وزارة التربية والتعليم

8

أمن وحماية المعلومات

كتاب الطالب

الصف الثامن

نحو ثقافة إلكترونية آمنة

هيئة تنظيم الإتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

aeCERT Computer Emergency Response Team

تمهيد

الإنترنت .. عالم واسع .. شبكة عملاقة .. تلف الكرة الارضية شمالا وجنوبا ، شرقا وغربا.. دخول شبكة الإنترنت أشبه بالجولة في مملكة معظم الموجودين فيها سواحٌ ومسافرون من جميع بقاع العالم، والكل يتجول ويتنقل بحرية تامة دون هويات أو تأشيراتٍ للزيارة، حيث لا حدود ولا مراكز جمركية ولا فواصل طبيعية ، والتنقل والتجول فيها ممتعٌ جدا وشيقٌ وهو لا يعدو أكثر من نبضات الكترونية تربط أطراف ومعالم هذه المملكة العامرة..ودخول الشبكة (المملكة) يمثل مغامرة مثيرة للوهلة الأولى، ورغبة شديدة في التعرف على كل شيء والإطلاع عليه ..

هذا الإتساع المترامي لشبكة الإنترنت، صاحبه بروز ظواهر سلبية بين مرتادي الشبكة، وظهور جوانب تستلزم منا أخذ الحيطة والحذر من بعض التهديدات والمخاطر، ولذلك لحماية أنفسنا من التأثيرات المجهولة عبر هذا العالم الإلكتروني الهائل.

قد تكون البداية مجهولة ومشوشة .. ولكن سرعان ما تبدو جميع الأمور طبيعية ومنتظمة، حين إتباع الإرشادات والتعليمات التي ستأخذك لبر الأمان.

هذا المنهج يمثل أحد المصادر الهامة للتوعية بأمن وحماية المعلومات، وهو مادة مساندة للتعريف بكيفية الحد من المخاطر والإستفادة من فرص الإنترنت. كما يهدف إلى تعزيز قدرات وتغيير سلوك الطلاب في التعامل مع الإنترنت. يسعى هذا المنهج في نهاية المطاف الى نشر ثقافة إلكترونية آمنة عبر المؤسسات التربوية والتعليمية بالدولة.

والله ولي التوفيق ،

المقدمة	

يحتوي هذا الكتاب على معلومات وتمارين مفيدة بشأن إستخدامك للهاتف النقال، والحاسب الآلي وشبكة الإنترنت ولكن بسلامة وأمان. سنتعلم معا كيفية حماية أنفسنا من المخاطر المرتبطة بالهانف النقال وكيف نحمي أنفسنا من الهندسة الإجتماعية وكيف نضبط إعدادات الحاسب الآلي وتفعيل خيارات الأمن والحماية بالجهاز. تم تصميم الكتاب ليكون سهلا وواضحا في شرح مفاهيم الأمن والسلامة المرتبطة بأجهزة الحاسب الآلي والهواتف النقالة لتتحقق أهدافنا بالمتعة والفائدة من التقنية ولكن بأمان.

المخرجات	

بنهاية العام الدراسي سيكون الطالب متمكناً من التالي :

- التعرف على التهديدات المرتبطة بأجهزة الهاتف النقال.
- معرفة كيفية الوقاية من المخاطر المرتبطة بالأجهزة النقالة.
- التعرف على أمثلة حول مخاطر الهواتف الذكية وتطبيقات الهواتف النقالة.
- تعريف مفهوم الهندسة الإجتماعية وطرق ممارستها.
- معرفة كيفية تجنب الوقوع في مصيدة الهندسة الإجتماعية.
- مناقشة الإستخدام المقبول لأجهزة الحاسب الآلي وشبكة الإنترنت.
- تعلم طرق الإعتناء بجهاز الحاسب الآلي.
- معرفة بعض النصائح الأساسية لتفعيل خواص الأمن والحماية بجهاز الحاسب الآلي.

جدول المحتويات

الدرس الأول	أمن الأجهزة النقالة

تعريفات

الهاتف الذكي Smart Phone : هاتف نقال يحتوي على برامج وتطبيقات إضافية إلى جانب الإتصال الصوتي والرسائل النصية القصيرة.

تطبيق الهاتف الذكي Smart Phone Application : برنامج صمم خصيصاً للعمل على الهواتف الذكية

الإستهداف التقني Technical Attack: محاولة غير مشروعة للدخول على أجهزة وأنظمة الحاسب الآلي بالإعتماد على المعرفة بتقنيات الحاسب الآلي والشبكات الإلكترونية

جيلبريك (فك منظومة العمل) Jailbreak: قرصنة الهاتف الذكي من حيث إمكانية الدخول على نظام وبرامج الهاتف النقال بطريقة غير رسمية بهدف إحداث تغيير معين لايتفق مع معايير الجهة المصنعة للجهاز.

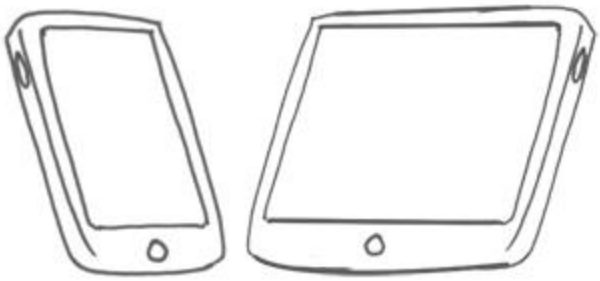
الإحتيال Fraud or Scam: عملية خداع وإخفاء للحقيقة بهدف الحصول على مكاسب معينة.

التصيد Phishing: حين يستخدم المهندس الإجتماعي البريد الإلكتروني بهدف خداع الآخرين لإرسال بيانات شخصية أو معلومات خاصة دون إدراكهم لذلك.

التصيد بالرسائل القصيرة Smishing: حين يستخدم المهندس الإجتماعي الرسائل النصية القصيرة بهدف خداع الآخرين لإرسال بيانات شخصية أو معلومات خاصة دون إدراكهم لذلك

متجر التطبيقات Application Store: موقع إلكتروني أو تطبيق يثبت بأجهزة الهواتف الذكية ويسمح بتنزيل وشراء التطبيقات المختلفة للهاتف المستخدم.

تهديدات الأجهزة النقالة



جاء وفق إحصائية للإتحاد الدولي للإتصالات بأنه يوجد حوالي 6 مليار شخص لديهم هاتف نقال، كما أشارت الإحصائيات بوجود هواتف نقالة أكثر من تلك الهواتف الثابتة في المنازل، بل أن البعض يعتبر الهواتف المنزلية أمر خارج المألوف ولانحتاج إليه اليوم.

نستخدم هواتفنا النقالة بشكل يومي للإتصال وإرسال الرسائل القصيرة للأصدقاء، والدخول على شبكة الإنترنت. أضحت الهواتف النقالة تعرف اليوم "بالهواتف الذكية" حيث توجد بها الكثير من التطبيقات الجديدة غير التقليدية مثل مشاهدة الصوّر والأفلام، وعرض الخرائط والألعاب وغيرها من التطبيقات بحيث أصبحت تلك الهواتف وكأنها أجهزة حاسب آلي صغيرة جدا.

رغم أن إستخدام الهواتف الذكية مهم جدا، إلا أنه من المهم أيضاً أن ننتبه لبعض الأمور حين نستخدم تلك الأجهزة. هناك بعض الأشرار ممن يحاولون سرقة الأجهزة وماقد تحتوي من معلومات، أو خداعنا بغرض الإحتيال وإعطائهم معلومات دون أن نعي ذلك كما هو الحال مع أجهزة الحاسب الآلي الأخرى. لنتذكر، الهواتف الذكية هي أجهزة حاسب آلي صغيرة!!.

هناك نوعان من التهديدات المرتبطة بأجهزة الهاتف. النوع الأول هو تقني، وهو محاولة الدخول على أنظمة تلك الأجهزة من خلال أدوات تقنية مختلفة ومن خلال البرامج المتخصصة كالشفرات الخبيثة، والفيروسات، وبرامج التجسس أو الإستفادة من الثغرات الأمنية في الأنظمة المشغلة لتلك الأجهزة. النوع الثاني من التهديدات هو ذلك المرتبط بالسلوك والتفكير البشري ويعرف أيضا بالهندسة الإجتماعية التي تسمى أحيانا "بإختراق العقل" وهي محاولة شخص ما - يعرف بالمهندس الإجتماعي - إقناعك بإفشاء معلومات خاصة أو سرية دون أن تدرك ذلك ويتم هذا من خلال طرق إحتيالية مختلفة. فمثلاً، من خلال الرسائل النصية القصيرة أو برامج المراسلة الفورية، سيحاول ذلك الشخص الحصول على رد منك بشأن توفير معلومة معينة أو تثبيت برنامج خبيث في جهاز هاتفك النقال.

الإختراق التقني

قد ترتبط البرامج والشفرات الخبيثة بالحاسب الآلي مباشرة ولكننا لاندرك بأنها ترتبط بالهواتف الذكية أيضاً إذ أنها بمثابة أجهزة حاسب آلي صغيرة. أحد أكثر شفرات البرامج الخبيثة للهواتف هي تلك المعروفة "بالتطبيقات المزيفة". التطبيقات المزيفة تشبه تماماً التطبيقات العادية المصممة لأجهزة الهواتف الذكية ولكنها في الحقيقة شفرات خبيثة من شأنها إحداث تهديد أمني في الهاتف الذكي .

في شهر أبريل من عام 2012 ظهرت نسخ لتطبيقات مزيفة من لعبة "الطيور الغاضبة" Angry Birdsوبرنامج تبادل الصوّر الشهير "أنستغرام". عند تثبيت تلك النسخ المزيفة فإنها تعمل في الخفاء ببعض الوظائف الخطرة مثل التجسس وإرسال المعلومات وتدمير البيانات دون أن نشعر بذلك إذ أن ظاهرها يكون شبيها بوظائف التطبيقات الحقيقية.

