزة (الكمبيوتر) لإخافة الناس، أو للاحتيال عليهم، أو للاستيلاء على معلوماتهم المهمّة، وقد تحولت العديد من الجرائم التقليدية التي ترتكب في العالم الحقيقي، مثل: الابتزاز، والتزوير، والسرقة، وغسيل الأموال والاختلاس إلى جرائم إلكترونية؛ نظرًا لكون مجرمي (الإنترنت) قادرين على استخدام (الإنترنت) لتنفيذ جرائمهم، حيث يتيح (الإنترنت) وبكل سهولة الوصول إلى شبكة عالمية تحتوي معلومات عن الناس والشركات والأسواق، وهذا بدوره يؤدي إلى تسهيل ارتكاب المزيد من الممارسات غير الأخلاقية.

أمثلة على الجرائم الإلكترونية:

سنتعرف من خلال هذا الموضوع الفرعي على أنواع الجرائم الإلكترونية، بالإضافة إلى استعراض التفسيرات، ودراسة حالات لجرائم إلكترونية حقيقية تم ارتكابها، وبعد ذلك ستكون قادرًا على تحديد الأنشطة التي تعتبر جرائم إلكترونية، إضافة إلى القدرة على رصد السمات التي قد تشير إلى كونك مجرمًا أو ضحية، وإليك بعض الأمثلة على جرائم إلكترونية حدثت على مدار الأعوام السابقة.

ما التصرف الأخلاقي الذي سوف تتخذه في حال قيام عضو في إحدى مجموعات المحادثة التي تشترك فيها بإهانتك؟

التحرش:

يرتكب هذا النوع من الجرائم للحط من قدر شخص ما لإرضاء الذات دون الحصول على أية مكاسب مادية، ويعرف التحرش على أنه التصرفات المتلاحقة أو المزعجة وغير المرغوب فيها، والتي ترتكب من قبل شخص واحد أو مجموعة من الأشخاص، وتتضمن تهديدات ومطالب مدفوعة بدوافع متعددة مثل: الأحقاد الشخصية، وقد تكون عبارة عن محاولات لإجبار شخص ما للاستقالة من عمله أو حتى تحقيق المتعة الشخصية.

الابتزاز:

الابتزاز عبارة عن تصرف، ويعد جريمة تتضمن تهديدات غير مبررة للحصول على مكاسب من الآخرين، أو لإلحاق الضرر به ما لم يقم بتحقيق مطالب المبتز، وهي عبارة عن الإجبار الذي يتضمن تهديدات بإلحاق الضرر الجسدي، أو التهديد بالملاحقة القانونية أو تلك التهديدات التي تهدف إلى التمكن من الاستيلاء على أموال الشخص أو ممتلكاته.

قانون الدولة للجرائم الإلكترونية.

بحسب المادة رقم(16) من قانون الجرائم الإلكترونية، يعاقب بالحبس مدّةً لا تزيد عن سنتين، وبغرامة لا تقل عن مائتين وخمسين ألف درهم، ولا تتجاوز خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين كُلَّ من ابتزّ، أو هدد شخصًا آخر لحمله على القيام بفعل، أو الامتناع عنه، وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات.

وتكون العقوبةُ السجنَ لمدّة لا تزيد عن عشر سنوات إذا كان التهديد بارتكاب جناية، أو بإسناد أمور خادشة للشرف أو الاعتبار.

دراسة حالة

العشرات من الفتيات تم ابتزازهم عاطفيًّا:

مؤخرًا تم اعتقال رجل بسبب قيامه بابتزاز وتهديد العديد من الفنيات، حيث تلقت إدارة الجريمة الإلكترونية شكاوى وبلاغات من (20) فتاة تقريبًا تتراوح أعمارهن بين (16) و(20) عامًا تفيد بتعرضهن للابتزاز، وبحسب مدير إدارة التحقيقات الإلكترونية الرائد سعيد الهاجري، فقد قام الجاني الذي يبلغ من العمر (21) عامًا بانشاء موقع على (الإنترنت) يحتوي على عدد من النشاطات الترفيهية لجذب المراهقات، حيث كان يطلب من كل من يقوم بزيارة الموقع ادخال عناوين البريد الإلكتروني وكلمات المرور الخاصة بهم، وبعد ذلك يتم استغلال عناوين البريد الإلكتروني الخاصة بالفتيات في الاستيلاء على صورهن ومعلوماتهن الشخصية، كما قام الجاني باستخدام هذه العناوين في التواصل مع أصدقاء أولئك الفتيات من أجل الحصول على الصور، ثم يقوم بعد ذلك بتهديد الفتيات بنشر بيانتهن ومعلوماتهن الشخصية عبر (الإنترنت) ووضعها في مواقع غير أخلاقية.

وبحسب الهاجري، قامت الادارة فورًا بتشكيل فريق لتحديد أسلوب الشاب بعد تلقي البلاغات وتحديد مكانه، وتم بالفعل إلقاء القبض عليه بعد استيفاء كافة الإجراءات القانونية. وحذر الهاجري جميع الفتيات من مغبة الاحتفاظ بالصور أو الفيديوهات الشخصية على هواتفهن المحمولة أو البريد الإلكتروني أو حتى على حواسيبهن الشخصية ما لم تكن محمية ببرامج حماية ملائمة.

[Emarat Al Youm, 1 April, 2010, http://www.emaratalyoum.com/local-section/accidents/2010-04-01-1.101363]

التعدي على حقوق الملكية الفكرية:

يعد التعدي على حقوق الملكية الفكرية من أكثر الأنشطة الإجرامية انتشارًا، والتي تستهدف الأعمال التجارية، وتتضمن - عادة - استخدامًا أو إعادة إنتاج غير قانوني للمعلومات أو التقنيات المملوكة للآخرين قانونيًّا، حيث تمكن التطورات الحاصلة في مجال تقنيات المعلومات من نسخ المعلومات أو التقنيات الهامة والاحتفاظ بها بشكل رقمي.

نشاط

كيف يمكنك استخدام الموارد المشتركة عبر (الإنترنت) دون انتهاك حقوق الملكية الفكرية للمؤلف؟

قرصنة البرامج:

قرصنة البرامج هي أمر واسع الانتشار بين مستخدمي الحواسيب و(الإنترنت)، حيث يقوم الناس -عادة- بمشاركة البرامج التي يقومون بشرائها ظنًا منهم أنه لا ضير في مثل هذا التصرف، ويمكن أن يحصل مثل هذا الأمر في أماكن العمل، حيث يقوم بعض الموظفين -عادة- بتثبيت النسخة نفسها من برنامج ما على عدة أجهزة، رغم أن هذه النسخة مرخصة للاستخدام على جهاز واحد فقط، وقد يتم هذا الأمر من قبل رؤسائه في العمل، وبمحاولة منهم لخفض كلفة شراء البرامج.

تعد هذه التصرفات منافية للقانون، وكل من يتم ضبطه يقوم بمثل هذه التصرفات قد يتعرض للغرامة أو قد يحكم عليه بالسجن، تكمن المشكلة في اعتقاد الكثير من الناس بأن قرصنة البرامج لا تعد أمرًا ذا أهمية نظرًا لكونها لا تلحق الضرر بأحد لأن شركات البرمجيات -في نظرهم- قد حققت مكاسب مالية ضخمة، وأن القليل من قرصنة البرامج بهذا الشكل لن تلحق الضرر بهذه الشركات على المدى الطويل.

الوصول غير المصرح به:

يعد الوصول غير المصرح به لأجهزة الكمبيوتر والشبكات والخوادم من الأمور المستجدة في عالم تقنيات المعلومات، ويسمى الشخص الذي يتمكن من الوصول بشكل غير مصرح به بالمخترق أو المخرب.

قانون الدولة للجرائم الإلكترونية.

المادة رقم (2): إن أيّ فعل متعمد يؤدي إلى إلغاء أو تدمير أو الكشف عن أسرار، أو إعادة نشر معلومات شخصية أو رسمية يعد جريمة، وتنص على أن أي شخص يدان بالدخول إلى موقع أو نظام للمعلومات يعاقب بالسجن أو بالغرامة أو بكليهما، وإذا أسفر الفعل عن إلغاء المعلومات أو تدميرها أو الكشف عنها أو تغييرها أو إعادة نشرها يُحكم عليه بالسجن لمدة لا تقل عن ستة أشهر، أو بالغرامة أو بكليهما، وإذا كانت هذه المعلومات شخصية، فَتُفرض غرامة لا تقل عن (200,000) درهم، بالإضافة إلى عقوبة السجن لمدة لا تقل عن سنة واحدة، أو بإحدى العقوبتين على مَن يثبت قيامه بهذا الفعل.

المحتوى غير الأخلاقي:

وهو نشاط يتم على شكل كتابة أو صور أو مقاطع (فيديو) لا تحتوي على اي قيمة أدبية أو فنية، يمكن العثور على الملايين من الصور والمقاطع غير الأخلاقية عبر (الإنترنت)، وهي واحدة من أكثر المشاكل التي تتسبب في إثارة القلق حول العالم.

قانون الدولة للجرائم الإلكترونية.

بناء على المادة رقم (17): يعاقب كل من يدان بإنتاج أو إعداد أو إرسال أو حفظ المعلومات بقصد استغلالها أو توزيعها أو تزويد الآخرين بمعلومات تلحق الضرر بالأخلاقيات العامة عن طريق (الإنترنت) أو وسائل التكنولوجيا، بالسجن مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن (250) ألف درهم.

وتنص المادة (19) على معاقبة أي شخص يدان بتحريض أو إغراء ذكر أو أنثى على ارتكاب الزنا أو البغاء باستخدام (الإنترنت) أو وسائل التكنولوجيا المعلومات بالسجن والغرامة.

وإذا كان الضحية حدثًا، فإن عقوبة السجن لا تقل عن خمس سنوات إضافة إلى غرامة لا تتجاوز (5) ملايين درهم.

التسلل:

ويعرف التسلل على أنه دخول غير قانوني أو هجومي أو غير مصرح به إلى منشأة أو نظام ما.

دراسة حالة

دراسة حالة، قيام مجموعة من المخترقين بالتسسل إلى شبكة النظام المصرفي في دولة الإمارات العربية المتحدة:

دبي: عصابة مكونة من أربع أشخاص من احدى 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 أحدى 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 واثناء 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)

التعدي:

يعرف التعدي على أنه الأعمال التي تتسبب في إثارة الغضب أو الاستياء أو الكراهية أو عدم الارتياح أو إهانة الغير. على سبيل المثال، تعد الإساءة إلى أي من قوانين الشريعة الإسلامية أو القيم الاجتماعية أو ما يقال ضد الأديان المعترف بها على أنها جريمة.

قانون الدولة للجرائم الإلكترونية.

تنص المادة رقم (35) على: مع عدم الإخلال بالأحكام المقررة في الشريعة الإسلامية، يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين الف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من ارتكب عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات أو على موقع إلكتروني،

ومن ضمن الجرائم:

1. الإساءة إلى أحد المقدسات والشعائر الإسلامية.
2. الإساءة إلى أحد المقدسات أو الشعائر المقررة من الأديان الأخرى.
3. سب أحد الأديان السماوية المعترف بها.

وإذا تضمنت الجريمة إساءة للذات الإلهية او لذات الرسل والأنبياء أو كانت مناهضة للدين الإسلامي أو 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 حبذ لذلك أو روج له، فيعاقب بالسجن مدة لا تزيد على سبع سنوات.

نشاط

ناقش مع زملائك ثلاثة إحتياطات يمكن إتباعها لتجنب المشاركة في الجريمة الإلكترونية.

قانون الدولة للجرائم الإلكترونية.

كما تنص المادة رقم (21) على: 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 معلومات إلكتروني ، أو إحدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانونا **بإحدى الطرق التالية:**

01 **استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية إو مرئية.**

02 **التقاط صور الغير أو إعداد صور إلكترونية أن نقلها أو كشفها أو نسخها أو الاحتفاظ بها.**

03 **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.

أسباب الجرائم الإلكترونية:

قد يتم ارتكاب الجرائم الإلكترونية عن طريق:

كيف تحمي نفسك من الوقوع كضحية لجريمة إلكترونية:

دعنا نجلس للحظة ولنعد التفكير مرة أخرى، لماذا تتزايد أعداد الجرائم الإلكترونية المرتكبة بشكل يومي؟ لماذا يقع العديد من الناس ضحية للجرائم الإلكترونية؟ لأنه من الممكن ألا تكون المشكلة كامنة في جشع وأنانية المجرمين فقط.

