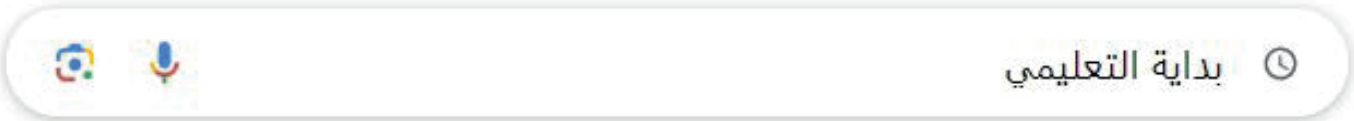
تم تحميل الملف
من موقع بداية

بداية
beadaya.com | موقع بداية التعليمي

للمزيد اكتب
في جوجل Google



موقع بداية التعليمي كل ما يحتاجه **الطالب والمعلم**
من ملفات تعليمية، حلول الكتب، توزيع المنهج،
بوربوينت، اختبارات، ملخصات، اختبارات إلكترونية،
أوراق عمل، والكثير...

حمل التطبيق

GET IN ON Google Play

Download on the App Store

رابط الدرس الرقمي

www.ien.edu.sa

4.4 كيف تحمي مواردك المالية؟

أهداف التعلّم

بعد الانتهاء من هذا الدرس، ستكون قادرًا على:

- تحديد الطرائق التي تساعدك على حماية مواردك المالية.
- شرح النقاط الرئيسة في حملة "خلك حريص".

المصطلحات الرئيسة

التحقق الثنائي (2FA)	Two-Factor Authentication		
التصيّد الاحتيالي	Phishing	الاحتيال	Fraud
المحتال	Phisher	سرقة الهوية	Identity Theft
		المخترق	Hacker

هل تترك باب منزلك مفتوحًا على مصراعيه عندما تذهب لقضاء إجازة؟ وهل يترك والداك مفاتيح السيارة داخلها أثناء وجودهما في العمل؟ عليك التأكد من الحفاظ على أصولك بأمان بهدف حمايتها من السرقة أو سوء الاستخدام.

بداية
موقع بداية التعليمي | beadaya.com



◄ ما الضرر الذي يحدث في حال حصول شخص آخر على كلمات المرور الخاصة بحسابك المصرفي وحساباتك على مواقع وسائل التواصل الاجتماعي؟

يمكن أن يؤدي ذلك إلى:

1- سرقة الهوية.

2- الاحتيال المالي.

3- الاختراق الإلكتروني

4- التشهير الإلكتروني.

5- الاستغلال الجنائي.

حماية الثروة المالية
Protecting Financial Wealth

تمامًا مثلما تحمي أصولك ومختلف حساباتك، يجدر بك أيضًا حماية ثروتك المالية. ولتجنب خسارة أموالك، هناك خطوات عديدة يمكنك اتخاذها، ونذكر منها ما يلي:

- تعامل مع المستشارين الماليين والمؤسسات المالية التي تعرفها وتثق بها فقط. وقبل أن تباشر العمل مع أيّ مستشار مالي جديد، تحرّ عنه بدقة. ويمكنك التحري عن أي شخص عن طريق:
  - الحصول على توصيات من الأصدقاء، والزملاء، ومحيط الأسرة.
  - الحصول على توصية من مؤسسات موثوقة، مثل: السوق المالية السعودية "تداول".
  - الاستعانة بالتعليقات الواردة في المنتديات ذات الصلة عبر الإنترنت.
- كن مطّلعًا على الاقتصاد وكيفية تأثيره على مواردك المالية الشخصية، فمن واجبك معرفة متى تطرح الأسئلة وتتخذ القرارات فيما يتعلق باستثماراتك. ويمكنك القيام بذلك باتباع الخطوات التالية:
  - قراءة ومشاهدة الأخبار من مصادر موثوقة.
  - قراءة مجلات التجارة والأعمال التي تتعلق باستثماراتك.
  - فهم الاقتصاد على الصعيد العالمي وكيفية تأثيره على الاستثمارات.
- احتفظ بسجلات دقيقة وتحقق من أرصدة الحسابات بانتظام، وذلك عبر اتباع الخطوات التالية:
  - استخدام طرائق حفظ السجلات الإلكترونية.
  - تحميل التطبيقات ذات صلة بالبنك وحسابات التداول الخاصة بك.
  - تخصيص وقت كل أسبوع لمراجعة مواردك المالية.
- احتفظ بالكشوفات الشهرية لحسابك المصرفي في مكان آمن عبر اتباع الخطوات التالية:
  - إذا كانت كشوفاتك المصرفية مطبوعة على ورق، فاحتفظ بها في درج أو خزانة ملفات مقفلة.
  - إذا كانت كشوفاتك المصرفية إلكترونية، فتأكد من استخدام كلمة مرور قوية لملفاتك وحاسوبك.
- احم كلمات المرور الخاصة بحسابات الخدمات المصرفية وحسابات الاسَتثمار عبر الإنترنت، وتأكد ممّا يلي:
  - عدم استخدام كلمات مرور سهلة التخمين، مثل: الأرقام "1234"، أو اسمك.
  - عدم استخدام كلمة المرور نفسها التي تستخدمها لحسابات وسائل التواصل الاجتماعي والحسابات الترفيهية الأخرى.
  - عدم تدوين كلمة المرور على ورقة يستطيع الآخرون الوصول إليها بسهولة.
  - عدم مشاركة كلمة المرور أو تفاصيل تسجيل الدخول الخاصة بك مع الآخرين على الإطلاق.
  - استخدام ميزة **التحقق الثنائي Two-Factor Authentication (2FA)** عند توفرها.

التحقق الثنائي (2FA)
خطوة إضافية للأمان تتطلّب شكلًا آخر لتعريف كلمة المرور، مثل: بصمة الإصبع، أو تطبيقات التحقق المستخدمة في الهاتف الجوّال

beadaya.com | موقع بداية التعليمي

◄ كيف يمكن لبصمة إصبعك أن تساعدك على حماية بياناتك الشخصية والمالية؟

تستطيع بصمة الإصبع أن تساعد في حماية بياناتك الشخصية والمالية بسبب طبيعتها الفريدة والصعبة الإنكار، و يمكن استخدامها كطريقة لتأمين حساباتك الشخصية و المالية على الإنترنت ، و يمكن الاستفادة من بصمة الإصبع في الأمور التالية:

1- فتح الحسابات المصرفية: يمكن استخدام بصمة الإصبع لفتح حسابات مصرفية عبر الإنترنت؛ وذلك بدلاً من استخدام كلمات المرور والأسئلة السرية.

2- فتح الهواتف الذكية: يمكن استخدام بصمة الإصبع لفتح الهواتف الذكية؛ وذلك بدلاً من استخدام أنماط فتح الشاشة أو كلمات المرور.

3- التحقق من الهوية: يمكن استخدام بصمة الإصبع للتحقق من الهوية عند الدخول إلى حساباتك الشخصية والمالية على الإنترنت، وذلك بدلاً من استخدام كلمات المرور.

4- التأكد من الشراء: يمكن استخدام بصمة الإصبع للتأكد من عمليات الشراء عبر الإنترنت؛ وذلك لضمان أن العملية تتم بواسطة حامل الحساب الشخصي فقط.



أساليب الاحتيال
Methods of Fraud

يحاول الناس، عبر أساليب عديدة، الاحتيال على الآخرين ليعطوهم المال. الاحتيال جريمة، وقد يكون من الصعب جدًّا في بعض الأحيان استرداد الأموال التي استُولِي عليها بطريقة غير قانونية عن طريق الاحتيال. وأفضل طريقة لحماية أموالك هي أن تكون على معرفة بالأساليب الشائعة المتبعة في الاحتيال.

التصيّد الاحتيالي
Phishing

يجب عليك أيضًا أن تتوخّى الحذر من عمليات **التصيّد الاحتيالي Phishing**. يرسل **المحتالون Phishers** و**المخترقون Hackers** رسائل إلكترونية ينتحلون فيها صفة أصدقائك، أو أفراد أسرتك، أو بنك ما، أو أي مؤسسة شرعية أخرى. وقد تطلب منك هذه الرسائل الإفصاح عن معلومات شخصية، مثل:

- أرقام الحساب المصرفي.
- أرقام البطاقة المصرفية.
- تفاصيل تتعلق بالأمان، مثل: كلمات المرور، أو الإجابات السرية.