قد ترى إعلاناً أو صفحة في شبكة الإنترنت تروّج لتطبيق معين للهواتف الذكية وعليه قد تقرر تنزيل ذلك التطبيق وتثبيته بهاتفك. في وقت لاحق وبعد التثبيت، قد يعمل ذلك التطبيق كما هو معلن عنه أو قد لايعمل بتاتاً ولكن في كلا الحالتين قد يكون الأمر مجرد خدعة يقوم من خلالها ذلك التطبيق بعمليات أخرى دون أن تعي ذلك. هناك تهديدات محتملة لمثل تلك الشفرات الخبيثة كإجراء المكالمات الهاتفية الدولية لاسيما تلك المرتبطة برسوم إضافية عند الإتصال دون أن تشعر بذلك، أو إرسال الرسائل النصية القصيرة للغير، أو سرقة بعض المعلومات وأرقام الإتصال والصوّر المخزنة بالجهاز. لاتقم أبداً بتنزيل أية تطبيقات من مواقع غير معتمدة رسمياً من الجهات المصنعة للهواتف الذكية، وأستشر من تثق به في هذا الشأن.

من جانب آخر فإن الهواتف الذكية معرضة لمخاطر الشفرات الخبيثة كتلك التي تأتي عند فتح ملحقات برنامج البريد الإلكتروني المثبته على الهاتف النقال، أو تنزيل النغمات من المواقع. إن شفرات البرامج الخبيثة المخصصة للهواتف الذكية في إزدياد ملحوظ كما جاء في تقرير صدر عام 2011 "لمركز جونبير لمخاطر الهواتف النقالة" والذي أشار لوجود أكثر من 28,000 شفرة لبرامج خبيثة للهواتف النقالة. ورغم أن هذا العدد يعد صغيراً مقارنة بالشفرات الخبيثة لأجهزة الحاسب

الآلي التقليدية إلا أنه دليل على الإهتمام بهذا النوع من الأجهزة، كما أن التقرير أشار إلى زيادة قدرها 155% في مثل تلك الشفرات من عام 2010 إلى عام 2011.

مهما كان نوع الشفرات الخبيثة فإن هدفها هو تعريض الجهاز لتهديدات أمنية مثل محاولة سرقة المعلومات، أو تدميرها أو تعطيل الجهاز كلياً عن العمل، أو أن يقوم الجهاز بإتصالات هاتفية وإرسال رسائل نصية قصيرة باهظة الثمن.

يقوم البعض بمايعرف ب "جيلبريك" أو فك منظومة العمل لهاتفه النقال، وهو نوع من أنواع القرصنة التي تتيح الدخول على نظام الهاتف النقال وبرامجه بطريقة غير رسمية بهدف إحداث تغيير معين لايتفق مع معايير الجهة المصنعة للجهاز. رغم أن هذا الإجراء من شأنه إتاحة الكثير من التطبيقات لتثبت على الهاتف النقال دون الحاجة لشرائها، أو التوسع في بعض المهام أو عدم إنتهاء فترة الصلاحية للتطبيقات المؤقتة أو نسخ العرض قبل الشراء، ولكنه من الجانب الآخر يفتح باباً واسعاً للتهديدات والمخاطر حيث تنفك القيود وتتحطم الحواجز التقنية لاسيما تلك المرتبطة بأمن تلك الأجهزة.

ننصحك بعدم اللجوء لفك منظومة العمل بالهاتف، فإلى جانب التهديدات الأمنية، هناك عواقب سلبية تتعلق بصلاحيات الضمان والدعم التقني من قبل الشركة المصنعة للجهاز، إلى جانب المسائلة القانونية عند تثبيت البرامج غير المرخصة أو تلك التي لم تقم بشرائها.

الهندسة الإجتماعية

تعد الهندسة الإجتماعية ضمن التهديدات المرتبطة بالهواتف النقالة، وتتركز أساساً في عمليات النصب والإحتيال. يحاول الشخص المتخصص بهذا التهديد ويعرف "بالمهندس الإجتماعي" سرقة المال أو المعلومات من خلال كسب ثقة الضحية المستهدفة وإقناعها بتزويده بمعلومات خاصة أو سرية تشكل في مجملها ضرراً بالغاً دون أن تعي تلك الضحية بهذا الأمر، وذلك من خلال طرق وأساليب متعددة تشمل الترغيب مثل الجوائز والهدايا المجانية والربح السريع أو من خلال التخويف كالإيهام بالإرتباط بشخصيات نافذة أو الإستعطاف أو المساعدة والحاجة الملحة ونحوه.

أحد أشهر أساليب الهندسة الإجتماعية عبر الهاتف النقال يكون عبر"التصيد" بواسطة الرسائل النصية القصيرة، وهي تلك الرسائل التي تصل وفيها دعوة للحصول على شيء مجاني، أو دعوة لزيارة موقع معيّن بشبكة الإنترنت، أو تنزيل تطبيق ما أو نغمة معينّة. في حقيقة الأمر، إن ذلك يعد جزء من التصيد وقد يؤدي إلى تثبيت شفرات وبرامج خبيثة في جهاز الهاتف من شأنها إحداث الأضرار البالغة مثل الإتصال بأرقام خارجية، أو إرسال الرسائل النصية القصيرة بشكل تلقائي بهدف دفع الرسوم والمبالغ المالية ذات الكلفة العالية أو سرقة الملفات والصوّر المخزنة على الجهاز.

لقد وجدت دراسة قامت بها شركة أمنية متخصصة تسمى (تراستير) بأن الأشخاص لديهم الدافع لفتح روابط الرسائل الإلكترونية في الهواتف النقالة أكثر ب 3 مرات من فتحها في أجهزة الحاسب الآلي العادية.

هناك العديد من الطرق التي سيقوم بها المهندس الإجتماعي لإقناع الشخص المستهدف لإتباع التعليمات حتى يقع في فخ للتصيد عبر الرسائل النصية القصيرة. أحد أشهر تلك الطرق حالياً مايعرف ب"حيلة الإتصال العكسي للخدمات غير المجانية". تكمن الحيلة في إستلام رسالة نصية قصيرة تدعوك للإتصال برقم أو إرسال رسالة نصية قصيرة بهدف الحصول على جائزة أو الإشتراك بمسابقة تبدو إجابتها سهلة جداً أو تنزيل نغمة للهاتف النقال. يبدو الأمر عادياً ومريحاً ولكن مالاتعلمه الضحية المستهدفة بأن الإتصال بذلك الرقم أو إرسال الرسالة لذلك الرقم لن يكون مجانياً أو حتى بسعر الإتصال العادي، وإنما وفق تسعيرة خاصة أغلى بكثير من السعر العادي

للمكالمة أو الرسالة القصيرة، وعليه سيحقق المحتال الربح الكثير من خلال مشاركات الضحايا ولن يحصل الضحايا على أية جوائز أو هدايا.

طريقة أخرى تكمن في الإستهداف من خلال "حيلة التسجيل" بحيث يدعوك إعلان معينّ للإستفادة من أسعار تفضيلية للمكالمات أو تنزيل نغمات جديدة للهاتف النقال بشكل مستمر وذلك بالتسجيل في خدمة مجانية لمدة شهر واحد على أن تدفع قيمة الإشتراك إن رغبت في الإستمرار بعد الفترة المجانية ولكن يتوجب عليك أولاً ملأ المعلومات اللازمة بشأن تفاصيل الحساب البنكي والمعلومات الشخصية الأخرى لإستكمال إجراءات التسجيل. بعد الفترة المجانية ستجد الضحية صعوبات كثيرة في إلغاء الخدمة أو ربما لن تحصل على الخدمة أساساً وستستمر عملية الخصم الشهري من الحساب البنكي مما يتوجب القيام بإجراءات صعبة بهدف وقف الخدمة أو تغيير البطاقة البنكية وقد يكون قد مضى بعض الوقت واستفادت جهة الإحتيال من المبالغ المستقطعة من الحساب البنكي للضحية قبل وقف الخدمة.

الرسائل مجهولة المصدر وعمليات الإبتزاز

يعد هذا النوع من التهديدات الأمنية الأكثر إزعاجاً وتخويفاً عبر استلام مكالمات أو رسائل نصية قصيرة ذات طابع عدائي بحيث يخبرك المهندس الإجتماعي مثلاً بأن هاتفك النقال مخترق من قبله أو أنه قد إطلع على مافيه من معلومات أو صوّر، وسيقوم بنشرها مالم تنفذ جملة مطالب يحددها المهندس الإجتماعي. تأتي تلك المكالمات أو الرسائل من أرقام غير معروفة أو غير حقيقية لتعقيد أجراءات تتبعها، كما تحدد الإجراءات المطلوبة لتحويل المال بهدف الإبتزاز.

يرسل المهندس الإجتماعي رسائل الإبتزاز تلك لعدد كبير من الناس بغية أن يستجيب ولو عدد محدود منهم للطلب، رغم أنه لايملك أية معلومات أو صوّر أو إختراق حقيقي لهاتفك النقال ولكن من الطبيعي أن يخاف بعض الناس ويشعروا بالإنزعاج وقد يبادروا في تحقيق مطالب المبتز.

كيف نحمي أنفسنا؟

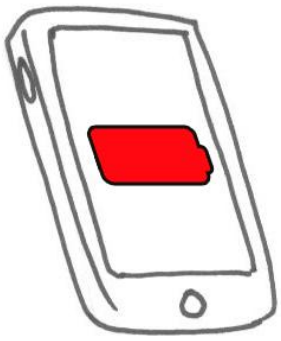
تجنب التطبيقات المزيفة

الإجراء الأهم هو تنزيل التطبيقات من المواقع الرسمية أو المعتمدة فقط. تقوم الجهات المشرفة على المواقع الرسمية لتطبيقات الهواتف الذكية بعملية إختبار وتحقق للتطبيقات قبل إتاحتها للتنزيل من قبل المستخدمين. من جانب آخر، يحسن بك قبل تنزيل أي تطبيق; الإطلاع على ملاحظات الآخرين حول هذا التطبيق، وتجدها عادة ضمن المعلومات المتاحة قبل عملية تنزيل التطبيق من الموقع. إن العديد من التطبيقات قد تكون مصممة بطريقة سيئة ومن شأن ذلك إستهلاك موارد الجهاز أو تعطيله، وقد لاتجد الدعم الفني المناسب وعليه يتوجب الحذر قبل تنزيل وتثبيت أي تطبيق في هاتفك الذكي.