ما لا ندركه هو أن أولئك الأشخاص الذين يقعون ضحية لجرائم إلكترونية قد ساهموا بخطأ ارتكبوه في الجرائم الإلكترونية التي ارتكبت في الحقيقة إن تجاهلنا هو السبب في ارتكاب جرائم إلكترونية بحقنا بدءًا من عمليات الاحتيال البسيطة على بطاقات الائتمان وصولًا إلى السطو على البنوك.

نميل في بعض الأحيان إلى إعطاء معلوماتنا الحساسة والشخصية إلى مواقع غير موثوقة، كما قد نفشل في اتخاذ إجراءات الحماية الملائمة لمنع الوصول إلى أجهزتنا أو اقتحامها، بالتالي فإن إجراءات الحماية التي يتم اتخاذها، إضافة إلى الوعي عند تصفح المواقع يلعبان دورًا هامًا لضمان حماية معلوماتنا الشخصية.

- لا تقم بفتح الرسائل والمرفقات التي تصلك من أشخاص غير معروفين بالنسبة لك.
- لا تقم بفتح الملفات ذات الإمتداد (EXE) أو الملفات غير المعروفة مباشرة من بريدك الإلكتروني.
- لا تقم بكتابة اسم المستخدم الخاص بك وكلمة السر في الصفحات التي تصل إليها من خلال روابط تصلك من بريد إلكتروني لا تعرفه أو في النوافذ المنبعثة، وبدلًا من ذلك اكتب اسم الموقع بنفسك في المتصفح.
- لا تجعل هاجسك بحماية نفسك يتحول إلى نقطة ضعف.
- لا تتصفح المواقع المشبوهة أو الغير أخلاقية لأنها تزيد من احتمالية تعرضك لهجمة إلكترونية، إحم نفسك وتصفح المواقع الآمنة.
- 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.

- قم بشراء برنامج جيد للحماية من الفيروسات وواظب على تحديثه باستمرار (مرة واحدة أسبوعيًّا على الأقل).
- قم بفحص جميع وحدات التخزين والأقراص المحمولة من الفيروسات قبل استخدامها.
- قم بتأمين متصفح (الإنترنت) الخاص بك.
- قم بعمل نسخ احتياطية من بياناتك وتأكد من سلامتها.
- قم بتثبيت التحديثات الدورية لنظام التشغيل على جهازك.
- إذا كنت تمتلك اتصالًا عالي السرعة بالإنترنت في مكان عملك، قم بشراء برامج أو أجهزة جدران الحماية لتأمين أنظمة الكمبيوتر لديك.
- إذا كنت تستخدم أنظمة الشبكات اللاسلكية فتأكد من حمايتها وخذ وقتك في فهم آلية عملها.
- تصرف بمسؤولية وخذ وقتك في تعلم كيفية الاعتناء بجهازك.
- تذكر أن جهاز كمبيوترك مثل السيارة من ناحية احتياجه لتنفيذ بعض الصيانة الأساسية من أجل إبقاءه يعمل بصورة جيدة.

مصداقية المصادر المتوفرة عبر (الإنترنت):

بعد أن أصبح بإمكان أي كان أن يصبح مالكًا أو مؤلفًا لمحتوى ما عبر (الإنترنت)، فقد باتت مصداقية المواد التي يتم نشرها عبر (الإنترنت) موضعًا للشك.

وعلى الرغم من هذا كله، ونظرًا للثورة الحاصلة في عمليات البحث الحديثة، فإنه تتوفر كميات هائلة من المعلومات التي لم تكن متاحة في السابق للباحثين عبر (الإنترنت)، ويخسر الباحثون الذين لا يستفيدون من هذه الميزة الكثير.

الطرائق الشائعة للتمييز بين الجيد والسيء:

- ابحث عن المواقع المعروفة ذات السمعة الطيبة، كموقع (بي بي سي) على سبيل المثال: (www.bbc.com)، فهو عبارة عن شبكة إخبارية باللغة الإنجليزية، وتتوفر منه نسخة باللغة العربية، ويقع المكتب الرئيسي في لندن، وفي الشرق الأوسط يقع المكتب الرئيسي في القاهرة، بالإضافة إلى قرابة (72) مكتبًا إخباريًّا 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، وغالبًا ما تعتبر المواقع التي تنتهي بالنطاق (gov) مصدرًا للبيانات الحكومية، وبناء عليه فإن موقعًا مثل:(www.moe.gov.ae) يعتبر من المواقع الحكومية الموثوقة في دولة الإمارات.
- لاحظ أن أغلب المواقع التجارية تستخدم النطاق (com) ولذلك يجب عليك التعامل معها بحذر.
- إن المواقع التي تحتوي على اسم المؤلف وشهاداته 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، ويمكنك التأكد من دقة الحقائق والأرقام طالما أنها منسوبة إلى مصدر معين.

مراجعة

1. أكتب ثلاثًا من الجرائم الإلكترونية الشائعة التي قد تتعرض لها أنت أو أصدقاؤك؟
   - ---
   - ---
   - ---
2. بيِّن أهم الأسباب الشائعة التي قد تؤدي لجرائم إلكترونية؟
   - ---
   - ---
   - ---
3. وضح أبرز الطرق التي توفر لك الحماية من الوقوع كضحية لجريمة إلكترونية؟
   - ---
   - ---
   - ---
   - ---
4. أوضح المقصود بالمفاهيم والمصطلحات الآتية:
   - الجرائم الالكترونية:

- التحرش:

- الابتزاز:


05

الاستخدام الآمن والأخلاقي للتقنيات

الأنماط الشائعة للانتهاكات الرقمية:

سرقة الهوية:

تتم سرقة الهوية عند قيام أحدهم باستخدام معلوماتك الشخصية، مثل الاسم والعنوان والمعلومات المصرفية بشكل غير قانوني لتحقيق مكاسبهم، وبمجرد استطاعة اللصوص الإلكترونيين من الوصول إلى معلوماتك الشخصية، فسيكونون قادرين على تنفيذ عمليات شراء باستخدام بطاقة الائتمان الخاصة بك أو حتى فتح حساب ائتماني جديد باسمك.

إن الضرر الناجم عن سرقة الهوية ليس ماديًا فقط، إذ قد يتم إشراك الضحايا في أنشطة إجرامية لم يقوموا بها أساسًا.

نصائح لتجنب الوقوع كضحية لجريمة سرقة الهوية:

- لا تقم بالرد أو الإجابة على الرسائل المشبوهة.
- كن حذرًا من محاولات أحدهم للتظاهر بأنه شخص آخر، إذْ يحاول المستغلون التظاهر بأنهم أشخاص من عمر وخلفية مختلفة عن الواقع في محاولة لإقناعك بإضافتهم (كأصدقاء).
- لا تقم أبدًا بمشاركة معلوماتك الشخصية عبر (الإنترنت) مع أي كان، إن أية معلومة مثل رقم الهاتف وعنوان المنزل يمكن أن تشكّل نقطة بدء للمجرمين لاصطيادك.
- استخدم الخيارات التي توفرها إعدادات الخصوصية في مواقع التواصل الاجتماعي؛ لأنها ستساعدك في تأمين معلوماتك، ويمكن اختيار مجموعة من الأصدقاء فقط لتمكينهم من الاطلاع على بياناتك الشخصية، وألا يكون ذلك للناس كافّة.
- وتذكّر أن ما تنشره عبر (الإنترنت) لن يبقى خاصًا بك، ويستطيع والداك ومعلموك وأرباب العمل المحتملين البحث عبر (الإنترنت) ومعرفة من تكون.
- لا تقم بوضع بياناتك كاملة في أي ملف تعريف شخصي على حساباتك عبر (الإنترنت)، حيث يتوجب عليك الإقلال من المعلومات التي تنشرها عبر (الإنترنت).
- هل حاولت البحث عن نفسك يومًا ما عبر (الإنترنت)؟ جرب الآن، وقد تتفاجأ بأن أحدهم قد قام بنشر معلوماتك الشخصية على (الإنترنت).

التصيد باستخدام رسائل البريد الإلكتروني:

التصيد هو عبارة عن رسائل بريد إلكتروني احتيالية تتمثل في قيام المهاجمين بارسال رسائل تبدو في ظاهرها شرعية وذات مصداقية في محاولة لجمع معلومات مالية وشخصية من المستلمين لهذه الرسائل.
يقوم المهاجمون بارسال رسالة بريد إلكتروني إلى عناوين عشوائية مدعين بأنهم من أفراد معروفون أو من جهات معروفة سعيًا لإجبار المستلم على الضغط على الرابط المرفق في الرسالة والمؤدي إلى موقع وهمي. قد يكون من الصعب التفريق بين الموقع الأصلي والوهمي نظرًا لقيام المجرمين بنسخ الموقع الأصلي بكل تفاصيله، وإذا قمت بزيارة مثل هذه المواقع دون أن يكون لديك برامج حماية ملائمة أو متصفح محمي، فإن باستطاعة المخترقين في هذه الحالة تثبيت برمجيات خبيثة على جهازك كأحصنة طروادة على سبيل المثال. تبدو أحصنة طروادة عادة كبرامج لا تتسبب بأي أضرار مثل ألعاب أو رسائل بريد إلكتروني ذات مرفقات. وعادة ما يتطلب تفعيل هذا النوع من البرمجيات قيام المستخدم بالضغط على الرابط أو فتح الملف المرفق لتنشيط الفيروس على الجهاز.

المخترقون والمخربون:

يعرف المخترق عادة على أنه الشخص الذي يستمتع بتعلم لغات البرمجة وأنظمة الكمبيوتر ويمكن اعتباره على أنه خبير في هذا المجال، المخترقون هم عبارة عن مبرمجين يحاولون العثور على الثغرات التي توجد في الأنظمة للارتقاء بمستواهم المعرفي.
وقد يقوم المخترقون أحيانًا بمشاركة المعلومات التي يكتشفونها مع الآخرين دون عقد العزم على اعتراض هذه الأنظمة أو الاستيلاء على المعلومات الشخصية العائدة للآخرين.
بينما المخرب هو الشخص الذي يقوم بالوصول بشكل غير قانوني إلى أنظمة الآخرين بنية نشر البرمجيات الضارة، حيث يستطيع المخرب تدمير نظام ما من خلال تدمير البيانات الرئيسة لهذا النظام.

قانون الدولة للجرائم الإلكترونية.

- بناءً على المادة رقم (7): يعاقب بالسجن المؤقت كل من حصل، أو استحوذ، أو عدّل، 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 (5): يعاقب بالحبس وبالغرامة التي لا تقل عن مائة ألف درهم، ولا تتجاوز ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين كل من دخل بغير تصريح موقعًا إلكترونيًّا بقصد تغيير تصاميمه، أو إلغائه، أو إتلافه، أو تعديله، أو شغل عنوانه.

نشاط

- إذا كنت تمتلك مهارات الاختراق، فهل يسمح لك ذلك باختراق حسابات أصدقائك بهدف المزاح؟ ناقش ذلك.

المطاردة الإلكترونية:

المطاردة الإلكترونية هي عبارة عن استخدام (الإنترنت) أو أي وسيلة إلكترونية لتعقب الآخرين، يستطيع المتتبعون الإلكترونيون الحصول على معلومات حول ضحاياهم من مصادر متعددة مثل المدونات ومحركات البحث ومواقع التواصل الاجتماعي.

عند استخدامك (للإنترنت)، لا تقم بالكشف عن معلوماتك الشخصية للآخرين واحفظها بأمان، ومن الجيد عدم استخدام اسمك الحقيقي عند التواصل مع الغير في المنتديات وغرف المحادثة، ومن النصائح الجيدة كذلك عدم الإفصاح عن الجنس وخاصة بالنسبة للإناث.

دراسة حالة

دراسة حالة: مشاركة المعلومات الشخصية، ولو بقدر بسيط، قد يجعل منك ضحية للمطاردة الإلكترونية.

تقوم (مايشا) بالدخول إلى محادثات بشكل دوري، وهناك التقت بشاب بدا لها أنها تعرفه جيدًا، إنه لطيف حقًّا.

وفي أحد الأيام، وفي أثناء حديثها مع هذا الشاب، قام بسؤالها عن العديد من تفاصيلها الشخصية، فاشتبهت (مايشا) بالأمر، ورفضت الإفصاح عن هذه البيانات، وقامت بإنهاء المحادثة مباشرة، ثم قامت بحظر حسابه حتى لا يتمكن من إرسال رسائل إليها.

وبعد يوم من هذه المحادثة، بدأ الشاب بالتحرش بـ (مايشا) من خلال إرسال رسائل بريد إلكتروني مرفقًا بها صورًا فاضحة، وعلى الرغم من أن (مايشا) طلبت منه الكف عن ذلك إلا أنه واصل إرسال هذه الرسائل والصور المزعجة، فقام والدا (مايشا) بالتواصل مع مزود خدمة (الإنترنت) وغيّروا بريدها الإلكتروني، وتمّ منع الشاب من إرسال المزيد من الرسائل.

