السلامة الرقمية العائلية

الفئة المستهدَفة

المرأة والأسرة

الأكاديمية الوطنية للأمن السيبراني

National Cyber Security Academy

السلامة الرقمية العائلية

الفئة المُستهدَفة: المرأة والأسرة

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

حقوق الملكية الفكرية

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

00974 404 663 62
00974 404 663 79
academy@ncsa.gov.qa
www.ncsa.gov.qa/

يناير 2025م
الدوحة، قطر

◆ عزيزي المشارك

في ظلّ التطوُّر التكنولوجي المتسارع، ودخول الإنترنت إلى مختلف مجالات الحياة؛ أصبحت التهديدات السيبرانية تُواجِه مختلف شرائح المجتمع، ما يتطلَّب العمل على تعزيز الوعي بمفاهيم السلامة الرقمية؛ التي تُعدّ الدّرع الذي يحمي المجتمع من هذه التهديدات.

وفي سياق جهود «المبادرة الوطنية للسلامة الرقمية» لتعزيز مؤشرات السلامة الرقمية في المجتمع؛ تُقدِّم الوكالة الوطنية للأمن السيبراني هذا الكُتَيِّب، والذي يتضمَّن مجموعةً من النصائح والإرشادات العامَّة المتعلّقة بالسلامة الرقمية.

الفهرس	رقم الصفحـة

الفهرس	رقم الصفحـة

مُقدّمـــة

لا تقتصر التهديدات السيبرانية على الأعمال التجارية والشركات بل تمتد إلى أفراد الأسرة بمختلف أعمارهم، والتي تتنوع بين البرمجيات الضّارّة وعمليات الاحتيال عبر الإنترنت وخروقات البيانات وأجهزة الحاسوب والهواتف الذكية، وكذلك إنترنت الأشياء الذي يترك الأُسرة عُرضة للجرائم الإلكترونية، ولهذا فإن ما يستلزم مؤسسات الأعمال والشركات القيام به لحماية مصالحها من آثار التهديدات السيبرانية الخطيرة هو نفسه المطلوب بالنسبة لأفراد الأسرة، بما يتضمّنه ذلك من الاعتماد على برامج الحماية والمكافحة المعتمدة، والوعي الرقمي، والاستخدام الصحيح لشبكة الإنترنت.

فعلى الرغم من المنافع العائدة من الإنترنت والتكنولوجيا بوجهٍ عامّ؛ إلا أن تكلفة الاستخدام اليومي رافقتها ظواهر سلبية؛ مثل: ظاهرة العنف الإلكتروني ضد المرأة والأطفال، وقد اشتمل هذا العنف على أنواع من الجرائم الإلكترونية؛ مثل: المضايقات، وسرقة الهوية والبيانات الشخصية، واستغلالها ضد الضحايا؛ إما للحصول على المال، وإما للقيام بخدمات يُعاقب عليها القانون، مثل: عمليات الاحتيال على الآخرين.

لهذا كان الوعي بالسلامة الرقمية السبيل لتخطّي هذه الأضرار، والحدّ منها؛ فالوعي الرقمي يُؤهّل المستخدِم للاستخدام الآمِن للإنترنت والتطبيقات والبرامج، ويزيد من مرونته وقدرته على التعامل مع المواقف المختلفة التي قد يتعرَّض لها؛ مثل: برمجيات الفدية، والخروقات الأمنية. كما أن السلامة الرقمية تُزوّد المستخدم بالآليات التي تحفظ أجهزته الإلكترونية وبياناته من الخرق أو السرقة.

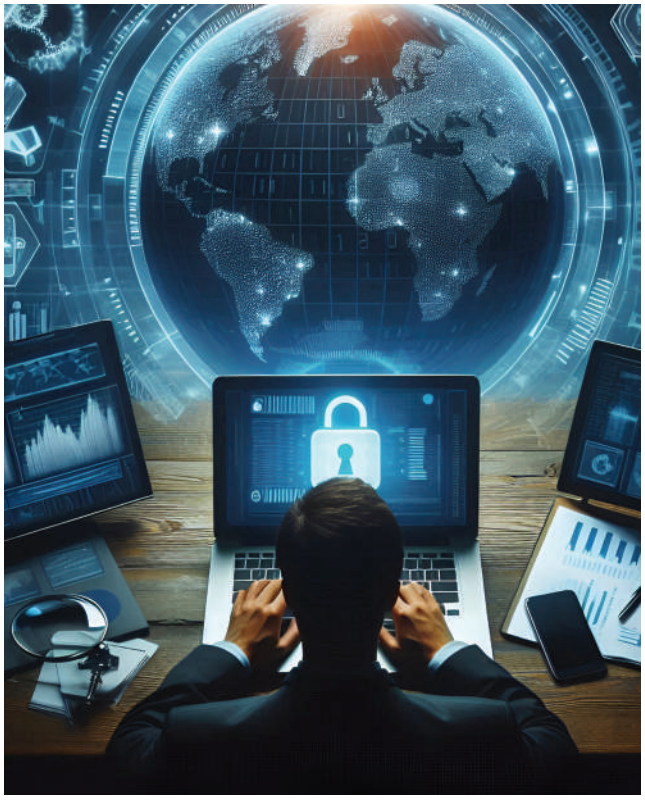
01

الفصل الأول

خروقات البيـــانات الشـــــــخصية

- أولاً: **خروقات البيانات الشخصية Personal data breache**
- ثانياً: **الأساليب الشائعة المستخدَمة في خروقات البيانات:**
  - التصيد الاحتيالي
  - البرمجيات الضّارَّة
- ثالثاً: **خروقات البيانات والجرائم الإلكترونية ضد المرأة.**

أولاً: خروقات البيانات الشخصية Personal data breaches



هي حوادث أمنية تَستهدف كشف المعلومات والبيانات الحساسة بشكلٍ غير مصرَّح به، وقد تحدث عبر الإنترنت، أو من خلال البلوتوث أو الرسائل النصية. وبالنسبة للأفراد، تحدث خروقات البيانات data breaches نتيجة فقد جهاز الحاسوب والهاتف الذكي، أو إصابتهما بالبرمجيات الضّارَّة، أو إتاحة الوصول للبيانات الشخصية المهمة لأفراد غير مصرَّح لهم بذلك.

إذاً خرق البيانات هو أيّ حادث أمني يتمكَّن فيه أفراد غير مصرَّح لهم من الوصول إلى معلومات حساسة، بما يشمل البيانات الشخصية مثل: أرقام الضمان الاجتماعي، وأرقام الحسابات المصرفية. ومن أمثلته: هجوم برمجيات الفدية الذي يحجب البيانات، ويشترط للإفراج عنها دَفْع مبالغ مالية[1].

احذر!

تهدف خروقات البيانات الشخصية Personal data breaches إلى كشف المعلومات والبيانات الحسّاسة بشكلٍ غير مصرَّح به، وقد تحدث عبر الإنترنت، أو من خلال البلوتوث والرسائل النصية.

1. What is a data breach? Follow link: https://www.ibm.com/topics/data-breach.

تحدث خروقات البيانات من خلال عدة نقاط ضعف؛ ومن أبرزها ما يلي:

الثغرات الرقمية:

وهي عيب أو خَلل في النظام، يتمكَّن المجرمون من اكتشافه واستغلاله لخَرق الأنظمة وسرقة البيانات.