لا تتفاعل مع محاولات تسعى إلى الحصول على معلوماتك الشخصية، فالبنوك والمؤسسات الشرعية لا تطلب تزويدها بمعلومات مماثلة عبر البريد الإلكتروني، أو حتى عبر اتصال هاتفي.

التصيّد الاحتيالي
عملية احتيال عبر الإنترنت تستخدم الرسائل الإلكترونية بهدف خداعك للإفصاح عن معلومات شخصية

المحتال
مهاجم ينتحل صفة شركة أو شخص حسن السمعة عبر الرسائل الإلكترونية أو أشكال التواصل الأخرى

المخترق
شخص يستغل نظام حاسوب معينًا للوصول بطريقة غير مصرح بها إلى نظام آخر لسحب البيانات

سرقة الهوية
استخدام معلوماتك الشخصية من قبل شخص آخر دون موافقتك لارتكاب جريمة احتيال، أو جرائم أخرى

سرقة الهوية
Identity Theft

في حال زودت هؤلاء المحتالين بمعلوماتك المالية، فقد تقع ضحية عملية **سرقة الهوية Identity Theft**. الأشخاص الذين ينجحون في الحصول على معلوماتك الشخصية قد يتقدمون بطلب للحصول على منتجات مالية جديدة باسمك، أو سحب الأموال من حساباتك.

وقد تتسبب سرقة الهوية بمشكلات قصيرة وطويلة الأجل. ومن المشكلات القصيرة الأجل الشائعة نذكر ما يلي:

- خسارتك لأموالك من حساباتك المصرفية.
- عدم القدرة على دفع تكاليف قصيرة الأجل (مثل: الغذاء والإيجار).
- هدر الوقت في التواصل مع البنوك والمؤسسات المالية الأخرى لإيقاف عملية سرقة الهوية.
- الاضطرار إلى تغيير التفاصيل المصرفية والمالية لمنع تكرار سوء الاستخدام.

ومن أمثلة المشكلات الطويلة الأجل الشائعة ما يلي:

- **مشكلات مالية:**
  - مواجهة الصعوبات في التقدم بطلب للحصول على قروض مصرفية ورهون عقارية في المستقبل.

بدايه
موقع بدايه التعليمي | bedaya.com

- **مشكلات نفسية:**
  - قد تلومك أسرتك إما بسبب عدم توخي الحذر بما فيه الكفاية، أو بسبب الآثار التي نتجت عن سرقة الهوية.
- **مشكلات اجتماعية:**
  - قد يلجأ المخترقون، الذين استطاعوا الوصول إلى حساباتك عبر مواقع التواصل الاجتماعي، إلى الإضرار بسمعتك بنشر تعليقات مضلِّلة عبر الإنترنت.

توخي الحذر
Staying Careful

قد يكون من الصعب توخي الحذر عبر الإنترنت حتى بالنسبة للأشخاص الذين يحترزون من التقنية ولا يثقون بها، أما جيل الشباب الذي نشأ على تقنية الهاتف الذكي ويستخدمها براحة تامة قد يكون أكثر عرضة للعمليات الاحتيالية غير المتوقعة.

الهندسة الاجتماعية
Social Engineering

ما مدى ثقتك بصحة رسالة تتلقاها عبر بريدك الإلكتروني أو حسابك عبر وسائل التواصل الاجتماعي؟ يتقن المجرمون فنّ التلاعب بالأشخاص لدفعهم إلى الإفصاح عن معلومات حساسة، مثل: تفاصيل حسابهم المصرفي. لذلك، تهدف حملة "خلك حريص" إلى رفع مستوى الوعي بالأساليب المتبعة في **الاحتيال Fraud**، لمساعدة جميع المواطنين السعوديين على حماية أنفسهم من هذه المخاطر.