هناك العشرات من مواقع تنزيل التطبيقات غير الرسمية وتوفر الكثير من التطبيقات المجانية ولكن يجب عليك توخي الحذر الشديد حيث تكثر فيها التطبيقات المزيفة.

كيف يمكنني التحقق من تثبيت تطبيق مزيف بهاتفي؟

فيما يلي بعض الملاحظات المفيدة ولكنها لاتغني عن الملاحظة الأهم وهي الحذر وتنزيل الملفات من المواقع المعتمدة فقط.



- ستلاحظ بأن بطارية الهاتف الذكي تستهلك أسرع من المعتاد مما يدل بأنه يوجد هناك تطبيق ما يقوم بوظائف غير ظاهرة لنا.
- فاتورة الهاتف قد تشمل أرقام إتصال أو رسائل نصية قصيرة لجهات غير مجانية وبأسعار غير تقليدية رغم أنك لم تقم بالإتصال أو إرسال رسائل نصية لتلك الجهات مما يدل على وجود تطبيق مزيف يقوم بذلك بصورة تلقائية دون أن تدرك ذلك.

إذا شعرت بوجود تطبيق مزيف على جهازك، ينصح بالقيام بعملية إلغاء لكل التطبيقات المثبتة مؤخراً ومن بعدها مراقبة أداء الهاتف، فإن استمرت المشكلة فيتوجب عليك الإتصال بشركة الإتصالات أو فني الصيانة المعتمد ولاتنسى أن تنسق ذلك مع والديك أولاً.

لاترد على الرسائل النصية القصيرة من الغرباء

إذا استلمت رسالة نصية قصيرة بشأن فوزك بجائزة أو عرض مجاني أو طلب إرسال بيانات شخصية أو معلومات خاصة فإنه يتوجب عليك تجاهلها وحذفها. تلك الرسائل ضمن الطرق الأكثر شيوعاً من قبل المحتالين خصوصاً تلك التي تحتوي على روابط من شأنها تثبيت برامج خبيثة بهاتفك النقال والتي من الممكن أن تقوم لاحقاً بعملية إتصال أو إرسال رسائل نصية قصيرة لأرقام وخدمات ذات أسعار مرتفعة. من المهم جداً ألا ترسل أية بيانات شخصية عبر الرسائل النصية القصيرة فلا يوجد هناك أي بنك أو شركة إتصالات أو متجر في شبكة الإنترنت يطلب مثل تلك المعلومات عبر هذه الرسائل.

لاتضغط على روابط المواقع أو تنزيل الملفات الملحقة بالرسائل القصيرة

إذا استلمت رسالة نصية قصيرة فيها إعلاناً لتطبيقات مجانية أو نغمات وتحتوي على رابط لموقع بشبكة الإنترنت، أو ملفاً ملحقاً لتنزيل تلك التطبيقات، فإنه يتوجب حذف تلك الرسالة حالاً وعدم الرد، هناك احتمالً كبير أن تكون تلك الرسالة مصيدة لبرامج خبيثة.

إنتشرت مؤخراً الرسائل النصية القصيرة والرسالة الإلكترونية التي تحتوي على عناوين إلكترونية مختصرة لمواقع شبكة الإنترنت مما قد يتسبب في بعض التشتت والقلق بشأن العنوان الحقيقي. فمثلاً، عنوان "http://wwww.aecert.com/partnership-ar.php" سيبدو "http://bit.ly/OmPYGs" . العنوان المختصر قد يكون رابط لموقع مشبوه أو موقع حقيقي وعليه فإننا ننصحك بتجنب فتح العناوين المختصرة لاسيما تلك التي تأتي ضمن رسائل مجهولة المصدر أو رسائل التسويق والإعلان، كما ننصحك بإستخدام العنوان الحقيقي دائماً عند كتابة العناوين في برنامج متصفح الإنترنت.

أخبر ولي أمرك في الحال حين تستلم رسالة نصية قصيرة أو مراسلة فورية ذات محتوى مزعج أو مريب

إذا مررت بتجربة إستلام رسالة نصية قصيرة ذات محتوى مزعج أو مريب أو غير أخلاقي أو تعدي إلكتروني، فإنه يتوجب عليك إخبار والديك بالأمر حالاً دون تردد. سيكون لدى والديك الحكمة والقرار الصائب بشأن التصرف السليم في هذا الموضوع الهام.

تهديدات الهواتف النقالة

إستعرضنا التهديدات والمخاطر المرتبطة بالهواتف النقالة والطرق التي يتبعها المهندس الإجتماعي في عمليات النصب والإحتيال بواسطة تلك الأجهزة. في هذا النشاط سنتعرف لماذا يقع الناس في مصيدة الهندسة الإجتماعية:

القسم الأول:

- أذكر خدمة أو ميزة غير موجودة في الهاتف الذكي وترغب في وجودها؟
- هل أنت على إستعداد لدفع المال مقابل الحصول على هذه الخدمة أو الميزة؟
- ماذا سيكون ردك لو عرض عليك أحدهم القيام بما تتمناه مجاناً دون مقابل؟ هل ستقبل ذلك العرض؟ إشرح سبب قبولك أو رفضك؟

القسم الثاني:

- أذكر موقعاً إلكترونياً واحداً تزوره بإستمرار وتعده مهما جداً لك؟
- لماذا يعد ذلك الموقع مهما لك؟ هل توجد أشياء مهمة بالنسبة لك بذلك الموقع؟
- لو إستلمت رسالة تخبرك بأن حسابك في ذلك الموقع قيد التوقيف ولايمكنك الدخول عليه مجدداً إلا إذا قمت بدفع المال لشخص معين، هل ستقوم بذلك؟ إشرح سبب قبولك أو رفضك؟

القسم الثالث:

- برأيك، لماذا تجد صعوبة في إتخاذ القرارات بشأن الأمور السابقة؟ هل من طرق لتجعل إتخاذ القرار أكثر وضوحاً وتركيزا؟
- هل كل التطبيقات المجانية تعني بالضرورة تلغيمها بالشفرات والبرامج الخبيثة؟ أين تجد البرامج المجانية المأمونة؟

تطبيقات تحديد المواقع

تقوم هذه التطبيقات برصد موقع الهاتف الذكي أو الشخص الذي يحمل الهاتف الذكي، وكذلك وقت وتاريخ تواجد ذلك الشخص! قد يكون الأمر غريباً ومثيراً أيضاً، ولكن كيف يكون ذلك؟ هناك طريقتان أساسيتان بهذا الخصوص:

الطريقة الأولى: من خلال خاصية "تبليغ الآخرين" بشأن موقعك وتتواجد الخاصية في بعض شبكات التواصل الإجتماعي مثل "فيس بوك أو فورسكوير". هذه الخاصية ستتيح للآخرين رصد موقعك بمجرد الضغط على رابط الإبلاغ الموجودة بالموقع.

الطريقة الثانية: من خلال "خدمات المواقع" الموجودة ضمن خيارات الضبط في الهواتف الذكية. معظم الهواتف الذكية فيها مثل هذه الخدمات. يجب أن تكون الخدمة في حالة "التعطيل" وعدم تفعيلها إلا عند وجود ضرورة لها. تقوم هذه الخدمات بجمع معلومات لبعض التطبيقات حول الموقع والأشخاص، كما تسمح بعض التطبيقات برصد الأشخاص المتواجدين في موقع معين ضمن خدمات الترفيه والخدمات الإجتماعية لشبكات التواصل.

لماذا تعد هذه الخدمة مشكلة؟

إليك بعض الأمور المهمة عند إختيار أو تفعيل خدمات رصد المواقع:

1. بتفعيل هذه الخدمة فإنك تعلن لكثير من الناس عن مكان تواجدك، وربما يشمل ذلك أشخاص لا ترغب أن تخبرهم بذلك.
2. تفعيل هذه الخدمة بينما انت مسافر يعني ببساطة أن المنزل قد يكون خالياً. أحدهم كان مسافراً ومفعلاً لهذه الخدمة وحين عاد اكتشف أن بيته قد تعرض للسرقة. حين علم اللصوص بعدم تواجد صاحب المنزل باشروا في عمليات السرقة.
3. هناك مخاطر عند تفعيل هذه الخدمة في الهواتف التي يحملها الأطفال أو الطاعنين في السن أو ذوي الإحتياجات الخاصة، إذ يمكن من خلال هذه الخدمة التعرض لهم وتعقبهم لأهداف غير مشروعة.
4. رصد موقعك دون سبب وجيه قد يعرضك لمخاطر أمنية، أو يسبب لك الحرج لتواجدك في مكان معيّن. قد يستغل أحدهم تواجدك ويقوم بالتواصل معك دون معرفة هوية الشخص الحقيقية والتي قد تستغل لاحقاً لغرض مشبوه كالإبتزاز أو التشهير.

الحماية من تطبيقات تحديد المواقع

تعطيل خدمات تحديد المواقع هو الخيار الأسلم لك. بالطبع، لن تتعطل خدمات الإتصال بالهاتف ولكن لن تتمكن تلك التطبيقات من تحديد موقعك عند تعطيل هذه الخاصية.

بعض المواقع الإلكترونية وبعض التطبيقات تنبهك عندما يتم رصدك من قبل شخص ما من خلال خدمات تحديد المواقع بهاتفك أو إستخدام أحد التطبيقات المثبتة بجهازك لهذه الخاصية. في كلا الحالات ينبغي الحذر. قد يشجعك البعض لتفعيل هذه الخاصية بهدف الترفيه والتواصل الإجتماعي، ولكن الصواب أن نذكّر الآخرين بالمخاطر المتوقعة بكل صدق ووضوح.