الثغرات المعرفية:

وهي ضَعْف في خبرة المستخدِمين، وعدم الدراية الكافية بأُسُس السلامة الرقمية، وهنا يستغلّ المجرمون هذا الضعف المعرفيّ للإيقاع بالمستخدِمين وسرقة بياناتهم الشخصية.

فأجهزة الحاسوب، وكافة الأجهزة الإلكترونية، نتيجة اتصالها بالإنترنت تتزايد مخاطر تعرُّضها لخرق البيانات، فعلى سبيل المثال: أجهزة إنترنت الأشياء The Internet of things (IoT)؛ حيث تواجه بعض منتجات "المنزل الذكي" عيوباً مثل الافتقار إلى التشفير؛ الأمر الذي يستغلّه مجرمو الإنترنت للتسلل إلى بيانات أفراد الأسرة[1].

ليست فقط التكنولوجيا هي السبب الوحيد للتعرُّض لخروقات البيانات، بل يُعدّ سلوك المستخدِم عاملاً رئيساً في تلك الحالات، فإذا تصرَّف فرد واحد داخل الأسرة بأسلوب خاطئ على شبكة الإنترنت مثل فتح المرفقات المشبوهة الواردة بالبريد الإلكتروني؛ فهذا يعني تعرُّض باقي أفراد الأسرة للتهديدات السيبرانية.

حقائق وأرقام

- تم تسريب بيانات 6,41 مليون مستخدِم في العالم في الربع الأول من عام 2023م، ممَّا أدَّى إلى تضرُّر ملايين الأفراد[2].
- أكثر من 52% من إجمالي حوادث خروقات البيانات خلال عام 2023م التي أصابت المؤسسات العالمية؛ استهدفت المعلومات الشخصية للعملاء.

1. How Data Breaches Happen & How to Prevent Data Leaks. Follow link: https://www.kaspersky.com/resource-center/definitions/data-breach.
2. Data breaches worldwide - Statistics & Facts. Follow link: https://www.statista.com/topics/11610/data-breaches-worldwide/#topicOverview.

ثانياً: الأساليب الشائعة المستخدَمة في خروقات البيانات

01 التصيد الاحتيالي

02 البرمجيات الضّارّة

التصيد الاحتيالي Phishing

التصيد الاحتيالي هو واحد من أكثر الجرائم الرقمية انتشاراً؛ حيث يستغل المهاجمون شبكة الإنترنت لخداع الضحايا بهدف سرقة معلوماتهم الشخصية، مثل كلمات المرور وأرقام بطاقات الائتمان. ويتم ذلك باستخدام مجموعة مُتنوّعة من الأساليب والأدوات، مثل إنشاء مواقع إلكترونية مزيَّفة لجذب الضحايا، ويتم إرسال الروابط عبر البريد الإلكتروني أو الرسائل النصية لاستدراجهم. وعند الضغط على الرابط، يتمكَّن المهاجمون من الدخول غير المشروع إلى حسابات وأجهزة الضحايا، وتثبيت برمجيات خبيثة تُمكّنهم من سرقة البيانات دون عِلْم المستخدِمين.

ويعتمد المهاجمون في التصيد الاحتيالي على الضغط النفسيّ لإقناع الضحايا باتخاذ قرارات سريعة دون تفكير؛ من خلال انتحال شخصية معروفة، وخلق شعور زائف بالضرورة المُلِحَّة، ويستغلّون مشاعر الخوف والقلق لتحقيق أهدافهم. وغالباً ما يتمّ إشعار الضحايا بأنهم مُهدَّدون بخسارة أموالهم أو مواجهة مشكلات قانونية، أو قد يُحْرَمُون من الوصول إلى موارد مهمة إذا لم يتخذوا إجراءً فوريّاً، ممَّا يدفع الضحايا إلى الاستجابة السريعة دون التحقُّق.

أما البيانات المُستهدَفة في هجمات التصيد؛ فمن أهمها ما يلي:

- أسماء المستخدمين.
- كلمات المرور.
- أرقام بطاقات الائتمان.
- معلومات الحسابات المصرفية.
- كافة المعلومات المهمَّة التي يتسبَّب الكشف عنها في تضرُّر الفرد أو المحيطين به.

احذر!

من البيانات المُستهدَفة في هجمات التصيد: أسماء المستخدمين، كلمات المرور، أرقام بطاقات الائتمان، معلومات الحسابات المصرفية، وكافة المعلومات المهمَّة التي يتسبَّب الكشف عنها في تضرُّر الفرد أو المحيطين به.

من أمثلة التصيد الاحتيالي:

احتيال الرسوم المتقدّمة Advanced-fee scam

يتم الاحتيال بواسطة رسائل البريد الإلكتروني؛ حيث يعرض المهاجم طلباً للضحايا المستهدَفين يطلب منهم مبلغاً من المال لمساعدته إلى حين استلام مبالغ مالية كبيرة "وهمية"، وهنا يتم التلاعب بالضحايا ورغبتهم في الحصول على المال بطرقٍ سهلةٍ.

احذر!

لتجنُّب مخاطر احتيال الرسوم المتقدّمة ينبغي التحقُّق من عنوان البريد الإلكتروني للمرسِل قبل فتح الرسالة؛ فقد يكون الاسم المعروض زائفاً. كما ينبغي الحذر من الأرقام التي تبدأ بـ 07 لأن الحصول عليها مجاني. كما أن الأخطاء الإملائية والنحوية من العلامات الدالَّة على أن اليانصيب والجوائز عموماً عملية احتيالية.

وللتعامل مع هذا الهجوم؛ يُنْصَح بعدم تلبية طلبات الأفراد المجهولين، التي تتضمَّن إرسال الأموال مقابل أداء خدمة ما، ويمكن البحث عن الأمر على محرّك البحث جوجل Google، لمعرفة تفاصيل عمليات الاحتيال ذاتها التي سبق تكرارها في خداع آخرين.

مثال

اليانصيب أو الجوائز المالية، هنا يقوم المحتال بإخبار الضحية المُستهدَفة عبر البريد الإلكتروني بأنه فاز بمبلغ كبير من المال. وفي حال الرد سيطلب المحتال معلومات شخصية ونُسَخ من المستندات الرسمية مثل: جواز السفر كإثبات للهوية، ثم سيطلب دَفْع رسوم معينة ليتمكَّن الضحية من الحصول على مبلغ الجائزة[1].

1. Lottery scams. Follow link: https://www.actionfraud.police.uk/a-z-of-fraud/lottery-scams.

احتيال تزوير موقع الويب Website forgery scam

يقترن هذا النوع من الاحتيال بعمليات أخرى، مثل إلغاء تنشيط الحساب -السابق ذكره-، ففي هذا الهجوم الإلكتروني يقوم مجرمو الإنترنت بإنشاء موقع ويب مزيَّف مطابق للموقع الأصلي لجهةٍ ما، مثل البنك، وبمجرد زيارة الضحية للموقع يقع فريسة لعمليات التصيد، ويحدث ذلك عبر إرسال رسائل البريد الإلكتروني أو من خلال مُحرّك البحث؛ حيث قد يزور الضحية موقعاً ما، معتقداً أنه موقع موثوق، والهدف من هذا الاحتيال جَمْع بيانات المستخدمين لإعادة استخدامها في جرائم أخرى أو لبيعها عبر الإنترنت المظلم.