الاحتيال
جريمة خداع الناس لاختلاس المال منهم

بداية | موقع بداية التعليمي
beadaya.com

خمس خدع يستخدمها المحتالون
Five Tricks That Fraudsters Use

أصدرت المؤسسات المالية السعودية، استنادًا إلى أبحاث أجرتها في هذا المجال، دليلًا مؤلفًا من خمس نقاط يوضح كيف يطبق المحتال الهندسة الاجتماعية للاحتيال. وتشمل الخدع الخمس التي يستخدمها المحتالون ما يلي:

- **انتحال الشخصية Impersonation:** قد يتظاهر المجرم بأنه موظف، مثل: محامٍ، أو طبيب، أو موظف يعمل في بنك بغرض إبهارك باللقب.
- **دراسة السلوك Study of Behavior:** قد يدرس المحتال سلوكك بهدف التوصل إلى معلومات خاصة بك وتحليل شخصيتك وإيجاد طرائق لخداعك.
- **استغلال الفرص Taking Advantage:** يحتاج العملاء إلى السلع والخدمات، وقد يستغل المجرمون هذه الاحتياجات لخداعهم.
- **استخدام العواطف Use of Emotion:** قد يستخدم المجرم أساليب عاطفية لإقناعك.
- **طلب المعلومات الشخصية Requesting Personal Information:** قد يطلب منك المحتال بيانات حساسة، مثل: المعلومات الشخصية، أو التفاصيل المصرفية.

كيفية كشف عملية احتيال محتملة

How to Identify a Potential Fraud

عندما تتلقى اتصالًا أو بريدًا إلكترونيًّا مجهولًا يدعوك إلى الضغط على روابط معينة ويعِدك بأمور يصعب تصديقها، يُرجّح أن يكون ذلك عملية احتيال.

فيما يلي بعض العلامات التي يجب توخي الحذر منها:



beadaya.com موقع بداية التعليمي

في حال تلقيت رسالة إلكترونية تحتوي على العديد من الأخطاء الإملائية، يجدر بك توخي الحذر، فالمؤسسات المحترفة دائمًا ما تتحقق من الرسائل قبل إرسالها وتحرص على خلوّها من أي أخطاء إملائية ولغوية. تشير بالتالي الرسائل التي صيغت بأسلوب ضعيف وغير واضح إلى أنها رسائل احتيالية.

دورك لتفكر

متروك للطالب

عند التعامل مع الموارد المالية، لا بد أن تفكّر في الأمان. ما الخطوات التي قد تتخذها لتحسين أمنك المالي؟

فكّر فيما يلي:

1. ما الخطوات التي يمكنك اتخاذها في الوقت الراهن؟
2. ما المجالات المتعلقة بأمنك المالي وأمنك عبر الإنترنت التي يمكنك تعزيزها؟
3. ما أفضل الأساليب التي تساعدك على حماية مواردك المالية وأمنك عبر الإنترنت؟

أسئلة المراجعة

اختَر الإجابة الصحيحة.

1. استخدام كلمات مرور مختلفة لكل من حسابات وسائل التواصل الاجتماعي والخدمات المالية ضروريّ.
   - أ. صواب
   - ب. خطأ
2. قد يستخدم المحتالون بياناتك المسروقة للقيام بما يلي:
   - أ. فتح حسابات مصرفية جديدة.
   - ب. سرقة أموالك.
   - ج. الذهاب في إجازة مع أصدقائك.
   - د. نشر رسائل خاطئة على حساباتك في وسائل التواصل الاجتماعي.
3. أيّ ممّا يلي ليس أحد أنواع المشكلات الطويلة الأجل التي قد تترتب على سرقة الهوية؟
   - أ. المشكلات المالية.
   - ب. المشكلات النفسية.
   - ج. المشكلات الاجتماعية.
   - د. المشكلات المكانية.
4. عليك اختيار كلمة مرور بسيطة يسهل تذكرها.
   - أ. صواب
   - ب. خطأ
5. تتطلّب ميزة التحقق الثنائي (2FA) بصمة الإصبع أو تطبيقًا من تطبيقات التحقق بالإضافة إلى كلمة المرور.
   - أ. صواب
   - ب. خطأ

beadaya.com | موقع بداية التعليمي