رغم ذلك، استمر الشاب في نشر رسائل في غرف المحادثة التي تزورها (مايشا)، وواصل نشر التعليقات الكاذبة والبذيئة حولها عبر (الإنترنت)، وفجأة، بدأت رسائل تهديد عدة تصل إلى (مايشا) من رقم هاتف محمول لا تعرفه، ونصت هذه الرسائل على أن الشاب سيجدها، وسيقوم بعدها بالتسبب بأمور فظيعة لها مما أدى إلى إثارة استياء (مايشا)، وبالتالي أخبرت والديها بالموضوع، فقاما بإبلاغ الشرطة.

يلاحظ من هذا أن قدرًا بسيطًا من المعلومات الشخصية التي قامت (مايشا) بمشاركتها عبر (الإنترنت) أدّت إلى تمكّن هذا الشاب من العثور على المزيد من معلوماتها الشخصية، كرقم هاتفها، وغيره، وقد لا يبدو هذا الأمر في ظاهره خطيرًا، ولكن هذه المعلومات قد تؤدي إلى ما لا تُحمد عقباه.

(Gulf News, 18 July, 2010, http://gulfnews.com/mobile/news/gulf/uae/crime/cyber-crime-victim-helps-catch-stalking-suspect-in-dubai-1.655656)

مفترسو الإنترنت:

مفترسو (الإنترنت) هم أشخاص يبحثون عن ضحايا محتملين لإشباع رغباتهم غير الأخلاقية عبر (الإنترنت).

تحذير

عادة ما يكون المفترس عبر (الإنترنت):

- ذكرًا.
- جذاب.
- إنطوائي.
- يتسم بالسادية.
- غير مميز جنسيًّا.

يحاول مفترسو (الإنترنت) الإيقاع بأكثر من ضحية في نفس الوقت باستخدام طرق مختلفة، وعادة ما يبحثون عن ضحاياهم في المواقع المعروفة ذات الشعبية العالية من قبل المراهقين مدعين أنهم من نفس أعمارهم. يبدأ مفترسو (الإنترنت) بالتحرش بطريقة غير مباشرة لا يمكن تمييزها من قبل أغلب المراهقين وخاصة الأطفال منهم، حيث يتصرفون معهم بلطف ويحاولون كسب ثقتهم حتى يتمكنوا من ملاقاتهم بعيدًا عن أعين الآخرين.

يبدي مفترسو (الإنترنت) لطفًا واهتمامًا ومودة تجاه ضحاياهم بشكل تدريجي وقد يصل الأمر إلى درجة تقديم الهدايا لهم في لكسب ود هؤلاء الضحايا الذين ما يعانون عادة من الوحدة والإهمال من والديهم أو من يتولى شؤونهم. كما أن مفترسي (الإنترنت) على استعداد لقضاء قدر كبير من وقتهم وجهدهم وأموالهم للإيقاع بضحاياهم.

إن مفترسي (الإنترنت) على استعداد لقضاء الوقت في البحث عن الموسيقى أو النشاطات التي يحبها الأطفال وتشكل نقاط جذب لهم، كما أنهم على استعداد تام للإصغاء لمشاكلهم، يحاول مفترسو (الإنترنت) اطلاق العنان للمراهقين من خلال تقديم المحتويات اللأخلاقية في حواراتهم معهم، وللأسف يقع العديد من المراهقين ضحية في مثل هذه المواقف التي يتم فيها التحرش فيهم جنسيًّا من خلال غرف المحادثة أو رسائل البريد الإلكتروني.

يقع بعض مستخدمي (الإنترنت) المراهقين في مثل هذه المشاكل بسهولة أكبر من غيرهم، وعليه فإن المعلومات التالية قد تساعدك في ملاحظتهم حيث تظهر عليهم غالبًا الأعراض الآتية:

1. عدم الإلمام بقواعد السلوك والتهذيب
2. السعي نحو الحصول على الاهتمام
3. التمرد
4. الوحدة أو الميل للعزلة
5. الفضول
6. الارتباك بشأن الهوية الجنسية
7. سهولة التعرض للخداع من قبل البالغين
8. الاغترار بالثقافات الأجنبية

الحوسبة السحابية:

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

إيجابيات وسلبيات الحوسبة السحابية:

(الحوسبة السحابية هي الوعي الجماهيري باستخدام الخدمات الحاسوبية حيث يتم تقديم خدمات تقنيات المعلومات بشكل أكثر عملانية من خلال بنية مرجعية يتم إنشاؤها من قبل مزودين بدلًا من المستخدمين أنفسهم)

Chris Poelkar

إيجابيات الحوسبة السحابية:

1. المرونة: يستطيع المستخدمون الوصول إلى المعلومات المخزنة سحابيًا في أي مكان وزمان.
2. قلة التكلفة: تتوفر للاستخدام الفردي، وللمؤسسات بتكلفة قليلة.
3. آلية بشكل كبير: لا توجد حاجة لشراء برامج حديثة، كل شيء معد سلفًا وجاهز للاستخدام.
4. الخدمة السريعة: يمكن الحصول على خدمات الحوسبة السحابية في اللحظة نفسها.
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؛ نظرًا 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 بدلًا من الأجهزة المادية أو المشتركة الموجودة في مقر المستخدم، تجذب خدمات الحوسبة السحابية العديد من المؤسسات نظرًا 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 أمرًا حاسمًا لضمان نجاحها.

دراسة حالة

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 احراجًا 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.

مواقع التواصل الاجتماعي:

مواقع التواصل الاجتماعي عبارة عن أدوات تستخدم من خلال أجهزة (الكمبيوتر) وهي تمكّن المستخدمين من إنشاء ومشاركة وتبادل المعلومات والأفكار والصور و(الفيديوهات) في شبكات ومجتمعات افتراضية، وتعرف مواقع التواصل الاجتماعي على أنها مجموعة من تطبيقات (الإنترنت) التي تعتمد على الأسس الفكرية والتقنية للجيل الثاني من (الويب) والذي يسمح بإنشاء وتبادل المحتويات التي ينتجها المستخدمون بأنفسهم.

وسائل التواصل الاجتماعي وقضايا الحماية والخصوصية:

يستطيع مستخدمو وسائل التواصل الاجتماعي مشاركة بياناتهم الشخصية مع الآخرين، ولكن من الممكن أن تتم إساءة استغلالها؛ لأن مشاركة البيانات الشخصية قد تؤدي إلى إساءة استخدامها، سواء أكان ذلك بشكل متعمّد أم غير متعمد، وعلى سبيل المثال: يقوم بعض الأشخاص بمشاركة تفاصيل حساباتهم مثل الاسم الكامل، والجنس، ورقم الهاتف مع مستخدمي الموقع، وكمثال آخر، قد يتم استغلال المعلومات التي تتعلق بالحالة الاجتماعية أيضًا.

ساهم مقدار المعلومات الشخصية المتوفرة وإمكانية الحصول عليها عبر مواقع التواصل الاجتماعي في جذب أصحاب النوايا الإجرامية الذين يسعون لاستغلالها والاستفادة منها، وإن 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 إلى سرقة كلمات المرور.

سرقة الهوية

التجسس

الهندسة الإجتماعية

القضايا الأخلاقية والقانونية المتعلقة باستخدام مواقع التواصل الاجتماعي:

عند استخدام مواقع التواصل الاجتماعي يتعين عليك أن تتأكد من بناء سيرتك البحثية بشكل صحيح، إن الأساس للقيام بمثل هذا الأمر يتمثل في تذكرأن القوانين والسياسات والقواعد الإجتماعية 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 عليها (كالأفكار والصور والبيانات وغيرها) 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.

التنمر الإلكتروني:

يحصل التنمر الإلكتروني عند قيام شخص ما وبشكل متكرر بالتحرش بغيره، وبمعاملته بطريقة سيئة، أو جعله مادة للسخرية والاستهزاء من خلال البريد الإلكتروني، أو مواقع (الإنترنت)، أو الرسائل النصية، أو الهواتف المحمولة، أو (الفيديوهات)، أو المدونات، أو أي شكل من أشكال التواصل الإلكتروني.

كما يتضمن التنمر الإلكتروني الصور والرسائل والصفحات التي لا تتم إزالتها، على الرغم من طلب الشخص الذي وضعها القيام بذلك. وبكلمات أخرى، فإن التنمر الإلكتروني هو أي شيء يتم نشره عبر (الإنترنت) بشكل يتعمد من خلاله إيذاء شخص آخر أو التحرش به أو إثارة استيائه.

قد يتمثل التنمر الإلكتروني في القيام بالأنشطة الآتية:

- نشر الرسائل المهينة على مواقع التواصل الاجتماعي.
- نشر الشائعات عبر (الإنترنت).
- إقصاء الشخص من مجموعة ما على (الإنترنت).
- إرسال رسائل غير مرغوبة باستخدام الرسائل النصية والرسائل الفورية ورسائل البريد الإلكتروني.

ونظرًا لأن مثل هذا النوع من التنمر يمكن أن يحصل في أي مكان، فإن الضحايا لا يستطيعون الشعور بالأمان حتى في بيوتهم، ويؤدي هذا بدوره إلى الإضرار بشكل كبير بثقة الضحية بنفسه، وبتقديره لذاته.

قد يكون التنمر الإلكتروني ضارًا ومؤذيًا على وجه التحديد؛ لأنه يتم من قبل أشخاص مجهولين، أو يصعب تتبعهم عادة، إضافة إلى صعوبة السيطرة عليه، مما يضع الضحية في حيرة من أمره حول عدد الأشخاص الذين رأوا هذه الرسائل أو المنشورات، وقد يتعرض الأشخاص لعذاب مستمر في كل مرة يقومون فيها بتفقد هواتفهم أو حواسيبهم، وفي بعض الأحيان قد لا يكونون على دراية بما يقال عنهم من ورائهم، أو من أين تأتيهم الإساءة.

بسبب الدور الذي تلعبه التقنيات الحديثة في حياتنا، قد لا يكون من الممكن العثور على مكان للاحتماء من المتنمرين، حيث يمكن أن يحصل التنمر الإلكتروني في المنزل أو المدرسة أو في أي مكان آخر يمكن للناس الوصول إليه عبر (الإنترنت).

قد يؤدي التنمر الألكتروني في بعض الأحيان - شأنه شأن أنواع التنمر الأخرى - إلى مشاكل خطيرة طويلة الأمد، إن التوتر الناجم عن حالة القلق المستمرة أو الخوف المستمر قد يؤدي إلى مشاكل تؤثر على المزاج والطاقة والنوم والشهية، كما تدفع بالشخص للشعور بالتوتر أو الانزعاج أو الحزن، وإذا كان الشخص يشعر بهذه الأحاسيس أصلًا، فإن التنمر الألكتروني سيزيد الأمور سوءًا.

من هو الذي يقوم بالتنمر؟

لماذا يقوم الناس بمثل هذت التصرف؟

لماذا يصبح أحدهم متنمرًا إلكترونيًّا؟ قد يكون هناك العديد من الأسباب كما أن هناك العديد من المتنمرين. إن ما قد يبدو تحرشًا إلكترونيًّا قد يكون بمحض الصدفة أحيانًا، إن الرسائل النصية والمنشورات وطرق التواصل الأخرى عبر (الإنترنت) ذات الطبيعة غير الشخصية قد يصعب فهم مقصد مرسلها فيما إذا كان مجرد مزاح أم لا.

يدرك الكثير من الناس اللحظة التي يتعرضون فيها للتنمر وذلك لأن التنمر يتضمن تهديدات وإهانات بشكل مستمر، كما يدرك المتنمرون بأنهم قد تجاوزوا حدودهم أيضًا، إنها ليست مزحة أو إهانة لمرة واحدة فقط، بل هي تحرش مستمر وتهديدات تتعدى حدود المزاح المثير للاستياء أو تعليقات مسيئة تكتب في لحظة غضب ما.

آثار التنمر الإلكتروني:

لا ينحصر التنمر الإلكتروني في المدارس أو في الشارع، قد يحصل التنمر في الوقت الحالي في المنزل كما في المدرسة وعلى مدار اليوم، إن الأطفال الذين يقعون كضحية للتنمر يشعرون بأنهم منتقدون بشكل مستمر وأنه لا مهرب لهم من هذا الأمر، وطالما أن الأطفال يمتلكون القدرة على استخدام الهاتف أو الحاسوب أو الأجهزة الأخرى كالحواسيب اللوحية فهم عرضة للخطر.