احذر!

يُنْصَح بالتحقُّق من عنوان الرابط URL الخاص بالمواقع عموماً في متصفح الويب؛ لتفادي الوقوع فريسة لعمليات الاحتيال، مع التأكُّد من بدء الرابط بـ HTTPS وليس HTTP.

التلاعب النفسي في عمليات احتيال تزوير المواقع

غالباً ما يلجأ مجرمو الإنترنت إلى التلاعب النفسي والعاطفي بضحاياهم؛ لتحفيزهم على اتخاذ قرارات تفيد هجماتهم الإلكترونية، ويتم ذلك من خلال عدة طرق، منها:

- **العروض السريعة أو التنبيهات التي تستعجل الضحية على اتخاذ إجراء عاجل دون تفكير جيد.**
- **الوعود الجذابة مثل: بطاقات الهدايا المجانية أو كسب المال، مما يدفع الضحية لعدم التفكير في مخاطر تنفيذ المطلوب للحصول على تلك الهدايا المجانية.**
- **التنبيهات الكاذبة بوجود فيروس ما تدفع الضحية إلى التدخل، وتنفيذ المطلوب في الرسائل دون تفكير أيضاً.**

ويُنْصَح بالتحقق من عنوان الرابط URL في متصفّح الويب لتفادي الوقوع فريسة لعمليات الاحتيال، مع التأكد من بدء الرابط بـ HTTPS وليس HTTP[1].

مثال

مع بدء تفشي فيروس كورونا (كوفيد-19)؛ ظهرت مواقع احتيالية مزيَّفة خاصة باللقاحات، ففي عام 2020م، ظهرت تقارير عن علاجات كاذبة للفيروس تتضمَّن جمع معلومات الدفع أو أرقام الضمان الاجتماعي الخاصة بالضحايا مقابل المشاركة التجريبية للقاح.

وما كشف زيف هذه المواقع هو تقديمها هدايا مقابل تسجيل الأسماء، كما طالبت الضحايا بتفاصيل حساسة مثل: رقم الحساب المصرفي.

1. What Are Scam Websites and How To Avoid Scam Websites. Follow link: https://www.kaspersky.com/resource-center/preemptive-safety/scam-websites.

معلومة

في النصف الأول من عام 2023م تم اكتشاف ما يقرب من 3 ملايين موقع ويب مزيّف مخصّص للتصيُّد الاحتيالي.

احذر!

يقوم مجرمو الإنترنت بإنشاء موقع ويب مزيَّف مطابق للموقع الأصلي لجهة ما مثل البنك، وبمجرد زيارة الضحية للموقع يقع فريسة لعمليات التصيد، ويحدث ذلك عبر إرسال رسائل البريد الإلكتروني، أو من خلال محرك البحث.

علامات تحذيرية للتعرُّف على مواقع الويب المزيفة:

- مخاطبة المشاعر عبر الإلحاح أو إثارة الخوف.
- ضعف جودة تصميم الموقع.
- كثرة الأخطاء الإملائية في النصوص أو الأخطاء النحوية.
- عدم تحديد صفحات الويب، مثل عدم تضمن الصفحة بيانات مثل «اتصل بنا» أو «نبذة عن».
- محاكاة أسماء النطاقات الأصلية؛ لذا يجب التأكد مراراً قبل زيارة أيّ موقع جديد؛ من خلال كتابة عنوان الرابط URL على مواقع مثل WHOIS للتحقُّق من صحته [1].
- طلب التحويل المصرفي المباشر؛ حيث يلجأ المحتال إلى طلب التحويل المباشر في عملياته الانتحالية لتيقّنه من صعوبة استرجاع المال.
- اكتب عنوان الويب يدوياً أو قم بحفظه في الإشارات المرجعية بدلاً من الدخول المباشر على الرابط المرسل الذي يتزايد خطر كونه مُزيَّفاً.
- تأكَّد من وجود رمز القفل، فجميع متصفّحات الويب مثل Firefox & Chrome تحتوي على ما يسمَّى «شهادة الأمان» SSL، لذا يُفضَّل التحقُّق من هذه الشهادة التي تعوق اعتراض مجرمي الإنترنت للمعلومات المرسلة للموقع. وللتحقُّق من وجود هذه الشهادة يتم البحث عن رمز القفل في عنوان URL الموجود في شريط العناوين.

احذر!

في حال الرد على البريد الإلكتروني الاحتيالي يجب قطع الاتصال مع المحتال، أما إذا تم تقديم بيانات الحساب المصرفي فينبغي في هذه اللحظة الاتصال فوراً بالبنك وإبلاغه.

1. Ryan Toohil, How To Identify Fake Websites: 11 Warning Signs, November 2023. Follow link: https://www.aura.com/learn/how-to-identify-fake-websites.

◆ في حال زيارة موقع احتيالي، اتبع الآتي:

- قطع الاتصال مع المحتال.
- البحث عن أيّ مدفوعات معلّقة أو مستمرة وإيقافها.
- إيقاف بطاقة الائتمان المُختَرقة.
- تحديث كلمات المرور الخاصة بالحسابات المصرفية والبريد الإلكتروني.
- تجميد الأرصدة لمنع وصول المحتال إليها.
- التحقّق من جهاز الحاسوب للتأكُّد من أنه خالٍ من البرمجيات الضّارَّة، أو برمجيات تسجيل لوحة المفاتيح.
- إبلاغ البنك، أو الجهة المقدِّمة للخدمة مثل متاجر التسوق الإلكتروني، أو الجهة الأمنية المختصة بتفاصيل عملية الاحتيال.

احذر!

يستهدف التصيد الاحتيالي Phishing خداع الضحية لدفعه إلى القيام ببعض الإجراءات التي تخدم الأهداف الخبيثة لمجرمي الإنترنت.

البرمجيات الضّارّة

هي مصطلح يشمل جميع أنواع برمجيات الحاسوب التي تتسبَّب في تضرُّر الأجهزة وخرق البيانات، فهي تسعى عمداً إلى غزو أجهزة الحاسوب والأنظمة والشبكات والأجهزة اللوحية والأجهزة المحمولة؛ إما بغرض إتلاف أنظمتها وإما تعطيلها أو سرقة بياناتها مع اختلاف الدوافع وراء ذلك، والتي تتنوع ما بين جني الأموال، أو تخريب العمل، أو لمصالح سياسية، أو لمجرد التباهي[1].

وغالباً يتم نشر البرمجيات الضّارّة عبر مواقع الويب ورسائل البريد الإلكتروني والبرمجيات المهكرة؛ حيث يمكن نشر تلك البرمجيات ضمن ملفات أخرى؛ مثل ملفات الصور أو المستندات. كما قد يتسبَّب المستخدِم نفسه في تثبيت برمجيات ضارة بدون قصد منه بعد الضغط على روابط مجهولة في رسالة بريد إلكتروني تصيدية، أو عند تنزيل البرامج من موقع ويب غير موثوق، أو عند توصيل الحاسوب بمحرك أقراص USB مُصَاب، أو عند زيارة موقع ويب مصاب ببرمجيات ضارّة.