تهديدات تطبيقات تحديد المواقع

من المهم فهم أسباب تحديد الخيارات. قد تكون تطبيقات تحديد المواقع ضمن الخيارات الشخصية، ولكن يتوجب التفكير بالمخاطر قبل تحديد الخيار المناسب لنا. ناقش في الفصل خياراتك بهذا الخصوص.

1. هل تستخدم تطبيقات تحديد المواقع ؟ إشرح إجابتك؟

2. هل تمانع لو تم رصدك أو رصد عائلتك من خلال تطبيقات تحديد المواقع لاسيما إن شمل ذلك صورا لك أو لعائلتك؟ إشرح إجابتك؟

3. ماهي الحالات التي تتوقع أن ينزعج فيها الناس عند رصدهم من خلال خدمات تحديد المواقع ؟

أمن التطبيقات في الهواتف النقالة

لم تعد الهواتف النقالة وسيلة للإتصال الصوتي أو إرسال الرسائل النصية القصيرة فحسب، بل أجهزة ذكية متطورة فيها الكثير من التطبيقات المختلفة. من خلال هواتفنا اليوم، نستطيع إرسال الرسائل الإلكترونية عبر تطبيقات البريد الإلكتروني، ونتصفح المواقع بشبكة الإنترنت، ونشاهد الأفلام، ونلعب ونتواصل عبر الشبكات الإجتماعية ونقرأ الكتب، وغيرها من التطبيقات الأخرى. أضحت هذه الهواتف أدلة إلكترونية بين أيدينا فلا نحتاج للخرائط للوصول إلى العناوين والمكتبات والمطاعم! كل تلك التطبيقات جزء لايتجزأ من تطبيقات الهواتف الذكية اليوم.

من المهم أن تعمل تلك الهواتف بشكل آمن وسليم لتجنب مخاطر عدة من شأنها إلحاق الأذى بنا إن لم ننتبه لها.

لاتحاول فك منظومة العمل (جيلبريك) الهاتف الذكي. إن لهذه العملية مخاطر أمنية وتقنية قد تؤدي إلى تعطل الجهاز كلياً، إلى جانب زيادة المخاطر المرتبطة بتلك الأجهزة، كما أن هذا التصرف قد يعني إنهاء الدعم الفني من قبل الشركة المصنعة و شركة الإتصالات. إن هذه العملية تعد نمط من أنماط القرصنة وتؤدي إلى إزالة الحواجز التقنية التي وضعت من قبل الشركة المصنعة لتحمي الجهاز من التهديدات.

من أين تنزل وتشتري التطبيقات؟ الجهات المصنعة للهواتف الذكية تدير بشكل عام متاجر إلكترونية لتنزيل التطبيقات المجانية وغير المجانية. التطبيقات المتاحة عبر تلك المتاجر تخضع للفحص والتدقيق قبل إتاحتها للجمهور مما يزيد من سلامتها وخلوها من البرامج والشفرات الخبيثة. أما تنزيل التطبيقات وشرائها من مواقع أخرى فإنه يتوجب منك الحذر الشديد، فقد تكون بعض التطبيقات متاحة بأسعار أرخص من مثيلاتها في المواقع الرسمية، ولكنها في حقيقة الأمر مصيدة. ننصحك بإستشارة من تثق به في هذا الشأن.

خذ المزيد من الحذر. حتى وإن قمت بتنزيل أو شراء تطبيقاً من موقع معتمد، فإنه من الأفضل أخذ المزيد من الحذر والتأكد بان التطبيق آمن. بالإضافه اللى ذلك، يمكنك مراجعة التعليقات والملاحظات التي يكتبها الآخرون في متجر التطبيقات قبل تنزيل التطبيق المطلوب. عادة ماتكون التعليقات مفيدة جداً، وإن كانت قليلة أو غير موجودة فيستحسن بك البحث عن تطبيق آخر، له نفس الوظائف والمهام إن وجد. من جانب آخر، فإنه من المفيد التحقق من الجهة المطورة للتطبيق والتعرف على التطبيقات الأخرى التي قامت بتطويرها إن وُجدت. قد يكون الإجراء طويلاً بعض الشيء ولكنه مفيد جداً وقد يجنبك الكثير من المتاعب مستقبلاً.

إنتبه للصلاحيات المطلوبة من قبل التطبيق. فكّر جيداً قبل الموافقة على أية صلاحيات يطلبها التطبيق عند تثبيته بالجهاز أو بدء إستخدامه. إن العديد من التطبيقات المرتبطة بشبكات التواصل الإجتماعي تطلب الدخول على قائمة العناوين أو الأصدقاء بل أن بعضها يطلب إتاحة المشاركة في كل الصوّر والملفات الموجودة بهدف التبادل والتواصل الإجتماعي. تجنب الموافقة على تلك الصلاحيات إن بدت كثيرة وغريبة وإستشر من تثق به في هذا الشأن.

من جانب آخر، يجب عليك اتخاذ الحذر على وجه الخصوص بالنسبة للخدمات المصرفية عبر الهاتف. حين تستخدم الخدمات المصرفية الإلكترونية ينبغي عليك إستخدام التطبيق الرسمي للبنك فقط لاسيما بأن تلك الخدمات لها طابع أمني خاص من حيث الإطلاع على الحسابات البنكية والتحويلات المالية.

المراجعة المطلوبة.. يجب مراجعة فواتير خدمات الاتصالات بشكل منتظم والتأكد من عدم وجود مبالغ إضافية غير طبيعية أو مبالغ لخدمات غير مستخدمة. كما أشرنا سابقاً فإن بعض التطبيقات تعمل في الخفاء وتقوم بالإتصالات وإرسال رسائل باهظة الثمن دون أن ندرك ذلك.

الدرس الثاني	الهندسة الإجتماعية

تعريفات

البيانات الشخصية Personal Information: هي تلك البيانات التي قد تستخدم للتعريف بشخص ما، وهي بيانات من شأنها التحقق والتأكد من تلك الشخصية مثل الإسم، والرقم الشخصي، وصفات مظهر الشخص، البيانات الطبية وبيانات تاريخ الميلاد.

المعلومات الخاصة Private Information: أية معلومات لايرغب بعض الناس إشاعتها ونشرها للآخرين. تلك المعلومات قد تشمل الأسرار، والأفكار، الأمور الخاصة وأية معلومات يراها الشخص خاصة وغير قابلة للنشر.

الهندسة الإجتماعية

سبق وإن استعرضنا الهندسة الإجتماعية عبر أجهزة الهاتف. سيحاول المهندس الإجتماعي إستخدام كل الأدوات والطرق المتاحة للحصول على المعلومات، لايهم إن كان ذلك عبر الرسائل النصية القصيرة، أو عبر المكالمات الهاتفية، أو عبر اللقاء المباشر وجهاً لوجه.

ماهي الهندسة الإجتماعية

الهندسة الإجتماعية هي محاولة الحصول على المعلومات الشخصية والخاصة من الطرف الآخر عبر وسائل مختلفة دون أن يشعر الطرف الآخر بأنه مستهدف فيفصح عن العديد من المعلومات. هذه المعلومات بمجموعها قد تشكل خطورة أمنية أو وسيلة لتهديد الشخص أو أسرته أو بيئة عمله. لايستخدم المهندس الإجتماعي أدوات تقنية بحتة لتحقيق هدفه مثل البرامج الخبيثة كالفيروسات مثلاً، ولكن إعتماداً على تقنيات مرتبطة بالسلوك لذا تعرف أحيانا ب"إختراق العقل"

.

يحاول المهندس الإجتماعي طرق مختلفة مثل التظاهر بالود والنبل، أو التظاهر بالنفوذ والقوة، أو إظهار الحاجة والضعف للإستعطاف. كل تلك الطرق قد تجعلك تخرق القوانين في سبيل المساعدة أو توقع مكاسب مالية في المستقبل.

للمهندس الإجتماعي أهداف مختلفة، قد يكون الهدف تحقيق بعض المال عبر أخذ المعلومات منك وإستغلالها لاحقاً للإبتزاز أو السرقة، أو نشر المعلومات لهدف مشبوه أو ضار كالتشهير مثلاً، أو قد يكون الهدف أعمق من ذلك كله كالتجسس والإضرار بمصالح الدولة! للأسف، فإن الهندسة الإجتماعية غير واضحة ويصعب تعقبها من قبل عموم الناس إلا إذا كان الشخص المستهدف محصناً من خلال زيادة ثقافته تجاه أمن المعلومات. سيحاول المهندس الإجتماعي طرق متعددة ومختلفة لتحقيق الهدف وقد يستغرق ذلك وقتاً في سبيل الحصول على المعلومات المطلوبة.

مامدى نجاح الهندسة الإجتماعية؟ أثبتت التجارب السابقة بأنه من خلال الهندسة الإجتماعية تمكن الأشرار من سرقة البنوك، والدخول على أنظمة الحاسب الآلي، بل تمكنوا من أنتحال الشخصيات واقناع موظفي البنوك بإعطائهم الأموال، والدخول على المواقع المحظورة، بل والسفر مجاناً!. تعد الهندسة الإجتماعية من أكثر الطرق جرأة وتعقيداً من خلال إستغلال الطبيعة السمحة للناس وتصرفهم الفطري نحو التعاون والتعارف والثقة.

ماهو شكل المهندس الإجتماعي؟ قد تظن خطأً بأن المهندس الإجتماعي تبدو عليه ملامح الشر والمكر والخداع، ولكنه في حقيقة الأمر عكس ذلك تماماً. المهندس الإجتماعي سيبدو كأي إنسان، لاتختلف ملامحه عنك أو عن أي شخص بالمجتمع، وهنا تكمن الخطورة فهو في الظاهر إنسان عادي بينما يبطن المكر والشر دون أن تدرك ذلك.

في المجمل، لايجب أن نعتقد بأن كل الناس أشرار ويتوجب تجنبهم! الأصل في العلاقات البشرية أن تكون صادقة ومحترمة ولكن بعضها قد يشوبه السوء، ومن هذا المنطلق فإن الحل يكمن في أن نؤسس علاقات إجتماعية إيجابية مع الناس ولكن بحذر وإنتباه. في الفقرات التالية سنتعرف على بعض طرق وأدوات الهندسة الإجتماعية. بمعرفتها سنكون أكثر تحصيناً ووعياً بشأنها.