إن التنمر الإلكتروني المتكرر أو طويل الأمد أو الحاد قد يعرض كلًا من المتنمر والضحية للحصار النفسي والاحباط و الاضطرابات الناجمة عن القلق، وفي بعض الحالات النادرة والتي تم الإفصاح عنها، قام بعض الأطفال بالانتحار، يقول المختصون أن الأطفال الذين يتعرضون للتنمر والمتنمرون أنفسهم عرضة بشكل كبير لمخاطر التفكير بالانتحار أو المحاولة، وحتى الانتحار ذاته.

قد يتم معاقبة المتنمر الإلكتروني من خلال إيقافه عن الدراسة أو فصله من الفرق الرياضية مثلًا، كما تعد بعض أنواع التنمر الإلكتروني جريمة في نظر القانون.

العلامات الدالة على التنمر الإلكتروني:

لا يحبذ العديد من الأطفال والمراهقين الذين يتعرضون للتنمر إخبار معلميهم أو أولياء أمورهم بما يمرون به نظرًا لشعورهم بالخزي أو بالمهانة الاجتماعية أو الخوف من حرمانهم من استخدام حواسيبهم في المنزل.

وتتعدد العلامات التي تدل على التعرض للتنمر الإلكتروني، ومنها ما يشير إليه الشكل.

تتعدد العلامات التي تدل على التعرض للتنمر الإلكتروني، ومنها:

- الشعور بالإزعاج أثناء استخدام الهاتف أو (الإنترنت) أو بعد انتهاء منه.
- السرية والحرص الشديدين على مكونات حياتهم الرقمية.
- الابتعاد عن أفراد العائلة والأصدقاء والنشاطات الأخرى.
- تجنب مجموعات الأصدقاء والذهاب إلى المدرسة.
- إنخفاض المستوى الدراسي والتصرف بعصبية بالغة في المنزل.
- التغيرات السلوكية والمزاجية والنوم والشهية.
- الرغبة في التوقف عن استخدام الحاسوب والهاتف المحمول.
- الشعور بالانزعاج والعصبية عند استلام رسالة نصية أو فورية أو بريد إلكتروني.
- تجنب الأحاديث عن أي نشاطات تتم باستخدام الحاسوب أو الهاتف المحمول.

كيف يمكنني التعامل مع التنمر الإلكتروني؟

في بعض الأحيان يكون الشخص الذي يتعرض للتنمر خائفًا أو غير متأكد فيما إذا كان يتعرض للتنمر أم لا، وبالتالي لا يقوم بفعل شيء حيال ذلك عدا الشعور بالاستياء أكثر فأكثر في خلجات نفسه، فإذا كنت تتعرض للتنمر أو إثارة استيائك بشكل مؤذٍ، أو كنت تعرف أن أحدهم يتعرض لذلك فلا داعي للمعاناة في صمت، بل يمكنك بكل تأكيد الإبلاغ عن أية رسائل أو منشورات أو رسائل بريد إلكتروني ذات طابع مسيء.

- **أَخبِرْ أحدًا ما**، بل إن أول ما يتعين عليك القيام به هو إبلاغ أحد البالغين الذين يمكنك الوثوق بهم، ولكن القول أسهل من الفعل، إذْ يشعر العديد من الأشخاص الذين يتعرضون للتنمر بالحرج وعدم الرغبة في الإبلاغ عن المتنمر، وقد يتردد بعضهم في الإبلاغ؛ لأنهم ليسوا متأكدين مَنْ هو الذي يقوم بالتنمر عليهم، لكن وتيرة هذا التنمر قد تزداد سوءًا لذلك يجب عليك الإبلاغ حتى تتمكن من الحصول على المساعدة، وتستطيع الشرطة تعقب هذا المتنمر الإلكتروني المجهول، ولذلك فإن الأمر يستحق الإبلاغ عنه.

- **ابتعد عن مصدر التنمر**، فإن ما تعلمته حول الابتعاد عن المتنمرين في العالم الحقيقي يصلح للتطبيق في العالم الافتراضي أيضًا، وإن تجاهل المتنمر هو أفضل طريقة للابتعاد عن هيمنته، ولكن هذا ليس بالأمر السهل في العالم الحقيقي أو حتى عبر (الإنترنت).

- **ابتعد عن مصدر التنمر**، إذا لاحظت أن أمرًا قد أساءك فابتعد عن الحاسوب، أو قم بإغلاق هاتفك لفترة وجيزة، ولا تقم بالرد أبدًا على الرسائل التي تصلك، ولا تقم بإعادة إرسالها إلى آخرين، وحاول البحث عن طريقة لتنأى بنفسك بها عما يحصل، ويمكنك ممارسة الأنشطة التي تحبها لتشغل نفسك عن التفكير فيما يحصل.

- **قاوم الرغبة في الرد أو الانتقام**، وإن الابتعاد عن تعرضك للتنمر الإلكتروني يمنحك فرصة حتى لا يتم استفزازك للرد أو المواجهة مع المتنمر، كما أن ردك وأنت في حالة الانزعاج هذه قد يؤدي إلى زيادة الأمور تعقيدًا، رغم أن التصدي للمتنمر قد يفيد في بعض الأحيان، إلا أنه قد يزيد من حدة تصرفاته وبالتالي يتم تصعيد الموقف، وإن الابتعاد يشحذ عزيمتك ويقويها.

- **وعلى الرغم من أن الرد على المتنمر ليس بالفكرة الجيدة**، إلا أنه من الجيد الاحتفاظ بالأدلة التي تثبت عملية التنمر إذا كان هذا ممكنًا، حيث تساعد هذه الأدلة في تقوية موقفك عند الحاجة، كما أنه لا يتعين عليك الاحتفاظ بالرسائل المسيئة، سواء أكانت نصية أم من البريد الإلكتروني أينما وجدتها، ويمكنك طلب المساعدة من ولي أمرك لنسخ هذه الرسائل أو الاحتفاظ بها وتخزينها على قرص خارجي.

- **إبلاغ مزود الخدمة:** إن العديد من المواقع مثل (فيسبوك) و(انستغرام) و(يوتيوب) تتعامل بجدية مع من يقوم باستخدامها لنشر المحتويات المسيئة أو بإنشاء الحسابات الوهمية، وفي حال قيام المستخدمين بالإبلاغ عن إساءة ما قد يقوم مسؤول الموقع بمنع المتنمر من استخدام الموقع مستقبلًا، وفي حال كنت تتعرض للتحرش من قبل شخص يقوم بإرسال رسائل مسيئة لك، يمكنك الإبلاغ عنه لمزود الخدمة الهاتفية أو مزود خدمة البريد الإلكتروني، مثل (جوجل) و(ياهو) و(تويتر) وغيرها.

- **حجب المتنمر:** توفر العديد من الأجهزة إعدادات تمكنك من حجب المتنمر ومنعه من التراسل معك، وإذا كنت لا تعرف كيف تستخدم هذه الميزة، فيمكنك الحصول على المساعدة من أحد البالغين أو من أصدقائك.

- **ابق آمنًا عند استخدام (الإنترنت):** تستخدم كلمات المرور لحماية هاتفك وحماية الحسابات التي تستخدمها عبر (الإنترنت)، ولذلك يجب عليك تغييرها باستمرار، وعليك ألا تشارك كلمات المرور مع أي شخص كان سوى أولياء أمرك، أو من يتولى رعايتك، ومن الجيّد التفكيرُ مرّتين قبل مشاركة أية معلومات شخصية أو صور أو (فيديوهات) قد لا ترغب بأن يراها أحد، قد يكون من الصعب إزالة الصورة أو الرسالة التي قمت بنشرها أو حتى قد يستحيل ذلك، لذلك عوّد نفسك على أخذ الحيطة والحذر عند نشر صور عبر (الإنترنت) أو حتى عند الرد على رسالة مزعجة وصلتك من غيرك.

بالنسبة للأطفال الأصغر سنًا فإن أفضل طريقة للتعامل مع مشكلة التنمر الإلكتروني تكمن في إبلاغ شخص بالغ وموضع للثقة، أما بالنسبة للمراهقين فإن إبلاغ شخص بالغ يعتمد على حالة التنمر التي يتم المرور بها:

1. لا تقم بالرد أو محاولة الانتقام.
2. احجب المتنمر، واضبط إعدادات الخصوصية.
3. الإبلاغ: إذْ يمكنك استخدام خاصية الإبلاغ التي يوفرها الموقع.
4. جمع الأدلة: احتفظ بالرسائل، واطبع رسائل البريد الإلكتروني والمحادثات التي تتم عبر مواقع التواصل الاجتماعي.
5. تحدث إلى شخص بالغ تثق به كأحد أفراد العائلة أو الأصدقاء.

إن التحدث إلى معلميك أو ولي أمرك أمر يصنع فرقًا لحل المشكلة، قد يكون لدى مدرستك سياسات ملائمة للتعامل مع قضايا التنمر والتنمر الإلكتروني.

ما الذي يمكنك القيام به إذا كان صديقك يتعرض للتنمر الإلكتروني.

رغم أنه قد يكون من الصعب معرفة فيما إذا كان صديقك يتعرض للتنمر الإلكتروني، لكنه يتعين في عليك في حال سمعت أو عرفت بهذا الأمر القيام بالأمور التالية:

1. لا تقم أبدًا بارسال الرسائل والصور التي يتم من خلالها التنمر على صديقك. على الرغم من أنك لست أنت من قام بعملها، إلا أنك بارسالها تصبح جزءًا من عملية التنمر التي يتعرض لها صديقك.
2. تجرأ وقم بالإبلاغ.
3. ساند صديقك وقم ساعده للابلاغ عن التنمر.

قانون الدولة للجرائم الإلكترونية.

بناء على المادة رقم (16): يعاقب بالحبس مدة لا تزيد عن سنتين، وبالغرامة التي لا تقل عن مائتين وخمسين ألف درهم، ولا تتجاوز خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين كل من ابتزّ، أو هدد شخصًا آخر لحمله على القيام بفعل، أو الامتناع عنه، وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية معلومات.

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

الاستخدام الملائم والأخلاقي لأدوات التواصل والتعاون الرقمية:

قد لا يبدو لك أنه من المهم التصرف بشكل ملائم في العالم الافتراضي، ربما يتأتى هذا الأمر من كونك لا تعرف الناس الذين تتواصل معهم في أغلب الأحيان، ومن المثير للدهشة وجود بعض الأشخاص الذين يتصرفون بشكل مغاير تمامًا عند استخدام (الإنترنت) نظرًا لاعتقادهم بأنهم يستطيعون إخفاء هوياتهم خلف اسم المستخدم وإبقاءها غير معروفة.

لكن الطريقة التي تستخدمها في التواصل لا تشكل أي فرق؛ لأنه من الضروري جدًا التحلي بالأخلاق عبر (الإنترنت) كما هو الحال فيما لو كنت شخصيًّا هناك.

كيف يمكنك معرفة فيما إذا كنت تتصرف بشكل ملائم عند استخدام (الإنترنت)؟

التواصل بشكل ملائم عند استخدام (الإنترنت):

لا فرق يذكر سواء أكنت تتواصل باستخدام (الإنترنت) أم وجهًا لوجه، إنه أمر ذو علاقة بالفطرة السليمة، وإن الأساس هو (عامل الناس كما تحب أن يعاملوك).

إليك بعض الاقتراحات حول كيفية التواصل عبر (الإنترنت):

1. استخدم اللغة المناسبة: يميل بعض الناس في الوقت الحاضر - ولا سيما المراهقون - إلى استخدام الاختصارات، ولا مانع من استخدامها مع من يستطيع فهمها من أصدقائك، ولكنهم ليسوا جميعًا على معرفة بمعاني هذه الاختصارات مما يوقع المستلم في حيرة من أمره، وبالتالي قد ينزعج الناس منك لمجرد أنهم لا يفهمون ما تقوله.
2. تعامل مع الناس كما لو كنت أمامهم وجهًا لوجه: من الضروري أن تعامل الناس كما تحب أن يعاملوك، لذا يجب عليك التصرف بشكل جيد ومؤدب عند الحديث مع الناس عبر (الإنترنت)، أو عند نشر التعليقات؛ لأنك قد تتسبب في جرح مشاعرهم دون أن تدرك ذلك.
3. إذا لم يكن لديك شيء جيد يمكنك قوله فاصمت: لا يستطيع أحد إجبارك على الاقتناع بأفكاره، وإذا لم تكن مقتنعًا فلا تقم بالتعليق بشكل مسيء، وإذا كنت مضطرًا للتعليق أو طُلِب منك ذلك فإنه يتعين عليك التعليق بأسلوب مهذب ومؤدب.
4. لا مانع من الاعتراض، ولكن قدم تبريرك: لا يمكن للآراء أن تكون غير صحيحة، ولذلك إذا كان أحدهم يمتلك رأيًا مخالفًا لرأيك فلا تنتقده، فقط أخبره برأيك، وقدم أسبابك بشكل مؤدب.
5. لا تثر المشاكل: إذا رأيت أحدهم يقوم بنشر تعليقات مؤذية أو مسيئة للآخرين فقم بإبلاغ الشخص المسؤول، وإن لم يكن هناك مسؤول فاطلب بلطف من الذي يقوم بنشر هذه التعليقات المسيئة التوقف عن أفعاله.