إذًا يمكننا القول بأن البرمجيات الضّارّة ليست فيروساً، بل نوع من البرامج مصمَّم بغرض إلحاق الضرر بجهاز الحاسوب ومستخدميه. والطريقة الأكثر شيوعاً لاكتشاف هذه البرمجيات هي فحص الحاسوب بحثاً عنها[2].

أما عن إزالتها من جهاز الحاسوب، فهذا يختلف حسب نوع البرمجية الضّارّة المثبتة على الجهاز؛ إلا أن أبرز الوسائل المستخدَمة في ذلك هي برامج مكافحة الفيروسات؛ لفحص جهاز الحاسوب وحذف أيّ برمجية يتم رَصْدها.

1. Malware. Follow link: https://www.malwarebytes.com/malware.
2. What is Malware?. Follow link: https://www.mcafee.com/en-us/antivirus/malware.html.

أنواع البرمجيات الضّارَّة

الفيروسات Viruse

وهي برمجيات ضارَّة تعمل على تعطيل الأجهزة الإلكترونية، أو تدمير البيانات والملفات، وتتمثل خطورة هذه البرمجيات في قدرتها على نسخ نفسها بسهولة، مما يؤدي إلى إصابة الأجهزة الأخرى بها في حال نقل أيّ ملفات من جهاز مصاب بها إلى جهاز آخر، فعلى سبيل المثال، في حال وجود ملف Word يحمل برنامجاً خبيثاً؛ فإن البرنامج الخبيث ينتقل إلى أيّ جهاز آخر يتم فتح ملف Word عليه.

برمجيات الفدية Ransomware

هي نوع من البرمجيات الضّارَّة التي تقوم بمنع المستخدِم من الوصول إلى بياناته، مستغلَّة قلة خبرته في التصفُّح الآمِن على الإنترنت. وتنتقل هذه البرمجيات عادةً من خلال فتح مرفقات البريد الإلكتروني الواردة من مصادر غير معروفة أو عبر تحميل برامج وألعاب من مواقع غير موثوقة. بعد تثبيت البرمجيات الضّارَّة، يتم تشفير بيانات الضحية بحيث لا يمكنه الوصول إليها، ولا يتم فك التشفير إلا بعد دفع فدية مالية يُحدِّدها المهاجم. وهناك عدة أنواع من برمجيات الفدية، ومن الضروري أن يكون مُستخدِم الإنترنت على دراية تامَّة بها وبكيفية عملها؛ حيث إن الوعي بهذه البرمجيات يُمكّنه من الوقاية منها.

احذر!

غالباً ما يلجأ مجرمو الإنترنت إلى التلاعب النفسي والعاطفي بضحاياهم لتحفيزهم على اتخاذ قرارات تفيد هجماتهم الإلكترونية.

ديدان الحاسوب Worms

تُعدّ هذه البرامج مشابهة للبرمجيات الخبيثة، ولكنها تختلف بشكلٍ رئيس في أنها تستهدف الشبكات بشكل أساسي. تتميز هذه البرمجيات بقدرتها على التكرار بسرعة كبيرة، والانتشار عبر الشبكات بالكامل. تبدأ بإصابة جزء محدد من الشبكة، وسرعان ما تنتقل بسرعة لتشمل باقي أجزاء الشبكة.

وتهدف هذه البرمجيات إلى تعطيل الخدمات، مثل تعطيل الخدمات العامة التي تُقدَّم عبر الإنترنت، أو سرقة البيانات السرية التي يتم نقلها عبر الشبكة، مثل المعلومات المالية للعملاء، أو سجلات المرضى في المستشفيات، أو بيانات المؤسسات التعليمية، وغيرها[1].

برمجيات التجسس Spyware

يُعدّ التجسس الإلكتروني واحداً من أبرز المخاطر التي تُواجه مستخدمي الإنترنت، وهو من أخطر التهديدات الإلكترونية نظراً لأن المستخدم غالباً لا يشعر بوجود برمجيات التجسس على جهازه. وتبقى هذه البرمجيات مخفية حتى بعد اختراق الجهاز، وتهدف بشكلٍ رئيس إلى سرقة بيانات المستخدم لاستغلالها لاحقاً، سواء من خلال الابتزاز أو الإضرار بسُمْعته. وقد تُستخدم البيانات المسروقة في جرائم مثل التصيد الاحتيالي أو التنمُّر الإلكتروني.

تعتمد برمجيات التجسس على عدة طرق لتحقيق أهدافها، مثل تتبُّع ما يكتبه المستخدِم على لوحة المفاتيح لسرقة كلمات المرور، أو الدخول إلى مُحرّكات الأقراص لسرقة الصور والبيانات الأخرى. واللافت أن هذه البرمجيات لا تُدمِّر الملفات، بل تكتفي بسرقتها لتبقى غير ملحوظة.

1. What Is a Worm?. Follow link: https://www.cisco.com/c/en/us/products/security/what-is-a-worm.html.

يتميز التجسُّس الإلكتروني عن الهجمات السيبرانية الأخرى بعدة جوانب؛ من أهمها: السرية. ففي حالة هجوم الفدية، يتم إعلام المستخدِم بعد تثبيت البرمجية الخبيثة بأن بياناته قد تم تشفيرها، ولن يتم استردادها إلا بعد دفع الفدية. أما في حالة برمجيات التجسس، فإن المهاجم لا يُبلّغ الضحية، وقد ينتهي الهجوم دون أن يدرك المستخدم أن بياناته قد سُرقت[1].

حصان طروادة Trojan

يُعدّ "حصان طروادة" من أكثر البرمجيات الضّارَّة شهرة وانتشاراً؛ حيث يُعتمَد عليه في تنفيذ العديد من الجرائم الإلكترونية؛ نظراً لسهولة تثبيته على جهاز الضحية. ويمكن أن يتم تحميله على الجهاز دون عِلْم المستخدِم عند تنزيل برامج أو ألعاب أو ملفات موسيقية من مواقع غير موثوقة. وبمجرد تثبيته، يبدأ البرنامج في تعديل إعدادات الجهاز وسرقة بيانات المستخدِم. ويوجد العديد من الأنواع المختلفة لبرنامج حصان طروادة، ولكنها جميعاً تشترك في نفس آلية العمل؛ حيث تَستغل ضَعْف أمان المستخدم لاختراق الجهاز وسرقة المعلومات[2].

برمجيات الإعلانات المتسللة Adware

تُعدّ الإعلانات جزءاً أساسياً من تجربة الإنترنت؛ حيث تعتمد الشركات على جمع معلومات حول مستخدمي الإنترنت لتوجيه إعلانات مخصَّصة بناءً على اهتمامات كلّ فرد. ومع ذلك، يستغل المجرمون الرقميون هذه الإعلانات لتنفيذ هجماتهم، من خلال تضمين برمجيات خبيثة في الإعلانات، مما قد يؤدي أحياناً إلى اختراق المتصفّح بهدف التلاعب بمحركات البحث ومراقبة أنشطة الشبكة.