طرق وأساليب الهندسة الإجتماعية

هناك طرق وأدوات عدة تستخدم في الهندسة الإجتماعية وكلها تهدف لإقناع الضحية المستهدفة بالإفصاح عن المعلومات السرية والخاصة دون أن يدرك أو يعي عواقب ذلك. رغم التحذيرات المتكررة بشأن مخاطر الهندسة الإجتماعية، يقع بعض الناس في شباكها، وقد تنتبه الشخصية المستهدفة لذلك ولكن بعد فوات الأوان ومرور وقت كاف لكي يفلت المهندس الإجتماعي، بل أحيانا قد تتفاقم الأمور وتقع المسائلة القانونية بشكل مباشر على الضحية المستهدفة، بينما يختفي أثر المهندس الإجتماعي أو أثر الممارسة وكأن الأمر قد تم بأمر وإقرار من الضحية. لنتعرف على بعض الطرق والأدوات:

عرض الهدية والمكافأة: ظاهرياً، فإن تلك الهدية أو المكافأة ستكون من مؤسسة، أو شخصية غنية، أو عبر سحوبات وعروض، أو شركة ترغب في شريك لحفظ أموالها. ستكون مغرية للقبول بها لاسيما بأنها لاتسبب أي ضرر (هذا ما تعتقده الضحية). فمثلاً، قد تستلم رسالة إلكترونية تطلب المساعدة لتحويل مبلغ مالي بسبب ظروف عسيرة مختلفة على أن تكون لك مكافأة نظير عملية التحويل تلك والخدمة الجليلة التي أسديتها!، ولكن لتحقيق ذلك فإنه يلزم بعض المعلومات كرقم الحساب بالبنك وبياناتك الشخصية ومعلومات أخرى حتى تتم عملية تحويل المال، كما تطلب رسوم رمزية جداً لاتقارن بمبلغ المكافأة المتوقعة وذلك لأغراض التأكيد والجدية من قبل الضحية وبعض الرسوم الإدارية. بعد تحويل المال أملاً في المكافأة، لن تسمع الضحية مجدداً أي شيء من المهندس الإجتماعي.

الطلب المستعجل: قد تستلم رسالة إلكترونية أو حتى إتصالاً هاتفياً من شخص يطلب منك أداء خدمة معينة بسرعة وعجالة لأهمية الأمر. فمثلاً، سيطلب منك في رسالته أو إتصاله تزويده ببعض المعلومات الخاصة مدعياً أنه موظف في البنك وأن هناك محاولة أختراق (وهمية طبعاً دون أن تدرك ذلك) ويقوم البنك حالياً بالتأكد من حسابات الزبائن، أو يطلب منك كلمة المرور الحالية وإختيار كلمة مرور جديدة لإيهامك بأنهم في صدد إعادة تهيئة النظام المعطل بسبب محاولة الإختراق، كما سيلح المتصل بضرورة سرعة الإستجابة حتى لا تخسر أموالك أو تتعرض للسرقة، بينما في حقيقة الأمر هذه هي محاولة السرقة الحقيقية.

مثال آخر، يكون من خلال إستلامك لرسالة نصية قصيرة أو رسالة إلكترونية أو إتصالاً من شخص يعرض عليك فرصة الفوز الأخيرة في مسابقة أو جائزة ما ولن يتبقى الوقت الكثير بينما قيمة الجائزة كبيرة جداً! كما سيطلب منك إرسال معلومات بطاقة الإئتمان للدخول في السحب أو تحويل مبلغ مالي أو إرسال رسالة نصية قصيرة ببياناتك الشخصية أو رسالة نصية قصيرة ولكن بسعر مرتفع بهدف الإشتراك. كل تلك المحاولات أمثلة من الإحتيال عبر الهندسة الإجتماعية.

التخويف والتهديد: قد تستلم رسالة تبدو وكأنها مرسلة من المدير أو أتصالاً يدعي بأنه مسئول ما أو موظف في الأمن ويطلب منك معلومات مهمة ويقوم بتخويفك وتهديدك إن رفضت الطلب. قد يتكرر الأمر نفسه وجهاً لوجه وعليه يجب أن تكون حذراً وتتصرف بهدوء وحنكة. عند تعرضك لهذه المواقف يتوجب عليك عدم الفزع والإتصال بوالديك حالاً.

إثارة الفضول: سيحاول المهندس الإجتماعي إثارة فضول الضحية من خلال تقديم عرض ما، كأن يرسل له ملفاً معنوّناً ب"أجمل أهداف كأس العالم" أو لعبة بعنوان "إختبر قوتك في تسلق برج خليفة!" أو رابط لموقع يحتوي على صوّر شيقة. كل تلك العناوين المثيرة قد تقود الضحية لفتح الملف أو تشغيل اللعبة أو تصفح الموقع المطلوب بينما هي في الحقيقة روابط وبرامج لشفرات خبيثة من شأنها تثبيت برامج التجسس والفيروسات بالحاسب الآلي.

عرض الصداقة والمساعدة: سيحاول المهندس الإجتماعي عرض الصداقة أو المساعدة وإدعاء النُبل. يتعارف الناس كثيراً في غرف الدردشة ومواقع التواصل الإجتماعي وقد يكون من بين أولئك الناس الكثر بعض الأشرار والمحتالين. سيحاول المحتال من خلال الحديث والدردشة معرفة أكبر كم من المعلومات عن الشخص المستهدف، وسيحاول إثارة الإهتمام من خلال الحديث عن نفس هوايات وإهتمامات الطرف الآخر بهدف كسب الثقة. في حالات عدة قد يعرض المحتال خدمة المساعدة كأن يطلب منك إسم الحساب وكلمة المرور لمساعدتك في تخطي المراحل بألعاب مواقع التواصل الإجتماعي، أو مساعدتك في شراء بعض الأمور من الشبكة على أن تعطيه بعض المعلومات مثل تفاصيل بطاقات الإئتمان، وعنوان الإستلام بل أن الأمر قد يكون خطيراً جداً كمحاولات الإستدراج واللقاء وجها لوجه، ومن أمثلة ذلك تبادل أقراص الألعاب الإلكترونية حيث يكتشف الضحية بأن الطرف الآخر شخصاً بالغاً يدعي بأنه طالب صغير لأغراض غير أخلاقية على سبيل المثال، وعليه يتوجب الحذر الشديد بهذا الشأن.

تشتيت الذهن أو الإستغفال: من الأساليب أيضاً أن يحاول المهندس الإجتماعي تشتيت الذهن من خلال طرح أسئلة متعددة غير مترابطة أو مناقشة مواضيع بشكل غير مركز. قد تبدو الأسئلة في ظاهر الأمر غير مهمة ولكنها في حقيقة الأمر وسيلة لجمع المعلومات، كما يستخدم المهندس الإجتماعي تعابير ومصطلحات ربما تكون غير مفهومة وغير صريحة مما يثير فضول الطرف المستهدف محاولاً الإستيضاح بطلب المزيد من المعلومات، أو طرح أسئلة قد تبدو سطحية جداً وتشجع الضحية على الرد وسرد المعلومات.

من جانب آخر قد يحاول المهندس الإجتماعي توجيه تركيز الضحية لموضوع معين وصرف إنتباهه عن مواضيع أخرى بهدف تحصيل المزيد من المعلومات بينما يعدها الضحية مواضيع هامشية ولا يعر إهتماماً لمايقول.

هذه بعض الطرق التي تستخدم في الهندسة الإجتماعية. قد تكون مجتمعة معاً أو بشكل منفرد، المهم أن تحقق الهدف في استخلاص المعلومات من الضحية دون أن تدرك ذلك سواء كان ذلك في موقف واحد أو مواقف متعددة وفي أوقات مختلفة.

تجنب الهندسة الإجتماعية

الوسيلة الأفضل لتجنب الهندسة الإجتماعية تكمن في زيادة الوعي بمفاهيم أمن وسلامة تقنية المعلومات، والوعي بطرق وأساليب ممارسة الهندسة الإجتماعية. يتوجب علينا الحذر والتفكير بعناية وتقييم الأمور قبل إتخاذ أي قرار. فمثلاً، هل محتوى الرسالة الإلكترونية ليس واقعياً؟ كأن تكون هدية قيمة جداً لمجرد الرد! أو الحصول على الأموال مقابل بعض البيانات الشخصية فقط! هل ُطلب مني القيام بتصرف ما من شأنه أن يسبب الضرر؟ لاسيما بأنه يمكن تحقيق المطلوب دون مساعدة مني، كأن يُطلب مني فتح حساب بنكي بإسمي لتحويل المال! لماذا يمكن لشخص غريب أن يثق بشخص لايعرفه أبداً، كأن يخصني شخص ما بطلب دون سابق معرفة بيننا ولم يلتقي بي قط ثم يخبرني بأنه سيرسل لي هدية أو أموالاً طائلة!.

لايجب أبداً إخبار الغرباء بأية بيانات شخصية أو معلومات خاصة أو ذات طبيعة سرية حتى ولوبشكل جزئي. يعرف المهندس الإجتماعي كيفية ربط المعلومات المستخلصة وفي أوقات متعددة بعضها ببعض للحصول على معلومة متكاملة. لوطلب منك شخص ما كلمة المرور، أو رقم بطاقة الإئتمان، أو رقم حسابك بالبنك، أو رمز التعريف الشخصي لبطاقة الصراف الآلي سواء بالبريد الإلكتروني، أو من خلال غرف الدردشة أو برامج المراسلة الفورية أو عبر شبكات التواصل الإجتماعي أو أية وسيلة أخرى دون سبب وجيه ومقنع فلا تستجب للطلب ابداً وأبلغ ولي أمرك بالأمر حالاً.

كن يقظاً وحذراً بالنسبة لأية طلبات مهما كانت مغرية إذا كانت مخالفة للقواعد والقوانين حتى وإن كان سبب الإستجابة لهدف نبيل أو مساعدة، فالنتائج قد تكون خطيرة وتتضمن المسائلة القانونية. إسأل نفسك دائماً، هل هذا العمل مخالف وينبغي ألا أقوم به؟ إذا كان الجواب نعم فإمتنع مباشرة عن أداء ذلك العمل.

إذا إستلمت رسالة معنونة ب (عاجل) بشأن حسابك البنكي أو بريدك الإلكتروني وتحتوي على رابط للضغط عليه لتتم إنجاز المطلوب فلا تستجب للطلب، وإن إحتوت الرسالة على رقم هاتف أو بريد إلكتروني للإتصال فلا تثق بتلك المعلومات وحاول الحصول عليها من الموقع الرسمي للبنك أو الشركة المرسلة ثم تأكد من الرسالة بالإتصال بتلك الجهة ومخاطبة قسم الدعم الفني المعتمد رسمياً.

تستطيع أحياناً معرفة الرسائل الإلكترونية الوهمية من خلال بعض المعطيات، فمثلاً، قد تستلم رسالة تبدو وكأنها مرسلة من جهة رسمية بينما عنوان "المرسل" مختلف ولايدل على الجهة المرسلة أو يكون عنواناً ضمن الخدمات البريدية المجانية مثل (هوت ميل - جي ميل - ياهو ميل). أو أن يكون محتوى الرسالة الإلكترونية مليء بالأخطاء الإملائية واللغوية مما يدل على وجود شبهة ما بالرسالة.

لايجب أن نرسل أية معلومات خاصة أوسرية عبر البريد الإلكتروني أو من خلال الرسائل القصيرة كما يجب أن تلتزم الحذر الشديد عند نشر المعلومات في شبكات التواصل الإجتماعي فكل تلك الوسائل لاتعد آمنة حين نتحدث عن المعلومات الخاصة والحساسة.

كيف نتصرف حين تسوء الأمور؟

ماهو التصرف السليم حين يتمكن المهندس الإجتماعي من إختراق عقولنا والحصول على معلومة ما؟

عند وقوع مشكلة ما مرتبطة بالهندسة الإجتماعية فيجب أن تطلب المساعدة من الشخص المناسب، وهما بلا شك الوالدين فهم اقدر منك على معالجة الأمور وأكثر خبرة بالتصرف والإتصال بالجهات التي تساعدك في حل المشكلة. تذكر، إخبار والديك بالأمر مهم جداً، فقد تكون الأمور أسوء مما تعتقد.

يتوجب عليك أيضاً القيام ببعض الخطوات الهامة مثل حفظ وكتابة وقت التعرض للحادثة، ونوع المعلومات التي طُلبت، وموقع الحادثة وأسلوبها.

أمثلة على الهندسة الإجتماعية

استُخدمت أساليب الهندسة الإجتماعية منذ القدم، ذلك بأن أساليب أقناع الناس لعمل شيء أو الإفصاح عن معلومة ما، موجودة سواء لأمور الخير أو أمور الشر. إبحث في شبكة الإنترنت عن قصص واقعية حول الهندسة الإجتماعية. يمكن أن تكون القصص من التاريخ القديم أو حدثت مؤخراً في مكان ما. إحدى تلك القصص يجب أن تكون حول إستخدام الهندسة الإجتماعية لتحقيق أمر محمود وليس لتحقيق الضرر. بعد الحصول على القصص، أجب عن التالي لكل قصة:

1. متى وأين حصلت القصة؟

2. ماذا حاول المهندس الإجتماعي أن يحقق أو يحصل من الضحية؟

3. ماذا فعل المهندس الإجتماعي للحصول على المطلوب من الضحية؟

4. ماهو الأسلوب المتبع بحسب ماتعلمته في الفصل الدراسي؟

5. كيف يمكن وقف الهندسة الإجتماعية؟ حدد إجابتك بوضوح

الإستخدام المقبول وحماية أجهزة الحاسب الآلي	الدرس الثالث

تعريفات

البرامج المقرصنة Pirated Software: هي تلك النسخ غير الأصلية من برامج وتطبيقات الحاسب الآلي التي تُنسخ وتوزع دون ترخيص معتمد من الجهة المصدرة لها.

إنهيار Crash: يقصد بعملية الإنهيار، توقف البرنامج عن العمل سواء بالخروج غير المتوقع أو التوقف تماما عن العمل وعدم الإستجابة للمهام المطلوبة من قبل المستخدم. قد يتسبب الإنهيار أيضاً بتوقف البرامج الأخرى.

الجدار الناري Firewall: وسيلة تسمح بتمرير أو صد مرور المراسلات الإلكترونية المتبادلة بين جهاز الحاسب الآلي والشبكات كشبكة الإنترنت لأهداف الأمن والحماية.

الجدار الناري الشخصي عبارة عن برنامج يثبت في أجهزة الحاسب الآلي الشخصية واللوحية والمحمولة لأداء هذه المهمة.

الإستخدام المقبول

أضحت الحاسبات الآلية أكثر تقدماً وتوفر كمّاً هائلاً من المعلومات مقارنة مع ذي قبل. تستطيع تلك الأجهزة إجراء العديد من العمليات الحسابية المعقدة في دقائق بل ثوان عدة، نستطيع كتابة الرسائل والبحوث وتعديل الصوّر، ونستطيع البحث عن المعلومات الكثيرة ونتواصل مع الناس من مختلف دول العالم. بسبب كل تلك القدرات الهائلة لأجهزة الحاسب الآلي، فإن التعامل معها وتشغيلها يتطلب قدراً من المسئولية والإلتزام وإحترام القوانين أيضاً في بعض الأحيان. حين نستخدم الحاسب الآلي أو الهاتف النقال أو الهواتف الذكية فإنه يجب أن نفكر بنتيجة ما قد نفعله فقد يكون مزعجاً أو مضراً لنا أو للغير.

يجب أن تكون خياراتنا المرتبطة بإستخدام أجهزة الحاسب الآلي والهواتف الذكية منسجمة مع تحقيق الأمن والسلامة عند إستخدام تلك الأجهزة.

لا تسبب الضرر

لاتسبب الضرر.. شعار يستخدم بقوة في عالم الطب والأدوية، ولكنه شعار مناسب أيضاً عند العناية بجهاز الحاسب الآلي. إن الكيفية التي يستخدم فيها الحاسب الآلي قد تكون نافعة أو ضارة لك ولغيرك، وعليه يحسن بك تجنب العديد من الأمور التي تسبب ذلك الضرر.

لاتستخدم الحاسب الآلي وأجهزة الهاتف في إزعاج الآخرين ومضايقتهم. قد يظن البعض بأنه من خلال إستخدام الحاسب الآلي يمكن إزعاج الآخرين دون إمكانية تعقبهم ولكن في حقيقة الأمر تتوفر لدى الجهات الأمنية والتقنية المختصة كافة الأدوات التي تتيح الوصول للشخص الذي أرسل رسالة مزعجة أو نشر تجريحاً أو تشهيرا بشخص آخر على شبكات التواصل الإجتماعي أو صفحات الإنترنت والمنتديات الإلكترونية. كن حاذقاً ولا تشترك في أية أمور من شأنها إزعاج الآخرين.

حذارى من النسخ غير المشروع

لاتقم بتنزيل نسخ البرامج المقرصنة أو نسخ البرامج دون ترخيص من غير الجهة المصدرة لها. إن تنزيل البرامج المقرصنة يعد عملاً غير مشروع ويستوجب المسائلة القانونية، كما أنه قد يكون خطيراً جداً من حيث تلغيم تلك البرامج بالفيروسات وبرامج التجسس ومختلف الشفرات الخبيثة بمجرد تثبيتها أو تشغيلها.

من الناحية القانونية فإن صاحب الجهاز سيكون مسئولاً عما فيه من برامج وتطبيقات حتى وإن ثُبّتت بواسطة شخص آخر، وهناك العديد من الأمثلة الواقعية التي دفع فيها بعض الأشخاص مبالغ مالية كبيرة أو تمت معاقبتهم بالسجن بسبب تثبيت نسخ غير أصلية ومقرصنة من بعض التطبيقات.

هناك ثلاثة مخاطر رئيسية عند تثبيت نسخ مقرصنة من البرامج:

- بسبب التعديل الخفي على شفرة تلك البرامج لحذف خصائص الحماية فقد لاتعمل بشكل طبيعي وتتسبب في التوقف أو تعطيل جهاز الحاسب الآلي نهائياً وقد يتوجب إعادة التهيئة الشاملة للجهاز.
- قد تكون النسخة المقرصنة من البرنامج أو التطبيق ملغمة بإحدى الشفرات الخبيثة وعليه فقد تمكّن القراصنة من إختراق الجهاز والعبث به وتنزيل محتوياته من ملفات وصوّر أو تغيير المعلومات أو حذفها، أو سرقة كلمات المرور الحساسة وقد يصل الأمر للتحكم التام بالجهاز.
- في أحيان عدة تقوم الجهات المصدرة للبرنامج بإجراء بعض التحديثات الفنية أو الأمنية على النسخ المنشورة وتطلب من مستخدمي تلك البرامج تنزيل تلك التحديثات لمعالجة القصور في تلك النسخ. في غالب الأحيان لن تتمكن من الحصول على تلك التحديثات عند إستخدامك نسخ غير أصلية أو نسخ مقرصنة من تلك البرامج.

أفضل نصيحة.. لاتقم بتنزيل أو تثبيت برامج غير أصلية ونسخ مقرصنة من البرامج والتطبيقات.

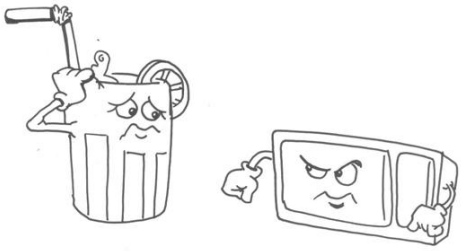
العناية بجهاز الحاسب الآلي

يتوجب علينا العناية التامة بجهاز الحاسب الآلي، ليس بسبب سعره فحسب وإنما لما فيه من معلومات وصوّر وملفات قد تكون مهمة جداً بالنسبة لنا وخسارتها تعني الكثير عند تعطل ذلك الجهاز أو إختراقه من قبل الغير. هناك عناية مماثلة بالهواتف النقالة أو الهواتف الذكية التي نحملها اليوم. على سبيل المثال، الصوّر الخاصة، والتقارير المهمة، وأرقام هواتف الأصدقاء والمعارف كل تلك الأمور من شأنها أن تسبب لنا إزعاجاً كبيراً عند ضياعها أو فقدانها لسبب أو آخر.

رغم تقدم التقنية اليوم وتطوّر أجهزة الحاسب الآلي وطرق تصميم الدوائر الإلكترونية ووسائط التخزين وتقنيات تبادل المعلومات ، تظل جوانب العناية بتلك الأجهزة ضمن أهم السلوكيات والمباديء التي يجب أن نلتزم بها.

العناية المادية للجهاز

العناية المادية بالجهاز قد تكون الأبسط ولكنها الأكثر إهمالاً من قبل المستخدمين، ونعني بالعناية المادية هي حماية الحاسب الآلي من العطل أو السرقة. حين يتعطل الجهاز فلن تستطيع الوصول إلى المعلومات والملفات المخزنة فيه ولن تستطيع القيام بأية مهام أخرى حتى يتم إصلاحه أو إستبداله.



أجهزة الحاسب الآلي والسوائل: الحاسب الآلي جهاز إلكتروني والسوائل تسبب ضرراً بالغاً له حين تنسكب عليه تلك السوائل، كما أن الأمر خطير أيضاً بالنسبة لك حيث أن أجهزة الحاسب الآلي تعمل بالكهرباء والسوائل من شأنها أن تحدث تماس كهربائي خطير، وعليه ينبغي الحذر الشديد. تجنب وضع السوائل بمختلف أنواعها بالقرب من أجهزة الحاسب الآلي أو الهواتف.

الحاسب الآلي والغبار: قد تتضرر الدوائر الإلكترونية المشغلة لجهاز الحاسب الآلي بسبب الغبار والأوساخ، وعليه يجب العناية بها وتنظيف الجهاز بشكل مستمر، ولاتنسى تنظيف الجهاز من أسفل ومن الخلف حيث توجد فتحات التهوية ومراوح التبريد، كما لاتنسى تنظيف الشاشة ولوحة المفاتيح. التنظيف السليم يكون بقماش نظيف أو من خلال السوائل المتخصصة لذلك، ولكن تذكر بأن التنظيف يجب أن يكون والجهاز مغلق.

تأثر الحاسب الآلي بالحرارة المرتفعة: إن الحرارة المرتفعة من شأنها تعطيل الدوائر الإلكترونية بجهاز الحاسب الآلي، وعليه تجنب وضع الجهاز لمدة طويلة في الشمس، وعدم ترك الجهاز في السيارة لفترات طويلة.

تأثر أجهزة الحاسب الآلي عند السقوط: قد تسقط أجهزة الحاسب الآلي المحمولة أو اللوحية أو الهواتف خصوصاً عندما نحمل أشياء كثيرة في أيدينا ومن شأن ذلك السقوط أن يكسر الجهاز أو الشاشة أو يوثر على المعلومات المخزنة فيه أو يمسحها أيضا. يحسن بك وضع الأجهزة والهواتف في الحقائب والأغطية الملائمة لها.

بما أن أجهزة الحاسب الآلي اليوم لاسيما المحمولة منها والأجهزة اللوحية والهواتف الذكية صغيرة الحجم وخفيفة الوزن، فإنه من المهم أن تكون تحت أنظارنا وألا نغفل عنها حيث أنها عرضة للضياع أو السرقة.

تعوّد دائماً أن تكون تلك الأجهزة معك وعدم تركها ولو لدقائق معدودة في الأماكن العامة كالمقاهي والمكتبات.

العناية التقنية

من المهم جداً أن نفعّل الخصائص التقنية التي تزيد من حماية أجهزتنا. لنستعرض معاً بعض الأمور الأساسية ثم ننتقل للأمور الأكثر تقدماً.

هناك خمسة خطوات أساسية يتوجب إتباعها لزيادة حماية الأجهزة.

1) تفعيل كلمة المرور للدخول على الجهاز
2) تفعيل خاصية حافظ الشاشة وتفعيل كلمة المرور فيها
3) تفعيل خاصية التحديث التلقائي
4) تثبيت برنامج مكافحة الفيروسات والجدار الناري بالجهاز
5) تعطيل مايعرف ب"حساب الزائر" في الجهاز وهو الحساب الذي يسمح بالدخول على موارد الجهاز كمستخدم زائر وليس كمستخدم أساسي

ضبط كلمة المرور للدخول:

عند الدخول على أجهزة الحاسب الآلي، قد يُطلب منك إدخال مايعرف بهوية المستخدم أو إسم المستخدم ويسمى أيضا ب"حساب المستخدم"، كما يطلب الجهاز بشكل إختياري إدخال كلمة المرور للمستخدم التي يجب أن تهيء سابقاً. في حال عدم تهيئة هذا الخيار، فسيُسمح له الدخول على الحساب دون إدخال كلمة السر. من المهم جداً إستخدام كلمة مرور للدخول، حتى نمنع الغير من إستخدام الجهاز والدخول على الملفات والصوّر الخاصة بنا بشكل مباشر.

إذا أهملنا تهيئة وضبط كلمة المرور فإن الجهاز سيكون عرضة لمخاطر أمنية متعددة مثل سرقة المعلومات أو حذفها أو التلاعب بها وتغيير محتواها أو تثبيت شفرات خبيثة بالجهاز.

تذكر، يجب أن تختار كلمات المرور بعناية. كلمة المرور يجب أن تكون سهلة التذكر بالنسبة لك.. صعبة التخمين بالنسبة للغير.

تفعيل خاصية حافظ الشاشة:

هذه الخاصية استخدمت سابقاً لحماية الشاشة من مخاطر التأثر نتيجة بقائها فترة طويلة دون تغيير في محتواها، ولكنها مفيدة أيضاً في حماية الأجهزة من مخاطر الدخول عليها وسرقة المعلومات أو الإطلاع عليها دون إذن. من خلال هذه الخاصية يتم ضبط حافظ الشاشة للعمل التلقائي عند ترك أو عدم لمس الجهاز دون إستخدام لفترة معينة. على سبيل المثال، بعد 10 دقائق من ترك الجهاز سيعمل برنامج حافظ الشاشة وعند العودة للعمل على الجهاز مجدداً فسيطلب منك إدخال كلمة المرور ليتسنى لك إكمال عملك على الجهاز. هذه خاصية مهمة جداً ويتوجب عليك ضبط وتفعيل خيار كلمة المرور أولاً في برنامج حافظ الشاشة.

التحديث التلقائي:

تتيح عملية التحديث التلقائي لملفات نظام التشغيل وملفات البرامج الأساسية الأخرى، الحماية ضد بعض المخاطر والتهديدات لاسيما أن الشركات لديها مراجعة دورية لبرامجها وقد تكتشف بعض الثغرات الأمنية الحساسة التي تتوجب تحديث بعض الملفات والمكتبات البرمجية. يحاول بعض قراصنة الحاسب الآلي الإستفادة من تلك الثغرات والبحث عن الأجهزة التي لم يتم تحديثها بغرض إختراقها أو تعطيلها. تعلم كيفية ضبط خيار التحديث التلقائي في جهاز الحاسب الآلي حتى تتجنب تلك المخاطر والتهديدات.

من جانب آخر فلا تنسى تفعيل خاصية التحديث التلقائي لبقية التطبيقات المثبتة بالجهاز فقد تكون أيضاً مصدراً لبعض التهديدات الأمنية. ننصحك بتفعيل عملية التحديث التلقائي لتكون كل 30 يوماً على أكثر تقدير.

تثبيت برنامج مكافحة الفيروسات وتفعيل الجدار الناري:

كل أنظمة الحاسب الآلي بمختلف أنواعها (حتى أجهزة أبل والأجهزة التي تعمل بنظام لينكس) معرضة لمخاطر الشفرات الخبيثة. لزيادة الفعالية ضد هذه الشفرات فإنه يتوجب عليك تثبيت برامج مكافحة الفيروسات للتأكد من خلو الجهاز من الفيروسات وبرامج التجسس والشفرات الخبيثة الأخرى، كما تقوم هذه البرامج بالتحقق الفوري من مرفقات الرسائل الإلكترونية الواردة والملفات المنزلة من شبكات التواصل الإجتماعي وغرف الدردشة وبرامج المراسلات الفورية، وينبغي أن نتأكد بأن برنامج مكافحة الفيروسات يعمل بشكل صحيح، وأن تكون قائمة الفيروسات المستهدفة محدثة بشكل دوري، علماً بأنه يوجد العديد من الفيروسات والشفرات الخبيثة التي تنتشر يومياً.

.

من جانب آخر، يعمل الجدار الناري كوسيلة تسمح بتمرير أو صد مرور المراسلات الإلكترونية المتبادلة بين جهاز الحاسب الآلي والشبكات كشبكة الإنترنت بهدف الأمن والحماية. الجدار الناري الشخصي عبارة عن برنامج يثبت في أجهزة الحاسب الآلي الشخصية و اللوحية والمحمولة لأداء هذه المهمة.

من خلال الجدار الناري لن يتمكن قراصنة الحاسب الآلي من الوصول لجهازك والتعرف عليه، فيحسن بك تفعيل عمل هذا البرنامج حيث يوجد ضمن البرامج الأساسية التي تأتي مع نظام التشغيل. تعلم كيفية تفعيل هذا البرنامج في نظام التشغيل المستخدم في جهازك.

تعطيل حساب الزائر وضبط المشاركة في الملفات بحاسبك الشخصي:

تحتوي العديد من أجهزة الحاسب الآلي على مايعرف "بحساب الزائر" والذي يسمح لأي شخص بالدخول على الجهاز للإستخدام المؤقت أو الإستخدام بالأماكن العامة. عادة مايتم ضبط هذا الحساب من خلال كتابة كلمة "زائر" كإسم للمستخدم أو هوية للمستخدم ودون الحاجة لإدخال كلمة المرور. من المهم تعطيل هذا الحساب في جهازك الشخصي لتجنب إستغلاله من قبل الغير بغرض التهديدات الأمنية مثل تثبيت برامج التجسس أو برامج ضارة أخرى.

تعلم كيف يمكنك تعطيل حساب الزائر في حاسبك الشخصي وستجد ذلك غالباً في خيار الحسابات ضمن قائمة ضبط النظام.

من جانب آخر يتوجب عليك أيضاً ضبط "خاصية المشاركة في الملفات" بحيث تكون متاحة فقط عند الطلب ومن خلال إسم المستخدم وكلمة المرور. هذه الخاصية تعني أن تسمح للغير بالدخول على مجلد معين يحتوي على ملفات وصوّر بغرض المشاركة مع الغير وهي خاصية مفيدة عند العمل الجماعي للمشاريع وتعديل الملفات وكتابة ومراجعة التقارير والبحوث، ولكنها قد تكون مصدراً لتهديد أمني إن لم تضبط بشكل صحيح فقد تستغل من قبل الغير لنسخ محتوى المجلد أو حذف مافيه من ملفات أو تغيير محتواها.

ينبغي تعطيل خاصية المشاركة في الملفات عند الإنتهاء منها ومراجعة محتوى المجلد بشكل دوري للتأكد من عدم وجود برامج وشفرات غريبة أو مشبوهة، كما ينبغي التأكد من تفعيل خاصية المشاركة لمجلدات معينة فقط وليس كل المجلدات الأساسية والمتفرعة منها.

تعلم كيفية ضبط خاصية المشاركة في الملفات بجهازك.

ضبط الخيارات الأمنية

إبحث في شبكة الإنترنت عن مصدرين أو أكثر حول حماية أجهزة الحاسب الآلي. قم بتحديد نوع نظام التشغيل (ويندوز، ماكنتوش أو إس).

1. لماذا تظن بأن المصادر المختارة يمكن الإعتماد عليها كمصادر موثوقة للمعلومات؟

2. من المصادر المختارة، أكتب عن ثلاثة أمور من شأنها زيادة حماية الحاسب الآلي ولم ترد ضمن هذا الكتاب؟ إشرحها بالتفصيل وكيف يمكن ضبطها في الجهاز؟

3. هل ستقوم بضبط هذه الأمور في حاسبك الشخصي ؟ إشرح الإجابة؟

نصائح سريعة

- لاتنزل أو تثبت برامج وتطبيقات للهواتف النقالة والهواتف الذكية مالم تكن من مصدر معتمد وموثوق به. التطبيقات المزيفة قد تحتوي على شفرات خبيثة من شأنها الضرر بك وبالجهاز.
- كن حذراً بالنسبة لطلبات الضبط المسموحة والممنوعة عند تثبيت التطبيقات بالهواتف لاسيما تطبيقات تحديد المواقع وتطبيقات الشبكات الإجتماعية. لاتقبل الطلب إذا كان غريباً أو مثيراً للريبة.
- لاترد على الرسائل النصية القصيرة، والرسائل الإلكترونية، والإتصالات من الغرباء.
- لاتضغط على الروابط للملفات أو المواقع في الرسائل النصية القصيرة.
- أخبر والديك حالاً عند إستلامك لرسائل أو مكالمات مزعجة أو مؤذية.
- كن حذراً عند إستخدام تطبيقات تحديد المواقع.
- كن فطناً بشأن الهندسة الإجتماعية وإحذر من خرق القواعد والقوانين.
- إذا استلمت رسالة إلكترونية أو رسالة نصية قصيرة تطلب منك الرد مقابل الحصول على مكافأة سخية أو هدية قيمة لمجرد الرد، فينبغي الحذر وحذف الرسالة فوراً وعدم الرد عليها.
- لاترسل أو تنشر بيانات شخصية أو معلومات خاصة عبر البريد الإلكتروني أو الرسائل النصية القصيرة أو برامج المراسلة الفورية.
- إذا استلمت رسالة "عاجلة" تطلب منك إرسال معلومات خاصة مثل كلمة المرور، أو العنوان، أو رقم الحساب البنكي، فلا تستجب للطلب، وأخبر والديك بالأمر حالاً، وقم بالإتصال مباشرة بالشركة التي طلبت المعلومات للتحقق من الأمر.
- كن حذراً بشأن طبيعة ماتنشر من معلومات وصوّر في مواقع التواصل الإجتماعي.
- لاتقم بتنزيل أو نسخ أو تثبيت البرامج المقرصنة وغير المرخصة.
- من أبسط إجراءات زيادة فعالية الحماية في أجهزة الحاسب الآلي ضبط كلمات المرور، وتفعيل برنامج حافظ الشاشة وتفعيل خاصية كلمات المرور فيه.
- لاتنسى أيضاً تثبيت برنامجي مكافحة الفيروسات والجدار الناري وتفعيل خاصية التحديث التلقائي لنظام التشغيل وبرنامج مكافحة الفيروسات.
- قم بتعطيل "حساب الزائر" إن وجد في جهاز الحاسب الآلي الخاص بك.
- إهتم بجوانب الحماية المادية للجهاز مثل نظافته، وحمله بعناية وعدم تعريضه للحرارة.

إختبر معلوماتك	

1. حدد نوعين من أساليب تعطيل الجهاز أو إختراقه بطرق تقنية؟
   أ. الشفرات الخبيثة
   ب. التطبيقات المزيفة
   ج. فك منظومة العمل (جيلبريك)
   د. التصيد بالرسائل النصية القصيرة

2. إشرح بمفهومك معنى فك منظومة العمل (جيلبريك) ولماذا يعد خطيراً؟

3. ماذا يمكنك القيام به لحماية هاتفك؟ حدد كل الإجابات الصحيحة:

   أ. معرفة وتجنب التطبيقات المزيفة
   ب. عدم الرد على الرسائل النصية القصيرة من الغرباء
   ج. عدم الضغط على الروابط للملفات والمواقع في الرسائل النصية القصيرة
   د. إخبار والديك عند إستلامك لرسالة نصية قصيرة تحتوي على محتوى مزعج أو تهديد
   ه. عدم تنزيل وتثبيت التطبيقات من المتاجر المختلفة بشبكة الإنترنت

4. في يوم ما، ذهبت للمقهى مع بعض الأصدقاء وترغب في إخبار الغير بموقعك. وعليه نشرت ذلك في مواقع التواصل الإجتماعي. هل تظن من المناسب أولاً الإستئذان من بقية الأصدقاء الحضور بما ترغب نشره؟ إشرح إجابتك؟

5. ماذا يمكنك القيام به لحماية هاتفك النقال من التطبيقات المزيفة أو الشفرات الخبيثة؟
   أ. تنزيل الملفات من المواقع المعتمدة فقط من الجهة المصنعة للهاتف
   ب. فك منظومة العمل (جيلبريك)
   ج. مراجعة التعليقات المنشورة حول تطبيق ما بمتجر التطبيقات قبل تنزيله من المتجر
   د. عند تثبيت أي تطبيق تأكد من الخيارات لطلبات الضبط المسموحة والممنوعة عند تثبيت ذلك التطبيق
   ه. راجع فاتورة الهاتف بشكل دوري

6. حدد بعض الأساليب المعتمدة في الهندسة الإجتماعية؟ إختر كل الإجابات الصحيحة
   أ. تقديم الهدية أو الجائزة للضحية المستهدفة
   ب. محاولة تشتيت الذهن والتركيز للضحية المستهدفة
   ج. تخويف وتهديد الضحية
   د. شد إنتباه الضحية من خلال موضوع يثير الفضول
   ه. إقناع الضحية بأنه صديق له ومحاولة كسب وده وثقته
   و. إخبار الضحية بالهدف الحقيقي من التواصل معها

7. كيف يمكنك تجنب الهندسة الإجتماعية وصدها؟ حدد كل الإجابات الصحيحة:
   أ. معرفة البيانات الشخصية والمعلومات الخاصة
   ب. عدم مشاركة الغرباء بأية بيانات شخصية أو معلومات خاصة
   ج. تجنب قبول العروض المالية والهدايا التي تبدو غريبة أو مشبوهة
   د. كن حذراً بشأن الشخص الذي يطلب منك خرق القواعد والقوانين بمقابل عائدٍ ما
   ه. تأكد من رسائل البريد الإلكترونية قبل القيام بأي رد
   و. الضغط على كل الروابط في الرسائل الإلكترونية للتأكد من محتواها
   ز. نشر أية معلومات في مواقع التواصل الإجتماعي

8. لماذا ينبغي عدم تنزيل أو تثبيت أية برامج مقرصنة؟ حدد كل الإجابات الصحيحة:
   أ. لأنها تحتوي على الفيروسات
   ب. يمكنني تنزيلها وتثبيتها بمساعدة المختصين
   ج. لأنها نسخة غير مشروعة وغير مرخصة
   د. لن تستطيع الحصول على التحديثات المتعلقة بتلك النسخ المقرصنة
   ه. ستعمل تلك النسخ بشكل طبيعي تماماً

9. حدد بعض الإجراءات التقنية التي تزيد من حماية جهاز الحاسب الآلي:
   أ. عدم إستخدام كلمات المرور نهائياً
   ب. تفعيل برنامج حافظ الشاشة وتفعيل خاصية طلب كلمة المرور فيه
   ج. تفعيل خاصية التحديث التلقائي
   د. تثبيت برنامج مكافحة الفيروسات والجدار الناري بالجهاز
   ه. تعطيل "حساب الزائر" وخاصية مشاركة الموارد بالجهاز

10. حين تسافر بالطائرة، ينبغي أن يكون جهاز الحاسب الآلي معك دائماً وليس في حقائب السفر.
   أ. صح
   ب. خطأ

11. حدد ثلاثة أمور أخرى من شأنها زيادة الحماية المادية لجهاز الحاسب الآلي من الأضرار؟

أ. .

ب. .

ج. .