استخدام أدوات التواصل الاجتماعي للأسباب الجيدة:

إن البساطة التي كان عليها عالمنا في السابق، حيث يصطف الناس في طوابير للحصول على مصادر محدودة أصبحت الآن تتكون من شبكات هائلة وذات مرونة، وإن كلًا من الشبكات الاجتماعية التقليدية والحديثة فضلًا عن البنى الجديدة التي أوجدتها البرامج الاجتماعية تمنحنا القدرة على أداء أمور رائعة لأنفسنا وللآخرين.

إن الاستفادة المتأتية من مواقع التواصل الاجتماعي التي تلاقي رواجًا بين الناس تعد مثالًا رائعًا على سرعة وفعالية استخدام التقنيات في الأمور الجيدة، ودعنا نقرأ معًا دراسات الحالة التالية حتى نفهم بشكل أفضل.

تبادل ومشاركة المعلومات عبر أنظمة الشبكات بشكل أخلاقي:

مقارنة بين الموارد المشتركة والموارد المخصصة:

الموارد المشتركة - في عالم الحاسوب - هي الأجهزة أو المعلومات التي يمكن الوصول إليها باستخدام حواسيب أخرى من خلال شبكة محلية أو داخلية، وبعبارة أخرى، الموارد المشتركة هي التي يمكن مشاركتها

مع الآخرين أو يسمح لهم بالوصول إليها، ومن الأمثلة عليها الملفات والمجلدات المشتركة والأجهزة الطرفية مثل الطابعات والماسحات الضوئية والخوادم والبريد الإلكتروني وغيرها.

في وقتنا الحاضر، لا تقتصر الموارد المشتركة على الأجهزة الطرفية فقط، بل تمتد إلى كل ما يتوفر على الشبكة من مهارات ومواهب وخبرات وصلاحيات وصول وحتى الأموال.

وفي وسائل مختلفة، يمكن اعتبارها على أنها امتياز عند السماح لك بالوصول إلى الموارد المشتركة في مدرستك أو مقر عملك أو مؤسستك، وبالمقابل، يتوقع منك إبداء أقصى مستويات الاحترام لحقوق الآخرين في استخدام هذه الموارد.

من ناحية أخرى، تعرف الموارد المخصصة على أنها جهاز موصول بحاسوب ما، والتي لا تتوفر للاستخدام إلا من خلال حاسوب واحد، ومن قبل مستخدم واحد في اللحظة نفسها.

- قام زميلك بنشر معلومات مغلوطة على لوح النقاش داخل المدرسة.

  في محاولة منك لتصحيح معلومة زميلك، هل ستقوم بالتحدث معه بشكل خاص، أو ترد عليه مباشرة على لوح النقاش؟ ولماذا؟

إليك تاليًا بعض الأمثلة على السلوكيات غير الأخلاقية عند استخدام الموارد المشتركة:

1. تحميل البرامج المقرصنة.
2. طباعة كميات كبيرة من الملفات الشخصية.
3. تخزين الملفات التي ليس لها علاقة بالعمل مثل الصور والملفات الشخصية على وحدات التخزين المشتركة.
4. تحميل الملفات كبيرة الحجم وغير الضرورية أثناء ساعات الدوام المدرسي.
5. إرسال رسائل البريد الإلكتروني المزعجة للآخرين.

الموارد المشتركة	الموارد المخصصة
◦ تطوير المواد بالاعتماد على منصات معينة مثل منصة (wikis). ◦ إنشاء شبكة في مقر الشركة للربط بين المستخدمين والموارد. ◦ إنشاء مجلد خاص لصفك حتى يتمكن جميع طلاب الصف من مشاركة الملفات فيما بينهم. ◦ طباعة الواجبات من خلال طابعة الشبكة الموجودة في مختبر الحاسوب بالمدرسة. ◦ حفظ صور النشاطات الصفية في مجلد عام. ◦ استخدام جهاز عام في المكتبة للوصول إلى (الإنترنت). ◦ إتاحة أحد الموارد المتوفرة على (الإنترنت) للمدرسة. ◦ الاستفادة من موارد المدرسة المتوفرة عبر (الإنترنت) بأكبر قدر ممكن. ◦ استخدام شبكة المدرسة في إكمال مشروع دراسي جماعي.	◦ طباعة عدد لا محدود من الأوراق باستخدام الطابعة الموصولة بشكل مباشر بحاسوبك. ◦ طباعة الواجبات المدرسية من خلال طابعة محلية في مختبر الحاسوب في المدرسة. ◦ تخزين صور النشاطات الصفية على مجلد خاص. ◦ استخدام وسائل التعريف الحيوية (مثل البصمة) للدخول إلى أحد المرافق.

اتخاذ القرارات الأخلاقية:

إن اتخاذ قرار أخلاقي ليس بالأمر السهل، ولكن يتعين على الشخص أن يكون قادرًا على اتخاذه، وقد يتم اتخاذ القرارات الأخلاقية بطريقة موضوعية لأبعد حد، كما أنه من الممكن أن تتباين هذه القرارات الأخلاقية من حالة إلى أخرى، وإن القرار الجيد الذي يناسبك قد لا يناسب غيرك.

وقبل اتخاذ قرار مماثل، اطرح على نفسك الأسئلة الآتية:

لاحظ وجود أي عقبات أخلاقية	كن واضحا ومتمكنًا من الحقائق الصحيحة	قيّم كافة الخيارات المتاحة
◦ هل يؤدي قرارك إلى إلحاق الأذى بشخص أو مجموعة أخرى أو يؤثر عليهم؟ ◦ هل سيعرض هذا القرار حياتك للخطر؟ ◦ هل أنت في ورطة ما من أجل اتخاذ القرار؟ ◦ هل قرارك سليم من الناحية القانونية؟ ◦ هل سيتعارض قرارك مع أي أمر آخر؟	◦ هل أنت ملم بالحقائق المتعلقة بالموقف أو الحالة؟ ◦ هل تمتلك المعرفة الكافية لاتخاذ القرار؟ ◦ هل أنت بحاجة إلى المزيد من المعلومات؟ ◦ هل أنت بحاجة إلى التثبت أكثر أو استشارة شخص ذي صلاحيات أعلى؟	◦ أي من الخيارات المتاحة يمكنك من اتخاذ أفضل قرار ممكن بأدنى حد من الضرر؟ ◦ ما هو الخيار الأنسب لعلاج الموقف أو القضية التي بين يديك؟ ◦ ما هو الخيار الأنسب والذي يتضمن احترام حقوق كافة أطراف القضية؟ ◦ ما هو الخيار الأنسب والذي يوفر حقوقًا متساوية وعادلة لكافة أطراف القضية؟

وفي نهاية المطاف، يمكنك التفكير لبرهة في النتائج الممكنة للقرار الذي توشك على اتخاذه، وإذا كان هناك أي احتمالات غير مريحة لك، تأكد من أن هناك خطبًا ما.

نشاط

إذا كانت لديك ملاحظات سلبية عن منتج قُمت بشرائه من (الإنترنت)، فهل لديك الحق بنشر هذا التعليق؟ ولماذا؟

الوقاية على الإنترنت:

الوعي الذاتي:

البصمة الرقمية:

البصمة الرقمية هي المعلومات التي يمكن تتبعها، والتي نتركها خلفنا عند استخدام (الإنترنت)، وقد تتسبب هذه المعلومات في مشاكل للذين يقومون بنشر تعليقات وصور وأمور خاصة بهم، والتي قد تظهرهم بشكل مرح، ولكنها قد تتسبب في ترك انطباع سلبي على وظائفهم المستقبلية أو شركائهم المحتملين.

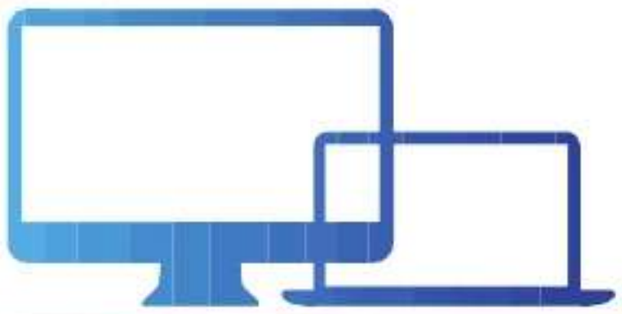
إليك بعض الخطوات التي يمكنك اتباعها لمراقبة وحماية سمعتك الرقمية على (الإنترنت):

1. ابحث عن المعلومات المتوفرة عنك على (الإنترنت)، ولذلك يمكنك استخدام محركات البحث ومواقع التواصل الاجتماعي.
2. صحح التعليقات السلبية ذات الصلة بك على موقع أو مدونة ما، وإذا لم تستطع التخلص منها فكن مستعدًا للإجابة عن الأسئلة التي قد تطرح عليك لاحقًا، وإذا كان لديك موقع أو مدونة شخصية فقم بمراجعة المحتويات التي قمت بنشرها.
3. كن حكيمًا عند اختيار المواقع التي تنضم إليها، وتأكد من أن الموقع الذي تود الاشتراك به لا يلحق الضرر بسمعتك، كما يمكنك تحسين سمعتك من خلال الاشتراك في المواقع التي تتسم بالاحترافية.
4. لا تقبل طلبات الصداقة من الغرباء.

5. اضبط إعدادات الخصوصية بحيث لا يتمكن سوى أصدقائك من استعراض معلوماتك.
6. لا تقم أبدًا بنشر أية أمور مسيئة بحق عملك أو مدرستك أو أي شخص آخر.
7. تجنب نشر الصور غير الملائمة.
8. تأكد من أن ما تقوم بنشره احترافي، ويراعي مشاعر الآخرين.

تأمين بياناتك السحابية:

إليك بعض النصائح لحماية خصوصية بياناتك؛ لتساعدك في التغلب على قضايا الخصوصية عند استخدام الخدمات السحابية:



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 بالإنترنت أو فقدانه.

2. تجنب تخزين البيانات الحساسة السحابية.

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. قم بتشفير بياناتك قبل رفعها على الخدمات السحابية.

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

4. استخدم الخدمات السحابية التي توفر إمكانية تشفير بياناتك.

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

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 شبكات (إنترنت) عامة، وفي هذه الحالة يتعين عليك عدم تخزين كلمات المرور والتأكد من تسجيل الخروج من حسابك قبل المغادرة.

مواقع التواصل الاجتماعي:

تشير مواقع التواصل الاجتماعي إلى مجموعات التعاون على (الإنترنت)، والتي تتيح مشاركة الصور و(الفيديوهات) والمقاطع الصوتية التي يقوم بإنتاجها مستخدمون معينون، والذين هم ليسوا موظفين تابعين لهذه المواقع.

مع تنامي شعبية مواقع التواصل الاجتماعي تتنامى كذلك المخاطر المترتبة على استخدامها؛ نظرًا لإمكانية استخدامها من قبل المخترقين وصانعي الفيروسات وسارقي الهويات وغيرهم من المجرمين.

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

1. توخ الحذر حيال ما تنشره عن نفسك على (الإنترنت)
2. لا تثق بأن الرسالة قد وصلتك ممن يبدو لك أنه قام بارسالها
3. لا تسمح لمواقع التواصل الاجتماعي بالوصول إلى جهات اتصال البريد الإلكتروني الخاص بك
4. لا تضغط على الروابط التي تظهر في بعض المواقع وفي مواقع التواصل الاجتماعي، اكتب العنوان مباشرة في المتصفح.
5. كن حذرًا عند إضافة أصدقاء على مواقع التواصل الاجتماعي

6 ضع في اعتبارك أن ما تنشره عبر (الإنترنت) يبقى هناك إلى الأبد

7 انتبه عند تثبيت التطبيقات التي يتم الحصول عليها من طرف ثالث

8 فكر مرتين قبل استخدام مواقع التواصل الاجتماعي في العمل

9 ثقف أفراد عائلتك حول مواقع التواصل الاجتماعي

التكنولوجيا:

برامج مكافحة الفيروسات:

استخدم فقط برامج الحماية من الفيروسات ذات المصداقية والتي يتم شراؤها مباشرة من منتجيها أو من وكلائهم المعتمدين.

تم تسجيل حالات قام فيها بعض الموردين ببيع برامج ضارة على أنها برامج للحماية من الفيروسات، لذا يتعين عليك اختيار الموردين الذين يمكن التحقق منهم والوثوق بهم.