تشمل التأثيرات السلبية لبرمجيات الإعلانات المتسللة ما يلي:

- **إبطاء الحاسوب:** تؤدي هذه البرمجيات إلى استهلاك جزء كبير من قدرة المعالج وسرعة الإنترنت، مما يبطئ أداء الجهاز.
- **استهلاك موارد المعالج:** تستهلك الإعلانات المتسللة مساحة كبيرة من الذاكرة، مما يؤثّر سلباً على الأداء العام للجهاز[3].

1. Spyware: What It Is and How to Protect Yourself. Follow link: https://usa.kaspersky.com/resource-center/threats/spyware.
2. Emma McGowan, Trojan viruses: Detecting and removing, May 2024. Follow link: https://us.norton.com/blog/malware/what-is-a-trojan.
3. ADWARE. Follow link: https://www.malwarebytes.com/adware.

- **الهجمات بالإعلانات:** يمكن أن تكون الإعلانات مصدراً للتهديد الإلكتروني؛ حيث يتمكّن المجرمون من تثبيت برمجيات خبيثة على أجهزة الضحية، لكن هذا يحدث فقط إذا قام المستخدِم بفتح نوافذ الإعلانات، لذا فإن تجاهلها يُعدّ وسيلة حماية فعَّالة.

علامات الإصابة بالبرمجيات الضّارَّة

- بطء أداء الحاسوب.
- إعادة توجيه المتصفح؛ حيث يتمّ نَقْل المستخدِم خلال تصفُّح موقع ويب ما إلى موقع آخر دون رغبته.
- تحذيرات من تهديدات سيبرانية وهمية مصحوبة بطلب شراء برامج لإصلاح الخلل.
- مواجهة مشكلات خلال إيقاف تشغيل جهاز الحاسوب أو بَدْء تشغيله.
- ظهور الإعلانات المنبثقة بشكلٍ متكرّر.
- انخفاض غير مبرَّر في مساحة التخزين؛ وذلك لأن العديد من أنواع البرمجيات الضّارَّة تحتوي على ملفات كبيرة تشغل مساحة التخزين[1].
- ظهور منشورات غامضة على وسائل التواصل الاجتماعي دون تحكم المستخدم.
- تشغيل البرامج وإغلاقها دون موافقة المستخدم.
- اختفاء الملفات بشكل عشوائيّ من جهاز الحاسوب.
- زيادة في نشاط المستخدِم على الإنترنت بشكل غير مُبرَّر، والسبب هو عمل البرمجيات الضّارَّة خلف الكواليس لخرق الجهاز.

1. 19 signs of malware + how to cure the symptoms, November 2022. Follow link: https://us.norton.com/blog/malware/signs-of-malware.

طرق الحماية من البرمجيات الضّارّة

- تحديث نظام التشغيل والتطبيقات بانتظام؛ لسدّ أيّ ثغرات قد يشنّ من خلالها مجرمو الإنترنت هجومهم.
- عدم الضغط على أيّ روابط تظهر في نوافذ منبثقة خلال تصفُّح الإنترنت، والاكتفاء بإغلاق الرسالة.
- تحديد عدد التطبيقات المثبَّتة على الأجهزة، والاكتفاء بالمهم منها فقط، وإلغاء تثبيت الباقي.
- استخدام أحد حلول أمان الأجهزة المتوفرة لأنظمة التشغيل؛ للتأكد من أن الجهاز مستعدّ لمواجهة أيّ تهديد سيبراني.
- عدم إعارة الأجهزة الإلكترونية، مع التحقُّق من الإعدادات؛ لأنه في حال ظهور تطبيق جديد بشكل مفاجئ قد يكون علامة على وجود برنامج تجسُّس.
- عمل نسخة احتياطية من البيانات بانتظام.
- التأكُّد من تنزيل التطبيقات التي تم التحقُّق منها فقط، مع قراءة مراجعات التطبيقات، واستخدام متاجر التطبيقات الرسمية فقط[1].
- التحقُّق من الحسابات المصرفية والبيانات المالية بانتظام.

1. Protect yourself from malware. Follow link: https://support.google.com/google-ads/answer/2375413?hl=en.

كيفية إزالة البرمجيات الضّارَّة من جهاز الحاسوب

- قطع الاتصال بشبكة الإنترنت.
- ثم الدخول على الوضع الآمِن.
- البدء في مراقبة الموارد على الجهاز بحثاً عن التطبيقات الضّارَّة.
- إكمال عملية الفحص باستخدام برنامج مكافحة الفيروسات.
- تنظيف متصفّح الويب، ومسح ذاكرة التخزين المؤقتة.
- تغيير جميع كلمات المرور.

هل تعلم؟

71% من جميع خروقات البيانات لها دوافع مالية.

ثالثاً: خروقات البيانات والجرائم الإلكترونية ضد المرأة

خلال اتصالها بالإنترنت قد تتعرَّض المرأة لأنواع متعددة من الجرائم الإلكترونية الناتجة بالأساس عن خروقات البيانات الشخصية، ومنها:

- التشهير عبر الإنترنت، من خلال الكشف عن تفاصيل خاصة بها أو صور مُتلَاعَب بها للحصول على خدمات غير مشروعة في المقابل.
- القرصنة الإلكترونية، يستخدم مجرمو الإنترنت البيانات الشخصية للنساء في تنفيذ معاملات مالية غير قانونية أو أي معاملات أخرى غير قانونية [1].
- المطاردة الإلكترونية، ويُقصَد بها التطفل على الحسابات الشخصية للنساء عبر مواقع التواصل الاجتماعي، ومحاولة الاتصال بهن لأغراض غير مشروعة، أو إرسال رسائل تهديد عبر الدردشات.

هل تعلم؟

تتعرَّض النساء في المراحل العمرية بين 18 و24 عاماً، لأنواع معينة من المضايقات عبر الإنترنت؛ حيث يتعرَّض 26% منهن للمطاردة عبر الإنترنت.

1. Cyber Crime Against Women. Follow link: https://www.geeksforgeeks.org/cyber-crime-against-women/.

02

الفصل الثاني
السلامة الرقمية العـــــائـــــلية

- أولاً: **السلامة الرقمية العائلية Family Cyber protection.**
- ثانياً: **السلامة الرقمية للمرأة.**
- ثالثاً: **دور الأسرة في السلامة الرقمية للأبناء.**
- رابعاً: **ما الخطوات التي يجب اتباعها عند سرقة الهوية؟**

أولاً: السلامة الرقمية العائلية Family Cyber protection

يترافق التطور التكنولوجي المتسارع مع تطوُّر التهديدات السيبرانية التي تُواجه مختلف شرائح المجتمع كافة، ما ينسحب بشكلٍ مباشر على الأسرة؛ حيث أصبحت الجرائم الإلكترونية أكثر احترافاً وأشد ضرراً، نظراً لتنوع الأساليب التي يعتمد عليها مجرمو الإنترنت في تنفيذ هجماتهم. ما يُعزّز من أهمية السلامة الرقمية العائلية، بما ينعكس إيجاباً على سلامة أفراد الأسرة الرقمية وسلامة بياناتهم الشخصية.

إذًا تستهدف السلامة الرقمية اتباع قواعد وإجراءات لحماية أجهزة الحاسوب والخوادم والأجهزة المحمولة والأنظمة والشبكات والبيانات من الهجمات التي تُنفَّذ بواسطة البرمجيات الضّارَّة. وبالنسبة للشبكات، فإن السلامة الرقمية تستهدف تأمين شبكة الحاسوب من تسلل المهاجمين الإلكترونيين أو البرمجيات الضّارَّة إليها. وعلى مستوى التطبيقات فالسلامة الرقمية تعني التأكد من خلوّ الأجهزة الإلكترونية والبرامج الموجودة عليها من الثغرات الأمنية والبرمجيات الضّارَّة، مما يحمي البيانات في أثناء تخزينها أو نقلها من الفقد أو الحجب مقابل دفع فدية.

وتشتمل السلامة الرقمية أيضاً على التعلُّم؛ للتأكد من الاستخدام الصحيح لشبكة الإنترنت، وما تحتويه من تطبيقات وبرامج ومواقع ويب، والتدرُّب على كيفية التعامل مع رسائل البريد الإلكتروني المشبوهة، وغيرها من أمور تُهدِّد سلامة أفراد الأسرة.

ثانياً: السلامة الرقمية للمرأة

- يُنصَح بعدم ترك كاميرا الويب متصلة؛ لوجود تطبيقات قادرة على تشغيل الكاميرا، وتسجيل التحركات دون عِلْم المرأة، لهذا يُفضَّل تعطيل إذن الكاميرا، وإبقاء عدستها مغلقة أو مغطاة عند عدم استخدامها[1].
- الحد من مشاركة الرسائل أو الصور أو المعلومات الشخصية؛ لأن هذه البيانات الشخصية يمكن استخدامها مِن قِبَل المجرمين في عمليات التصيد الاحتيالي.
- يُشكّل أيّ جهاز مزوّد بـ"خدمة الموقع" خطراً على تسريب التفاصيل الشخصية، مثل مكان الوجود؛ لذا ينبغي توخّي الحذر وتعطيل تلك الخاصية.
- تحديث كافة أنظمة التشغيل الموجودة على الأجهزة الإلكترونية بانتظام، واستخدام برامج مكافحة الفيروسات.
- قراءة سياسة الخصوصية وشروط الخدمة المستخدَمة عبر الإنترنت.
- الهدايا المجانية على شكل عروض وصفقات غالباً تكون مليئة بالفيروسات وبرمجيات التجسُّس.
- حظر الأشخاص الذين يثيرون الشكوك حولهم على وسائل التواصل الاجتماعي.
- في حال التعرُّض لأيّ من أنواع الجرائم الإلكترونية السابق ذِكْرها، على المرأة إبلاغ وحدة مكافحة الجرائم الإلكترونية بوزارة الداخلية.

1. Cyber safety for women. Follow link: https://us.norton.com/blog/privacy/cyber-safety-for-women.

ثالثاً: دور الأسرة في السلامة الرقمية للأبناء

دور الأسرة في حماية الأبناء من مخاطر الذكاء الاصطناعي (AI)

اليوم، ومع الثورة التي يشهدها الذكاء الاصطناعي؛ تحوَّل إلى جزءٍ رئيسٍ في الحياة اليومية للأفراد، مثل "روبوتات الدردشة"، والتي أصبح يستخدمها صغار السن، وتثير فضول الأطفال مستفيدين منها في أداء المهام المدرسية وإجراء الدردشات.

وعلى الرغم من المنافع العائدة من استخدام الذكاء الاصطناعي؛ إلا أنه قد يُشكّل خطراً يتمثّل في فقدان خصوصية البيانات والتهديدات السيبرانية، والمحتوى غير اللائق لليافعين والأطفال[1]. ويتمثل هذا الخطر أيضاً في ظهور تطبيقات مجهولة تبدو كالأصلية تُستخدَم في إجراء التعديلات على الصور، وبالطبع يتطلب الأمر الولوج إلى القسم الخاص بالصور على الأجهزة الإلكترونية والهواتف الذكية وتحميل الصور لبدء عملية التعديل، لهذا يُنْصَح الآباء بتتبُّع أطفالهم للتأكُّد من نوعية التطبيقات المستخدَمة لتحذيرهم من تلك المجهولة أو غير المعتمدة؛ حيث قد تُعرِّض المعلومات الشخصية مثل الهوية والعنوان وغيرهما لخطر الخرق أو السرقة.

لذا يُنصَح الآباء والأمهات بالتحدُّث باستمرار مع أبنائهم، وإقامة علاقات وثيقة معهم؛ ليستطيعوا متابعة نشاطهم على الإنترنت عامة، وتطبيقات الذكاء الاصطناعي بوجه خاص. كما يُنْصَح الآباء والأمهات بإبعاد أبنائهم عن الألعاب التفاعلية التي تُغرقهم برسائل البيع؛ مما يجعلهم هدفاً محبّذاً للحملات الإعلانية. إضافةً إلى إمكانية استخدام تلك الألعاب في تنفيذ عمليات احتيالية وقرصنة وإنشاء صور مزيفة للأبناء بواسطة التزييف العميق واستنساخ الصوت مقابل دفع الأموال.

لهذا يُنْصَح بإجراء نقاش حول الخصوصية والسلامة الرقمية مع المراهقين -تحديداً- لتعريفهم بمخاطر الذكاء الاصطناعي، وما يحتاجون إلى معرفته من معلومات عن ذلك. وكذلك التحدُّث معهم عن الانتحال، وشرح كيفية القيام به عبر تعريفهم بعدم قانونية نشر صور أو بيانات دون علمهم.

1. Tiffany Munzer, How Will Artificial Intelligence (AI) Affect Children?. Follow link: https://www.healthychildren.org/English/family-life/Media/Pages/how-will-artificial-intelligence-AI-affect-children.aspx

أرقام وحقائق

- في استطلاع للأمم المتحدة، كشف 80% من الشباب عن تفاعلهم مع الذكاء الاصطناعي عدة مرات في اليوم.
- يوجد على Facebook Messenger وحده أكثر من 300.000 روبوت دردشة قيد التشغيل، ليست جميعها آمِنة.

◆ دور الأسرة في حماية الأبناء من مخاطر الألعاب الإلكترونية

مما يثير المخاوف من الألعاب الإلكترونية: هو قضاء الأطفال واليافعين الوقت مع الغرباء، والتواصل معهم عبر الدردشات الصوتية والنصية غير الخاضعة للإشراف، الأمر الذي استغله مجرمو الإنترنت لبناء الثقة الافتراضية معهم للحصول على البيانات الشخصية، واقتراح روابط احتيالية، بهدف تنزيل برمجيات ضارَّة في صورة ألعاب مقترَحة لبدء تنفيذ هجماتهم.

ومما يزيد من المخاوف: ظهور ألعاب الواقع المعزّز والواقع الافتراضي، التي تتطلّب يقظة الآباء والأمهات ومراقبة سلوك الأبناء دائماً لرَصْد أيّ تغيُّرات به.

ولتجنُّب تلك المخاطر يُنْصَح بالآتي:

- تجنُّب استخدام معلومات شخصية في الألعاب ومنتدياتها مثل: الاسم أو الموقع.
- تجنُّب تنزيل البرامج والألعاب من مصادر غير موثوقة.
- عند التخلُّص من جهاز الألعاب إما بالبيع وإما التخلي، يجب التأكُّد من حذف معلوماتك الشخصية.
- تثبيت واستخدام VPN عند ممارسة الألعاب.