يتم يوميًّا إطلاق فيروسات جديدة على (الإنترنت)، لذا يجب عليك تحديث برامج مكافحة الفيروسات لديك بشكل دوري لضمان قدرتها على حمايتك من الفيروسات الحديثة.

برامج مكافحة التجسس:

يمكن استخدام برامج مكافحة التجسس لالتقاط وإزالة برامج التجسس التي تم تثبيتها بالفعل على جهازك، ويمكنك ضبط عملية الفحص لتتم بشكل شهري أو اسبوعي أو حتى يومي، كما يوفر لك هذا النوع من البرامج قائمة بالتهديدات التي يتم العثور عليها، مما يتيح لك القدرة على اختيار ما تريد ازالته منها.

جدار الحماية.

تحتوي بعض أنظمة التشغيل على جدار حماية بشكل افتراضي للتصدي للتهديدات القادمة من (الإنترنت)، ويجب عليك عدم تعطيل هذا الخيار حتى تستبدله بآخر تحصل عليه من طرف ثالث، ويمكن لجدران الحماية منع التهديدات سواء أكانت واردة إلى جهازك أم صادرة عنه.

تأمين المتصفح:

من الممارسات الجيدة استخدام عدة متصفحات (للإنترنت) بدلًا من الاعتماد على برنامج واحد فقط، ويمكنك تعيين أحد المتصفحات لاستخدامه في تصفح المعلومات الحساسة مثل تنفيذ التعاملات المصرفية عبر (الإنترنت) واستخدام آخر لأغراض التصفح الأخرى بشكل عام.

تبدأ عناوين العديد من المواقع بالأحرف (http)، وبالتالي فقد يكون من الصعب معرفة إذا ما كانت هذه المواقع آمنة أم لا، ولكن إذا كان عنوان الموقع يبدأ بالأحرف (https) فهذا يعني أن الموقع يوفر حماية للمستخدمين، ويعد استخدام بروتوكول (SSL) كاستخدام لغة خاصة بين المتصفح والخادم، مما يعني أنه لا أحد يستطيع فهم البيانات التي يتم تبادلها بين الخادم والمتصفح حتى لو استطاع التقاط هذه البيانات.

التحديثات التلقائية:

من أجل ضمان أمان جهازك يجب عليك تثبيت التحديثات الجديدة دائمًا، حيث تسمح هذه التحديثات بتصحيح الأخطاء التي قد تكتشف في نظام التشغيل، مما يؤدي إلى تحسين كفاءة وأداء نظام التشغيل ومضادات الفيروسات وبرامج الحماية الأخرى.

النسخ الاحتياطي:

من الأمثلة على الحوادث التي قد تتسبب في فقدانك البيانات الموجودة على حواسيبك الاستخدامُ غير الملائم، وفقدان الأجهزة أو تعطلها بسبب الكوارث الطبيعية مثل الصواعق والفيضانات، ولكن إذا كنت تقوم بإجراء نسخ احتياطي للبيانات لديك فسوف تكون قادرًا على

استرجاع المعلومات التي قد تفقدها بسبب هذه الحوادث غير المتوقعة.

الطريقة المثلى لإجراء النسخ الاحتياطي هي تخزين الملفات الهامة والضرورية على وحدة تخزين خارجية مثل: قرص صلب خارجي، أو استخدام الأقراص المدمجة، أو حتى إجراء النسخ الاحتياطي عبر (الإنترنت).

إليك بعض أنواع الملفات التي ينصح بإجراء النسخ الاحتياطي لها:

- السجلات البنكية والمعلومات المصرفية الأخرى.
- الصور الرقمية.
- ملفات الموسيقى أو البرامج التي قمت بشرائها أو بتحميلها عبر (الإنترنت).
- المشاريع الشخصية.
- رسائل البريد الإلكتروني وجهات الاتصال والمفكرة.
- مواقع (الإنترنت) المحفوظة في المفضلة.

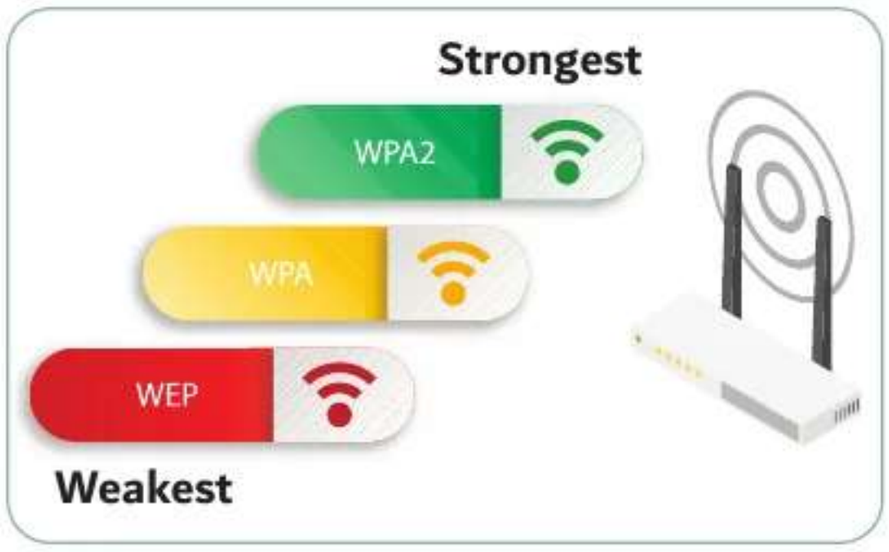
(بروتوكولات) الحماية المستخدمة في تأمين الشبكات اللاسلكية:

عند استخدامك للشبكات اللاسلكية فإنك تقوم بإرسال البيانات من جهازك عبر نقطة وصول، ومن ثم عبر (الإنترنت) إلى خادم ما، ويكمن حدوث 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 حاليًّا 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) لحماية البيانات في أثناء انتقالها بين جهازك ونقطة الاتصال، وتجنب 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.

افعل:

- 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، وعطّل خيارات الإدارة عن بُعد، أو من خلال الاتصال اللاسلكي).
- فعّل خاصية التسجيل على جهاز (الراوتر) اللاسلكي لديك.

تجنب:

- لا تترك الشبكة اللاسلكية دون حماية.
- لا تستخدم (بروتوكول): (WEP).
- لا تشارك كلمات المرور مع غيرك.

الأخطاء الشائعة:

- تعطيل خاصية عرض اسم الشبكة يخفيها، ويحميها من المستخدمين غير المصرح لهم.
- اعتماد التصفية بناء على عناوين (MAC) يمنع المستخدمين غير المصرح لهم من الاتصال بشبكتك.
- خفّض مستوى الإشارة من (الراوتر)، أَوْ ضعه في مكان بحيث لا تخرج الإشارة خارج حدود المنـزل أو المؤسسـة.
- إيقاف (DHCP) أو استخدام عناوين (IP) ثابتة يعدّ طريقة لمنع وصول غير المصرح به.
- تشفير اسم الشبكة أو تغييره باستمرار يزيد من مستوى حماية شبكتك اللاسلكية.

قام شقيقك بربط جهاز (التابلت) الخاص به بشبكة (الواي فاي) غير الآمنة الخاصة بأحد الجيران من دون أخذ إذنه، فما نصيحتك الأخلاقية لشقيقك؟ وما نصيحتك التي يمكن أن تقدمها إلى جارك لجعل شبكة (الواي فاي) الخاصة به أكثر أمانًا؟

مراجعة

1. وضّح أبرز الفروق بين المُخترق والمُخرِّب؟

المخترق	المخرب

2. الحوسبة السحابية هي عبارة عن تقديم الخدمات الحاسوبية عبر (الإنترنت)، وضّح الإيجابيات والسلبيات لهذه التقنية وفق الجدول الآتي:

الإيجابيات	السلبيات

3. بيّن أبرز الأعراض التي قد تظهر على الشخص الذي يتعرض للتنمر الإلكتروني، وكيف يمكنك تقديم المساعدة له؟

- ---
- ---
- ---

4. سجل ثلاثًا من الملفات التي تنصح بإجراء النسخ الاحتياطي لها:

- ---
- ---
- ---

الصحة والسلامة

فهم مبدأ قوانين بيئة العمل الصحية وأهميتها:

إن قوانين بيئة العمل عبارة عن عِلْمٍ يساعد الناس في تكوين وتصميم أجهزة أو أدوات مريحة وسهلة الاستخدام، وبعبارة أخرى، بدلًا من صنع أجهزة حاسوب يضطر المستخدمَ للتكيّف مع الطريقة التي تم فيها تصميم هذه الأجهزة، يتم تصميم الأجهزة والأدوات بطريقة تتلاءم مع أجساد المستخدمين وطريقة تحركهم، وحتى قدراتهم العقلية، ويتضمن هذا قِطعَ الأثاث المريحة المستخدمة وملحقات الحاسوب مثل: الكراسي والفأرة ولوحة المفاتيح التي تقلل من الإجهاد الذي تتعرض له أجساد المستخدمين.

تطبيق قوانين بيئة العمل الصحية في حياتنا:

بعد أن أصبحْتَ تعرف ما هي قوانين بيئة العمل الصحية، وما الذي يمكنك القيام به لتطبيقها؟ توفر قوانين بيئة العمل الصحية للناس الطريقة التي يمكنهم من خلالها العمل والعيش بتناغم مع البيئة المحيطة، كما تساعدهم على الاستمتاع بما حولهم، والشعور بالراحة عند التكيف معها، سواء أكانوا يعملون في وظائفهم أم يستريحون في منازلهم، وعند شعور الأشخاص بالراحة، فإن إنتاجيتهم سوف تتحسن طالما أنهم قادرون على العمل بسهولة كبيرة، والتفكير بصفاء أكثر.

ارتفاع سطح العمل:

1. في البداية، يجب عليك ضبط ارتفاع سطح الطاولة التي تعمل عليها.
2. تأكد من أن مرفقك يرتفع بمقدار إصبع تقريبًا عن سطح الطاولة التي تعمل عليها، وبالتالي لن تضطر للانحناء كثيرًا أو لرفع نفسك عاليًا للوصول إلى الطاولة.
3. قم بتعديل الكرسي بالشكل الذي يلائمك، وقد تحتاج إلى تعديل كل من الطاولة والكرسي أو أحدهما.

الكرسي:

1. من الضروري اختيار كرسي ملائم يسند ظهرك، ويسمح لك بالعمل بسهولة.
2. اختر كرسيًّا يمكن تعديل ارتفاعه ودرجة ميلانه، وتأكد من أن الكرسي في وضع أفقي تقريبًا مع ميلان خفيف يمكّنك من الوصول إلى لوحة المفاتيح أو سطح الطاولة واستخدامها بشكل مريح.

استخدم مساند للأرجل لحمايتها من الإجهاد، أو في حال لم تكن رجلاك تصلان إلى الأرض.

3. لا تجلس بشكل منخفض أو منحني على الكرسي، وعدل مسند الظهر لإراحة أسفل الظهر وتجنب الضغط الزائد.
4. استخدم كراسٍ ذات مساند للأذرع وتأكد من إمكانية ضبطها، قم بتعديل مسند الذراع بحيث يكون ذراعك مرتفعًا قليلًا عند الكتف حيث يسمح هذا الأمر بتخفيف إجهاد الرقبة والأكتاف.

موضع لوحة المفاتيح:

1. عدّل موضع لوحة المفاتيح بحيث يكون الساعدين على استقامة مع اليدين. يجب أن يكون الساعدان في وضع أفقي ويكون الرسغان في وضع مستقيم.
2. تأكد من ألا يكون المرفقان بعيدان جدًا عن جانبي الجسم، وفي هذه الحالة قم بتعديل ارتفاع الطاولة بالشكل المناسب.

موضع الشاشة:

1. قم بتعديل الكرسي بحيث تكون العينان في وضع مريح أمام الشاشة، وتأكد من أن المسافة بين عينيك وبين الشاشة تسمح لك بالتركيز الكامل على ما تراه.
2. عدّل ارتفاع الشاشة بحيث تكون عيناك فوق الحد العلوي لها، مع القدرة على النظر إلى أسفل الشاشة دون الحاجة لإمالة رأسك للأسفل، في هذه الحالة يكون منتصف الشاشة في مستوى الكتفين تقريبًا، وبالتالي لن تحتاج سوى تحريك عينيك إلى الأعلى والأسفل وليس رأسك؛ لرؤية الشاشة كاملة.

حامل المستندات:

1. من الأفكار الجيدة استخدام حامل للمستندات لمساعدتك على تقليل حركة رأسك عند تبديل النظر بين الشاشة والمستندات.
2. ضع حامل المستندات قريبًا من شاشة الحاسوب، واضبطه بحيث لا تضطر للفّ رأسك أو إمالته كثيرًا نحو كل من الشاشة والمستندات التي أمامك.

ترتيب سطح المكتب:

تأكد من أن كافة المستندات والأدوات التي تحتاجها في متناول يديك بحيث لا تضطر لثني أي جزء من جسمك دون حاجة.

وضعية الجسم والبيئة المحيطة في أثناء استخدام لوحة المفاتيح:

1. من الضروري معرفة كيفية الجلوس بالوضعية الصحيحة في أثناء العمل، وقد يتضمن هذا وضعية جلوس مريحة وطبيعية، وبحيث تستطيع التحرك بحرية واتخاذ وضعيات جلوس أخرى، ولا تجلس بطريقة متزمتة أو قاسية.
2. تجنب إجهاد نفسك من خلال تغيير وضعيتك بشكل متكرر، وتجنب الوضعيات الصعبة التي يمكن أن تتسبب في إرهاق المفاصل، ولاسيما الرسغان.
3. خذ فترات قصيرة ومتكررة للاستراحة بدلًا من الفترات الطويلة والمتباعدة، وانتبه لمقدار العمل الذي تقوم بإنجازه، ومن أنك لا تتسبب بأي شكل في زيادة معدل العمل المطلوب منك بشكل حاد أو سريع، وعوضًا عن ذلك، تأكد من أنك تؤدي العمل المطلوب منك بشكل تدريجي وبالسرعة الملائمة لتجنب الإجهاد.
4. يمكنك إطالة المدة التي تعمل من خلالها باستخدام لوحة المفاتيح بعد قضاء فترة راحة طويلة، وذلك فقط في الحالات التي تسمح فيها الظروف بذلك.

مستوى الإضاءة عند استخدام وحدات العرض المضيئة

1. تأكد من أن مستوى الإضاءة حولك كافٍ للعمل على جهاز الحاسوب.
2. تجنب وضع الشاشة بالقرب من النافذة.
3. إذا كانت هناك مستويات مختلفة من الإضاءة، استخدم - وباعتدال- إمكانية تحديد مستوى الإضاءة، ومع ذلك فقد تضطر لاستخدام الشاشات ذات الجودة العالية والمقاومة للمعان.

استخدام الفأرة

1. استخدام فأرة ذات تصميم جيد يساعدك على تجنب الضغط على ساعديك أو رسغيك.
2. لا تستخدم الأنواع ذات الحجم الكبير أو الضخم، والتي ستضطرك لثني رسغيك بزوايا غير مريحة باستمرار.
3. اترك الفأرة لفترات قصيرة متكررة لتجنب الضغط على الرسغين.
4. ضع الفأرة على بعد مناسب من الحاسوب في أثناء الاستخدام.

استخدامات الحاسوب التي تؤثر على الصحة الجسدية:

دعنا نُلقِ نظرة على بعض الإصابات الجسدية التي يمكن أن تحدث نتيجة استخدام الحاسوب باستهتار ولفترات طويلة، وانتبه لكيفية حدوث هذه الإصابات حتى تكون قادرًا على تجنبها.

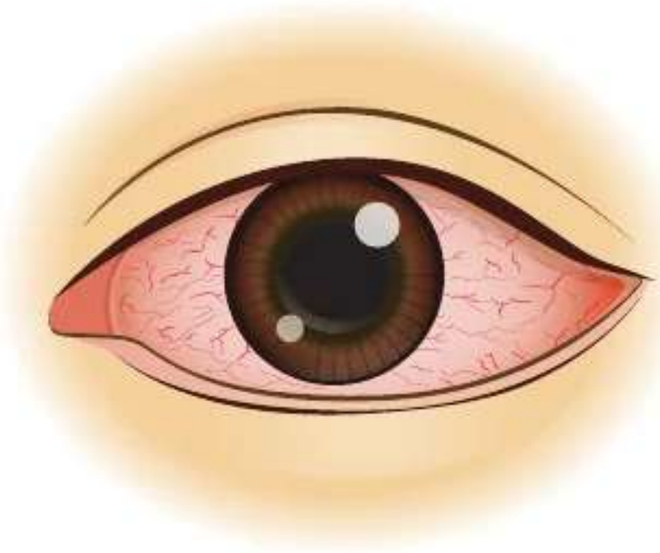
إصابات الإجهاد المتكرر:

تحدث إصابات الإجهاد المتكرر (RSI) بعد استخدام اليدين لفترات طويلة، وقد يؤدي هذا الأمر إلى أعراض عديدة مثل: الإحساس بالألم والحرقان والتورم وتنميل الأطراف وفقدان الإحساس بها بشكل مؤقت، وفقدان المهارة المعتادة في العمل وحتى الضعف، وتعرف إصابات الإجهاد المتكرر بأسماء أخرى مثل: متلازمة الاستخدام الوظيفي الزائد، أو اضطرابات الإصابات التراكمية ومتلازمة الحركة المتكررة.

يعرف الاضطراب الناجم عن حركة اليد المتكررة على نحوٍ أكثر دقة بمتلازمة النّفق الرسغي (CTS)، ويحدث هذا نتيجة لحركة اليدين بتكرار معين مثل: استخدام لوحة المفاتيح في الطباعة واستخدام الفأرة، ويمكنك ملاحظة أعراض هذا الاضطراب مثل: تنميل اليدين وآلام الرسغين، ويحدث كلا العَرضين نتيجةً للضغط على العصب الأوسط الذي يمتد من أسفل الذراع وحتى الأصابع، وقد يكون الألم شديدًا في هذه الحالة، كما قد يمتد ليصل إلى الرقبة.

إجهاد العين:

هل تعلم بأن أكثر من (50%) من مستخدمي الحاسوب يعانون من إجهاد العين! كما أنهم يعانون من نوبات الصداع المتكرر وعدم وضوح الرؤية، إضافة إلى مشاكل بصرية أخرى تحدث بسبب النظر أو التحديق المستمر في شاشات الأجهزة. إن الضغط الواقع على المنظومة البصرية يمكن أن يؤدي إلى ارهاق الجسم كاملًا وتقليل قدرتك على العمل.



إليك بعض أعراض إجهاد العين:

- الشعور بالجفاف والحرقان والحكة في العينين.
- الرؤية غير الواضحة أو المزدوجة.
- الصداع.
- الغثيان.
- الإرهاق.

نصائح لتجنب إجهاد العين:

- استخدم الشاشات التي لا تعاني من اهتزاز، حيث إنّ الشّاشات التي تعاني من الاهتزاز تؤدي إلى إجهاد العين نتيجة النظر غير المريح.
- أسدل الستائر على النوافذ لمنع ضوء الشمس من السقوط مباشرة على الشاشة.
- استخدم أنواع الإنارة التي تسمح بتوزيع الضوء؛ لضمان عدم انعكاسها على الشاشة مباشرة.
- استخدم مصفي (فلتر) الشاشة.
- تأكد من أن عينيك تبعدان (45) سنتيمترًا على الأقل عن الشاشة.
- أعط الفرصة لعينينك للراحة من خلال التوقف بشكل دوري عن النظر إلى لشاشة، وقم بالتركيز على شيء بعيد.
- خذ استراحة لمدة (5) دقائق في كل ساعة.
- قم بفحص عينيك بشكل دوري، واستخدم نظاراتك -إذا كانت موصوفة لك طبيًّا- عند العمل على جهاز الحاسوب.

آلام الظهر:

من الممكن أن تكون قد أحسست بالألم في أسفل الظهر نتيجة العمل باستخدام الحاسوب والجلوس على الكرسي لفترة طويلة، وربما تكون هذه الحالة قد تسببت في زيادة مشاكل الظهر أو الرقبة سوءًا، فلماذا يحدث هذا الأمر؟ يحدث هذا الأمر بسبب الجلوس أمام الحاسوب، أو في أي مكان آخر بوضعية ثابتة مما يؤدي إلى زيادة الضغط الواقع على الرقبة والظهر والأكتاف والساعدين والساقين، مما يؤدي إلى زيادة الضغط على عضلات الظهر وفقرات العمود الفقري.

إضافة إلى ذلك، يميل الناس عادة إلى الجلوس بشكل منحنٍ على الكراسي عند الجلوس لفترات طويلة، وقد يؤدي هذا إلى زيادة تمدد الأربطة الشوكية، كما يؤدي إلى زيادة إجهاد فقرات وبنية العمود الفقري.

المشاكل الاجتماعية المرتبطة باستخدام الحاسوب و(الإنترنت):

دعنا نُلقِ معًا نظرة على بعض المشاكل الاجتماعية المرتبطة بالاستخدام الزائد للحاسوب و(الإنترنت).

نصائح لتجنب آلام الظهر:

- استخدم كرسيًّا يمكن تعديله بشكل كامل، وعلى نحو سهل، وتأكد من أنك تستطيع تعديل الارتفاع ووضعية الجلوس.
- ابحث عن الكراسي التي تأتي مع مسند للأرجل، أو قم بشراء واحد منفصل حتى تتمكن من وضع رجليك في زاوية مريحة.
- استخدم شاشات قابلة للتعديل، وضعها في مكان ملائم بحيث لا تضطر إلى ثني رقبتك للنظر إليها.
- تذكر أن تأخذ فترات استراحة قصيرة ومتكررة، وانهض من مكانك، وامش في الأرجاء، ومارس تمارين التمدد للذراعين والرقبة والساقين للتخفيف من الشد العضلي.
- حافظ على ظهرك مستقيمًا ورأسك للأعلى عند الجلوس، ولا تقم بالانحناء في الكرسي، وإذا قمت بهذا لاشعوريًّا فعدّل وضعية جلوسك فورًا.

مفترسو (الإنترنت):

يعتمد الكثير من الناس على استخدام مواقع التواصل الاجتماعي نظرًا للقدرة على التواصل مع الآخرين ومشاركة المعلومات وتحسين العلاقات الاجتماعية بشكل متبادل، حيث يمكن العثور على أصدقاء جدد أو حتى ملاقاة الشريك المستقبلي عبر (الإنترنت)، ولكن انتبه، قد تترتب على مشاركتك الكثير من معلوماتك الشخصية مع من أصبحوا أصدقاءً لك عبر (الإنترنت) خطورةٌ بالغة.

يمكن أن تتعرض لخطر ملاحقتك من قبل أحدهم على (الإنترنت)، وهذا نوع من التحرش باستخدام (الإنترنت)، وبوضوح أكثر، يعرف هذا باسم المطاردة الإلكترونية، وقد يبقى هذا النوع من التحرش على (الإنترنت)، أو قد يبدأ من هناك حتى يمتد إلى العالم الحقيقي، وفي كلا الحالين يبقى هذا الأمر مزعجًا جدًا، وعلاوة على ذلك فإن العديد من ضحايا المطاردة الإلكترونية هم من صغار السن، ويطلق على من يقومون بهذا النوع من التصرفات تسمية (مفترسو (الإنترنت).

الانعزال عن العائلة والأصدقاء:

إن الأشخاص الذين يقضون ساعات طويلة منعزلين عمن حولهم في أثناء استخدام (الكمبيوتر) يميلون إلى إهمال علاقاتهم مع الآخرين، ولاسيما أُسرهم وأصدقاؤهم، كما يؤدي هذا الأمر إلى إهمالهم لتطوير مهاراتهم الضرورية الأخرى أيضًا، كما يعانون في أغلب الأحيان من صعوبات ومن عدم الارتياح عند الالتقاء بالآخرين والتحدث معهم.

اضطرابات النوم:

يعاني مدمنو (الإنترنت) من اضطرابات النوم، ويتسبب هذا الوضع القهري في إعاقة دورة النوم الطبيعية، مما يعني أن الشخص الذي يبقى مستيقظًا في الوقت الذي يفترض أن ينام فيه أو العكس إلى تكوين عادات سلبية، وإلى نقص في الأداء الدراسي أو الوظيفي، وإلى نقص في الإنتاجية والنوم في أوقات غير مناسبة.

نشاط

كيف يمكنك معرفة أن صديقك مدمن على (الإنترنت)؟

التسوق القهري عبر (الإنترنت):

من العادات السلبية الأخرى التي تنتج عن استخدام (الإنترنت) لفترات طويلة التسوق القهري عبر (الإنترنت)، إذْ يقوم المتسوقون القهريون عبر (الإنترنت) بشراء أشياء بشكل عفوي أو فوري، وبتنفيذ عمليات شراء غير مخطط لها مسبقًا أو حتى شراء أمور لا يحتاجونها أصلًا.

لذلك ينبغي علينا الحذر من هذا النوع من التصرفات حتى لا يتحول الأمر إلى شكل من أشكال الإدمان المؤدي لتبديد الأموال وتضييع الكثير من الوقت في البحث عن أرخص المنتجات، كما يكون من الصعوبة عليك الحصول على راحة البال إذا تورطت في تعاملات مصرفية سيئة عبر (الإنترنت)، والتي ستؤدي بك إلى فقدان التركيز على النواحي الأخرى من حياتك.

المقامرة القهرية عبر (الإنترنت):

نوع آخر من العادات السيئة أو الإدمان التي قد تتعرض لها عند قضاء وقت طويل على (الإنترنت)، مثلها مثل التسوق القهري، حيث تتم المقامرة عبر (الإنترنت) بشكل عفوي وفوري، وطبعًا هذه المواقع التي تمكن من إجراء مقامرات عبر (الإنترنت) ليست بالمواقع المرخصة أو المسموح بها.

تعمل المقامرة عبر (الإنترنت) على حرمان المقامر من التفاعل الاجتماعي مع الآخرين بالشكل السليم، لذا فإن الناس الذين يقضون أوقاتهم أكثر فأكثر في المقامرة على (الإنترنت) يجدون أنفسهم وقد أصبحوا في منأى عن عائلاتهم وأصدقائهم، كما يؤدي هذا إلى تدمير العلاقات مع الآخرين نظرًا لأن المقامر يصعب عليه التركيز على أي شيء سوى المقامرة.

وقد يأخذ هذا الأمر منحىً آخر أكثر حدة، كسرقة المال والاستدانة من المرابين من أجل المقامرة من جديد، مما يعرض المقامر وكل مَن حوله إلى خطر بالغ.

إدمان اللعب عبر (الإنترنت):

من أنواع الإدمان الأخرى كذلك إدمان اللعب عبر (الإنترنت)، وقد يتعرض الأطفال الصغار لمثل هذا النوع من الإدمان وخاصة أولئك الذين يُتْرَكون دون رقابة من ذويهم على أفعالهم أو على الأنشطة التي يقومون بها.

وفي الوقت ذاته يجب على اللاعبين تعلم كيفية البقاء متأهبين ونشطين لحل المشاكل أو التعامل مع المواقف الصعبة، وعلى الرغم من هذه الفوائد إلا أن الألعاب الإلكترونية لها تأثير سلبي أيضًا قد يكون ناتجًا عن قضاء أوقات طويلة في ممارسة هذه الألعاب، ومن هذه السلبيات:

- الانطواء الاجتماعي: يقضي ممارسو الألعاب عبر (الإنترنت) الكثير من الوقت مُلتصقين بألعابهم، ويعانون من صعوبة التوقف عن ممارستها نتيجة الشغف لمعرفة ما سيحدث أو للفوز باللعبة.
- وفي أغلب الأحيان، يقوم اللاعبون - حالهم كحال من يقضي أوقاتًا طويلة على (الإنترنت) - في الدردشة والرسائل الفورية للتواصل مع الآخرين.
- يمكن أن يواجه اللاعبون الذين يعانون من تردي المهارات اللفظية - بسبب المشاكل المذكورة آنفًا - من مشاكل أخرى مثل: إجراء مقابلات العمل أو عند إتمام مهمة ما في العمل تتطلب منهم التواصل اللفظي مع المتعاملين.
- يميل الكثير من الناس الذين يقضون أوقاتًا طويلة على (الإنترنت) إلى الإستعجال والإسراع في الرد على نظرائهم على (الإنترنت)، مما يعني الاستعجال في طباعة الكلمات وبالتالي ارتكاب الأخطاء الإملائية والنحوية، قد يؤدي اعتيادهم على هذا الأمر لامتداده إلى حياتهم الواقعية مما سيسبب لهم مشاكل كثير عند الكتابة أو الإجابة على أسئلة الامتحانات.
- إن ممارسي الألعاب الإلكترونية عرضة لفرط الحساسية والإحباط الاجتماعي، كما قد يكونون عرضة للغة بذيئة في حال خسارة اللعبة أو عندما يعلقون في موقف يصعب حله.
- في النهاية، إن قضاء الأوقات الطويلة على (الإنترنت) قد يؤدي بك لتدمير الروابط بينك وبين أفراد عائلتك وأصدقائك، ولن تنتبه إلى حاجتك لتحسين مهاراتك الاجتماعية لأنك فقدت الاهتمام بالحياة الاجتماعية.

أعراض الإدمان على (الإنترنت):

هناك العديد من الأعراض والعلامات الدالة على الإدمان على (الإنترنت)، وقد تختلف هذه الأعراض من شخص لآخر، ولا يمكن تشخيص الإدمان على (الإنترنت) من خلال معرفة الساعات التي يقضيها الشخص في استخدام الحاسوب، أو من خلال عدد الكلمات التي يطبعها؛ لأنه قد تكون من متطلبات العمل، ولكن يمكن معرفة ما إذا كان أحدهم مدمنًا على (الإنترنت) بشكل عام في حال ملاحظة العلامات التحذيرية الآتية:

01

قضاء أوقات طويلة على الإنترنت لدرجة فقدان الإحساس بالوقت:

هل اكتشفت ولعدة مرات أن قضيت أكثر من الوقت الذي كنت تنوي قضاءه على (الإنترنت)؟ هل طالت (العشر دقائق) لتصل إلى (ساعتين)؟ هل تسبب قضاء الوقت الطويل على الإنترنت في تأخيرك عن مواعيدك أو عن مدرستك أو عملك؟ هل يضايقك بشدة أن يقاطعك أحدهم أثناء تركيزك على نشاطاتك على الإنترنت؟

02

المعاناة من صعوبة إكمال المهام في العمل أو المنزل:

هل اكتشف فجأة أنه لا يوجد طعام لوجبة العشاء؟ أو أنه يوجد الكثير من الملابس المتسخة وليس لديك سوى القليل من الملابس لترتديها؟ ربما يحصل أن تبقى في العمل لوقت متأخر - ربما دون أن تحس بذلك - من أجل إنهاء عملك لأنك أضعت وقتك على (الإنترنت)، وقد يكون تأخرك أحيانًا من أجل تصفح (الإنترنت) بحرية أكبر.

03

الابتعاد عن العائلة والأصدقاء:

هل تهمل حياتك الاجتماعية وينتابك شعور بالذنب نحو هذا الفعل؟ أو ربما لا تكون قد لاحظت أن عائلتك وأصدقاءك قد بدأوا بالانسحاب من حياتك؟ هل تشعر بأنه لا يوجد أحد في حياتك الواقعية قادر على فهمك مثل: أصدقائك في حياتك على (الإنترنت)؟

04

فقدان الشعور بالذنب والمشاعر الدفاعية حيال استخدامك للانترنت:

هل سئمت من تذمر من هم حولك بسبب الوقت الطويل الذي تقضيه على (الإنترنت) والوقت القصير الذي تقضيه معهم؟ هل تحاول اخفاء استخدامك (للانترنت) أحيانًا أو تكذب حيال الوقت الذي قضيته؟

التخلص من معدات الحاسوب وتدويرها بالشكل الملائم:

يتحتم عليك معرفة الطرائق الملائمة لإعادة تدوير مخلفات الحواسيب بالشكل الملائم؛ نظرًا لأن أجهزة الحاسوب لها تأثيرات كبيرة على البيئة، سواء أكان ذلك في عملية إنتاجها أم استخدامها أم التخلص منها. تتضمن عملية تصنيع الحواسيب استخدام مقادير بسيطة من المعادن والمواد ذات المخاطر الصحية مثل: المخلفات السامة التي يمكن أن تشكل تهديدًا على صحتك، وعلى الرغم من أن الحواسيب المستعملة توفر بعض العناصر المفيدة مثل: النحاس والرصاص إلا أنها تحتوي أيضًا على مواد مؤذية يمكن أن تتسبب في إلحاق الأذى بالبيئة إذا تم التخلص منها بطريقة غير ملائمة، وتشمل هذه الأجزاء إضافة إلى أجزاء أخرى:

- الزئبق الموجود في مصابيح الإنارة.
- (الكادميوم) والمواد السامة الأخرى المحتملة، والموجودة في بطاريات الأجهزة المحمولة.
- الرصاص الموجود في الدوائر الكهربائية.

يمكن استخدام الحواسيب في إيجاد بيئة تستفيد من تقليل كميات الورق في مكاتب العمل، وبالتالي تقليل عدد الأشجار التي يتم قطعها للحصول على الورق، كما يسهم في دراسة الأنظمة البيئية المعقدة وإتاحة العلوم البيئية بشكل أكثر توسعًا، ولكن أجهزة الحاسوب في نهاية عمرها تصبح خطرًا على البيئة نظرًا للعناصر الضارة التي تحتويها، لذا يجب عليك معرفة ما الذي يمكنك فعله للتقليل من آثار مخلفات الحواسيب على البيئة؟ وإليك بعض الأمور التي يمكنك القيام بها.

الاستخدام عند الضرورة:

1. قم بشراء الشاشات التي لا تستهلك كميات كبيرة من الطاقة في أثناء عدم استخدامها.
2. اطبع فقط عند الضرورة، واقرأ المستندات من الشاشة إذا أمكن، وأعطها لغيرك في نسختها الإلكترونية.
3. أطفئ جهاز الحاسوب بدلًا من تركه في وضع الاستعداد إذا كنت ستتركه لفترة من الوقت.

التبرع:

1. إذا احتجت لشراء جهاز جديد، لا تحتفظ بجهازك القديم ما لم تكن تنوي الاستمرار في استخدامه.
2. بالمقابل، يمكنك إعطاء جهازك القديم لشخص يستفيد منه، أو تبرّع به للجهات الخيرية، وتذكر أن تقوم بإزالة القرص الصلب حتى لا يتمكن المستخدم الجديد من استرجاع بياناتك المهمة.

إعادة التدوير:

1. يمكنك جمع الأوراق المستخدمة التي لم تعد بحاجة إليها وإرسالها إلى مراكز إعادة التدوير، وعندما ترغب في طباعة صفحة تجريبية استخدم الوجه الفارغ من صفحة سبق استعمالها.
2. قم بإعادة تدوير حواسيبك القديمة وتعبئة أحبار الطابعات.
3. في حال تعطل جهازك بشكل لا يمكن إصلاحه أو لم يعد صالحًا للاستخدام لأي سبب ما، يجب عليك أخذه إلى أقرب مركز لإعادة التدوير، وتأكد من إعطائه لقسم إعادة تدوير الحواسيب إن أمكن.

نشاط

- ناقش مع زملائك الإجراءات التي يمكنك اتخاذها من أجل مراعاة البيئة عند استخدام التقنيات الحديثة.

كيف يمكنك مسح البيانات نهائيًّا من حاسوبك القديم:

يقوم الناس باستبدال أجهزتهم في الوقت الحاضر في كل ثلاث أو أربع سنوات، ولكن للأسف لا يعرف الكثير منهم كيفية التخلص من هذه الأجهزة بالشكل السليم.

هل تعلم أنه حتى لو قمت بمسح البيانات جميعها فعليًّا من جهازك فإنه يمكن للآخرين العثور على طريقة تمكّنهم من استرجاعها!

اتبع الخطوات الثلاث البسيطة هذه حتى تتخلص وبشكل نهائي من البيانات الموجودة على جهازك القديم:

إذا كنت تنوي التبرع بجهازك القديم للجهات الخيرية، أو حتى لو كنت ترغب في بيعه فيجب عليك في هذه الحالة شراء البرامج الملائمة التي تسمح لك بالتخلص من البيانات الموجودة على القرص الصلب.

مراجعة

1. سجل ثلاث طرائق لتجنب آلام الظهر.
   - _____
   - _____
   - _____
2. وضّح ثلاثًا من أعراض إجهاد العين، وكيفية تجنبها؟
   - _____
   - _____
   - _____
3. ناقش مع زملائك واحدًا من أعراض الإدمان على (الإنترنت)، واكتب عنه تقريرًا، واعرضه على زملائك.
   - _____
   - _____
   - _____
   - _____
4. بيِّن ثلاثًا من المشاكل الاجتماعية المرتبطة باستخدام الحاسوب و(الإنترنت)، وسجلها.
   - _____
   - _____
   - _____

5. اكتب أربعًا من سلبيات إدمان اللعب عبر (الإنترنت).

- _____
- _____
- _____
- _____

الخدمة

الوطنية

لون الحلقة

- يدل الرمز على نوع الكتاب (مثال كتاب طالب)
- الرقم 3 المظلل يرمز الى رقم **المجلد** من كتاب الطالب
- الرقم 9 يرمز الى الصف
- يرمز المسار التعليمي

- كتاب الطالب
- كتاب النشاط (التمارين)
- كتاب القراءة (اللغة العربية، الدراسات الاجتماعية)
- دليل الطالب التفاعلي (الرياضيات)
- دليل الأنشطة المختبرية (العلوم)
- دليل المعلم

مركز اتصال وزارة التربية والتعليم
اقتراح - استفسار - شكوى

80051115
www.moe.gov.ae
Info@moe.gov.ae