دور الأسرة في حماية الأبناء من مخاطر المعاملات المالية

يلجأ بعض الآباء لمنح أبنائهم بطاقات ائتمانية خاصة بهم لإجراء المعاملات المالية بأنفسهم، أو إعارتهم بطاقات الآباء، إلا أن هذا قد يجعلهم ضحية عمليات احتيالية؛ حيث يستغل مجرم الإنترنت ثقة الأطفال، ثم يطلب تفاصيل البطاقة، أو تحويل الأموال إلى حساباته، أو وعدهم بجوائز قيّمة. ويُفضّل توعية الأبناء لتفادي الوقوع فريسة للهجمات الإلكترونية المختلفة، مع مراقبة إنفاقهم اليومي وتحديد حدود السحب من البطاقات، ومراجعة بياناتها وأرصدتها بانتظام، ولتجنُّب فقدانهم للبطاقة يُوصَى بتثبيت التطبيقات على هواتفهم بدلاً من البطاقات البلاستيكية.

دور الأسرة في حماية الأبناء من مخاطر التنزيلات الضّارَّة

في حال عدم إتاحة أحد التطبيقات للأبناء؛ فإنهم قد يلجؤون للبحث عن بديل، والذي غالباً ما يكون نسخة غير آمِنَة من التطبيق.

رابعاً: ما الخطوات التي يجب اتباعها عند سرقة الهوية؟

تحدث سرقة الهوية عندما يحصل مُجرم ما على معلومات شخصية للآخرين؛ بهدف استخدامها في ارتكاب المزيد من الجرائم الإلكترونية؛ كالاحتيال عبر الإنترنت. وتتضمَّن هذه المعلومات اسم الشخص الضحية والعنوان، ورقم الهاتف، والبيانات المالية كأرقام البطاقات الائتمانية، ويتم الأمر غالباً نتيجة خرق البيانات.

وتحدث سرقة الهوية نتيجة عدة ممارسات خاطئة يقوم بها المستخدمون، أو نتيجة ثغرات رقمية يستغلها المجرمون، وفيما يلي تبيان لهذه الممارسات والثغرات:

- الاستخدام غير المسؤول لوسائل التواصل الاجتماعي كمشاركة المعلومات الخاصة.
- خرق البريد الإلكتروني نتيجة إعادة استخدام كلمة المرور نفسها في عدة مواقع وصفحات.
- شراء مجرمي الإنترنت المعلومات الشخصية للضحايا عبر الإنترنت المظلم.
- خرق شبكات Wi-Fi الخاصة أو استخدام الشبكة العامة دون تأمين البيانات الحساسة.
- سرقة الهاتف الذكي أو جهاز الحاسوب تُعرّض صاحب الجهاز لخطر خرق البيانات، ومِن ثَم سرقة الهوية.
- بعض مجرمي الإنترنت يقومون بقشط البطاقات الائتمانية من خلال تركيب جهاز فوق قارئ البطاقات الموجود على ماكينة الصراف الآلي لسرقة البيانات المخزنة على الشريط المغناطيسي للبطاقة وتخزينها.

أما عن الخطوات التي يجب اتباعها عند سرقة الهوية فهي كالآتي:

- تتزايد مخاطر سرقة الهوية عبر الخدمات الشائعة عبر الإنترنت مثل: مواقع التسوق عبر الإنترنت، والخدمات المصرفية، ويمكن التأكُّد من ذلك عبر ملاحظة علامات مثل: إجراء عملية شراء دون عِلْم المستخدِم أو تغيير بيانات التواصل مع الجهات الرسمية كالبنوك[1].
- فور اكتشاف سرقة الهوية؛ ينبغي إبلاغ جهات إصدار البطاقات الائتمانية؛ لغلق الحساب، مع ضرورة تغيير جميع كلمات المرور.
- ضع تنبيهاً بشأن الاحتيال في تقرير الائتمان الخاص بك، فهذا يُعرقل أيّ محاولات للمحتال لفتح حساب جديد بالهوية المسروقة دون رجوع الجهة المالية إلى الضحية أولاً للتأكُّد.
- مراجعة تقارير الائتمان فور تفعيل التنبيه، ويُنْصَح بمراجعة كل تقرير من تقارير الائتمان الخاصة مجدداً خلال العام التالي للتحقُّق من عدم وجود أيّ مؤشرات مستمرة لسرقة الهوية.
- إبلاغ وحدة مكافحة الجرائم الإلكترونية بوزارة الداخلية.
- الاتصال بمُزوّدي الخدمات وشركات الهاتف للتأكيد على تعرُّض هويتك للسرقة لإفشال محاولة المحتال لاستغلالها أو فتح حساب بالهوية المسروقة.
- استخدِم برنامج مكافحة فيروسات للتعامل مع التهديدات الشائعة والمعقَّدة مثل: الفيروسات والبرمجيات الضّارَّة وبرمجيات الفدية، وتطبيقات التجسُّس والقرصنة.

1. Identity theft and identity fraud: What to do if your identity is stolen. Follow link: https://www.kaspersky.com/resource-center/threats/what-to-do-if-your-identity-is-stolen-a-step-by-step-guide.

التمارين تعتمد على المادة العلمية المقدَّمة في سياق هذا الكتيب، وهي مذكورة هنا بدون حل، وتم إرفاق الحل في نهاية الكُتَيِّب.

التمرين الأول

• اختر الإجابة الصحيحة

1. من أجل توفير الحماية السيبرانية يُنصَح بعدم استخدام ..... لأنها تساعد مجرمي الإنترنت في التسلل إلى الأجهزة المربوطة بها؛ من خلال هجمات التنصت الوسيط man-in-the-middle attacks.

1. بيانات الاتصال.
2. شبكات Wi-Fi العامة.
3. كلمات المرور.

2. تتعرض المرأة لمضايقات عبر الإنترنت منها .....

1. الشائعات.
2. التنمر الإلكتروني.
3. المطاردة الإلكترونية.
4. جميع ما سبق.

3. إحدى علامات الإصابة بالبرمجيات الضّارَّة .....

1 عمليات إعادة توجيه المتصفّح.

2 ظهور الملفات بشكل عشوائي.

3 انخفاض في نشاط المستخدِم على الإنترنت.

4. يقوم مجرمو الإنترنت بجمع معلومات تتضمّن اسم المستخدم وكلمة المرور المسروقة، لاختبارها على مواقع الويب للوصول إلى حسابات المستخدِمين فيما يُعرَف بهجمات .....

1 القوة الغاشمة.

2 حشو بيانات الاعتماد.

3 أحصنة طروادة.

5. نوع من هجمات القوة الغاشمة يحتاج فيه المهاجم لمعرفة مسبقة باسم الضحية ليبدأ في تجربة كلمات المرور المحتملة .....

1 هجوم القوة الغاشمة العكسي.

2 هجوم القوة الغاشمة الهجين.

3 هجوم القاموس.

6. من العلامات التحذيرية للتعرف على مواقع الويب المزيفة .....

1. البعد عن مخاطبة المشاعر.
2. اعتدال الأخطاء الإملائية والنحوية.
3. محاكاة أسماء النطاقات الأصلية.

7. جميع متصفحات الويب مثل Firefox & Chrome تحتوي على ما يسمى .....

1. شهادة الضمان.
2. شهادة الأمان SSL.
3. شهادة الموثوقية.

8. في حال زيارة موقع احتيالي ينبغي .....

1. مواصلة الحديث والاتصال مع المحتال للتعرُّف على أهدافه.
2. تحديث كلمات المرور الخاصة بالحسابات المصرفية فقط.
3. البحث عن أيّ مدفوعات معلّقة أو مستمرة وإيقافها.

التمرين الثاني

اكتب كلمة (صحيح) بجانب العبارة الصحيحة، وكلمة (خطأ) بجانب العبارة الخاطئة، وفي حال الخطأ صحِّح العبارة

1. تفتقر ديدان الحاسوب إلى القدرة على نسخ نفسها من جهاز إلى آخر، وتحتاج للمستخدم لتبدأ الهجوم.
2. يتم تثبيت برمجيات التجسس Spyware على جهاز الحاسوب بعلم المستخدِم.
3. تتنكر برمجية أحصنة طروادة كتطبيقات غير ضارَّة لخداع المستخدمين، ودفعهم لتنزيلها واستخدامها على جهاز الحاسوب.
4. من علامات الإصابة بالبرمجيات الضّارَّة: انخفاض مساحة التخزين على الجهاز.
5. هجمات القوة الغاشمة من الأساليب الشائعة المستخدَمة في خروقات البيانات.

التمرين الثالث

أكمل العبارات الآتية

1. يتم التلاعب النفسي في عمليات احتيال تزوير المواقع من خلال عدة طرق، هي: ..... ، ..... ، .....
2. من العلامات التحذيرية الدالة على مواقع الويب المزيفة ..... ، ..... ، .....
3. يُنصَح للوقاية من هجمات احتيال إلغاء تنشيط الحساب بـ ..... ، ..... ، .....
4. من البيانات المُستهدَفة في هجمات التصيد ..... ، ..... ، .....
5. تحدث خروقات البيانات بسبب نقاط الضعف في ..... ، .....

حلّ التمارين والتدريبات

السؤال

التمرين الأول: اختر الإجابة الصحيحة

الإجابة

1. شبكات Wi-Fi العامة.
2. جميع ما سبق.
3. عمليات إعادة توجيه المتصفّح.
4. حشو بيانات الاعتماد.
5. هجوم القوة الغاشمة الهجين.
6. محاكاة أسماء النطاقات الأصلية.
7. شهادة الأمان SSL.
8. البحث عن أيّ مدفوعات معلَّقة أو مستمرة وإيقافها.

السؤال

التمرين الثاني: اكتب كلمة (صحيح) بجانب العبارة الصحيحة، وكلمة (خطأ) بجانب العبارة الخاطئة، وفي حال الخطأ صحِّح العبارة.

الإجابة

1. **خطأ.**

تتسم ديدان الحاسوب بقدرتها على نسخ نفسها من جهاز إلى آخر، مستغلّة في ذلك الضعف الأمني في برنامج ما أو نظام تشغيل، ولا تحتاج للمستخدم لتبدأ الهجوم.

2. **خطأ.**

يتم تثبيتها على جهاز الحاسوب دون عِلْم المستخدِم؛ بهدف جمع المعلومات الشخصية، أو رصد عادات تصفح الإنترنت، ونقلها إلى المهاجم، مما يُمكنه من مراقبة جميع أشكال الاتصالات على الجهاز المستهدَف.

3. **صحيح.**

4. **صحيح.**

5. **صحيح.**

السؤال

التمرين الثالث: أكمل العبارات الآتية

الإجابة

1. يتم التلاعب النفسي في عمليات احتيال تزوير المواقع من خلال عدة طرق، هي:
   - العروض السريعة أو التنبيهات التي تستعجل الضحية على اتخاذ إجراء عاجل دون تفكير جيد.
   - الوعود الجذابة مثل بطاقات الهدايا المجانية أو كسب المال.
   - التنبيهات الكاذبة بوجود فيروس ما يدفع الضحية إلى التدخُّل وتنفيذ المطلوب في الرسائل دون تفكير.

2. من العلامات التحذيرية الدالة على مواقع الويب المزيفة مخاطبة المشاعر عبر الإلحاح أو إثارة الخوف، ضعف جودة تصميم الموقع، كثرة الأخطاء الإملائية والنحوية.

3 يُنصَح للوقاية من هجمات احتيال إلغاء تنشيط الحساب بـ عدم فتح المرفقات أو الروابط الموجودة في رسائل البريد المشبوهة، إجراء جميع التنزيلات من المتاجر الرسمية، تثبيت برنامج مكافحة فيروسات وتحديثه باستمرار.

4 من البيانات المُستهدَفة في هجمات التصيد كلمات المرور، أرقام بطاقات الائتمان، معلومات الحسابات المصرفية.

5 تحدث خروقات البيانات بسبب نقاط الضعف في التكنولوجيا، سلوك المستخدم.

المراجع

1. What is a data breach?. Follow link: https://www.ibm.com/topics/data-breach
2. How Data Breaches Happen & How to Prevent Data Leaks. Follow link: https://www.kaspersky.com/resource-center/definitions/data-breach
3. Data breaches worldwide - Statistics & Facts. Follow link: https://www.statista.com/topics/11610/data-breaches-worldwide/#topicOverview.
4. Lottery scams. Follow link: https://www.actionfraud.police.uk/a-z-of-fraud/lottery-scams
5. What Are Scam Websites and How To Avoid Scam Websites. Follow link: https://www.kaspersky.com/resource-center/preemptive-safety/scam-websites
6. Ryan Toohil, How To Identify Fake Websites: 11 Warning Signs, November 2023. Follow link: https://www.aura.com/learn/how-to-identify-fake-websites
7. Malware. Follow link: https://www.malwarebytes.com/malware
8. What is Malware? Follow link: https://www.mcafee.com/en-us/antivirus/malware.html

9. What Is a Worm? Follow link: https://www.cisco.com/c/en/us/products/security/what-is-a-worm.html
10. Spyware: What It Is and How to Protect Yourself. Follow link: https://usa.kaspersky.com/resource-center/threats/spyware
11. Emma McGowan, Trojan viruses: Detecting and removing, May 2024. Follow link: https://us.norton.com/blog/malware/what-is-a-trojan
12. ADWARE. Follow link: https://www.malwarebytes.com/adware
13. 19 signs of malware + how to cure the symptoms, November 2022. Follow link: https://us.norton.com/blog/malware/signs-of-malware
14. Protect yourself from malware. Follow link: https://support.google.com/google-ads/answer/2375413?hl=en
15. Cyber Crime Against Women. Follow link: https://www.geeksforgeeks.org/cyber-crime-against-women/
16. Cyber safety for women. Follow link: https://us.norton.com/blog/privacy/cyber-safety-for-women
17. Tiffany Munzer, How Will Artificial Intelligence (AI) Affect Children?. Follow link: https://www.healthychildren.org/English/family-life/Media/Pages/how-will-artificial-intelligence-AI-affect-children.aspx
18. Identity theft and identity fraud: What to do if your identity is stolen. Follow link: https://www.kaspersky.com/resource-center/threats/what-to-do-if-your-identity-is-stolen-a-step-by-step-guide

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative