التزوير والاحتيال عبـــر الإنترنـــت

الفئة المستهدَفة
كبار القدْر

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

التزوير والاحتيال عبر الإنترنت

الفئة المستهدفة: كبار القَدْر

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.

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

مُقـــدّمة

في ظلّ الطّفرة الرّقميّة التي يشهدها عالمنا اليوم، تداول على مرأى ومسمع منّا جميعًا الكثير من المُصطلحات المُستحدثة ذات الصّلة بعالم الجريمة، كما هو الحال مع الجرائم الإلكترونيّة التي تستهدف أجهزة الحاسوب والشّبكات، وتحاول استغلالها في القيام بأنشطة إجراميّة لكسب المال أو التّسبُّب في ضرر لمالكيها لأسباب شخصيّة، وتقع مُعظم الجرائم الإلكترونيّة على أيدي القراصنة أو الهاكرز.

وتتعدّد أنواع وأشكال الجريمة الإلكترونيّة، فهناك الاحتيال عبر البريد الإلكترونيّ والإنترنت وتزوير الهُويّة، حيث تتمّ سرقة المعلومات الشّخصيّة واستخدامها، وكذلك سرقة البيانات الماليّة أو بيانات الدّفع بالبطاقة، ويُطلق على هذا النّوع من الجرائم أيضًا (هجمات برمجيات الفدية). إضافةً إلى جرائم انتهاك حُقُوق النّشر والتّأليف، وبيع السّلع غير المشروعة عبر الإنترنت.

ووفقًا لتقرير حالة مُرُونة الأمن السّيبرانيّ لعام 2021م من Accenture، زادت الهجمات الرّقميّة بنسبة 31% بين عامي 2020م – 2022م، وزاد عدد الهجمات لكُلّ شركة من 206 إلى 270 على أساس سنويّ، وبالطّبع تلك الهجمات تُؤثّر على الأفراد أيضًا لأنّ العديد من الشّركات تحتفظ ببيانات مهمّة ومعلومات شخصيّة خاصّة بالعُملاء. فيُمكن لهُجُوم واحد، سواء كان خرقًا للبيانات أو برمجيّات خبيثة أو برنامج طلب فدية أو هُجُوم حرمان من الخدمات، أن يُكلّف الشّركات من جميع الأحجام ما مُتوسّطه 200 ألف دولار[1].

هل تعلم؟

تحميل التطبيقات من متاجر معروفة يُقلّل من مخاطر التعرُّض للاحتيال الإلكتروني

وفي عام 2021م نشرت Javelin Strategy & Research دراسةً عن احتيال الهُويّة أوضحت فيها أنّ خسائر هذا النّوع من الجرائم الإلكترونيّة بلغت 56 مليار دولار[2]؛ أمّا بالنّسبة للأفراد فقد يكون تأثير الجريمة الإلكترونيّة عميقًا، مُخلّفًا ضررًا ماليًّا في المقام الأوّل، وأيضًا فُقدان الثّقة والإضرار بالسُّمعة.

1. How aligning security and the business creates cyber resilience, State of Cybersecurity Resilience 2021. On site: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-165/accenture-state-of-cybersecurity-2021.pdf
2. Report: The 2021 Identity Fraud Study, BY ALEX ROLFE, April 2021, on site: https://www.paymentscardsandmobile.com/report-the-2021-identity-fraud-study/

01

الفصل الأول

مفهـــوم التّزوير والاحتـــــيال عبر الإنترنت وأنواعه

- **أوّلًا:** مفهوم الاحتيال عبر الإنترنت
- **ثانيًا:** أسباب الوُقُوع ضحيّةً للاحتيال عبر الإنترنت
- **ثالثًا:** أنواع وأشكال الاحتيال عبر الإنترنت

أوّلًا: مفهوم الاحتيال عبر الإنترنت

الاحتيال عبر الإنترنت هو أحد أشهر أنواع الجرائم الإلكترونيّة انتشارًا، وممّا ساعد على انتشاره في السّنوات الأخيرة تزايُد عدد مُستخدمي الإنترنت وتطبيقاته المُختلفة، كوسائل الدّفع الإلكترونيّ وانتشار وسائط التّواصل الاجتماعيّ وغيرها، إذ زادت جرائم التّصيُّد والاحتيال على الأفراد بالتّزامُن مع ارتفاع أعداد الأشخاص على شبكة الإنترنت وتداخُلها في جميع جوانب الحياة الاقتصاديّة والتّجاريّة والسّياسيّة والاجتماعيّة، فأصبح العمل والتّسوُّق والتّرفيه أمورًا يمكن إجراؤها على شبكة الإنترنت بسهولة وسُرعة من خلال هاتف ذكيّ مربوط بشبكة إنترنت.

يُعدّ الاحتيال عبر الإنترنت من أسهل الجرائم الإلكترونيّة ارتكابًا كونه لا يحتاج إلى خُبراء أو برامج مُتخصّصة أو مُتخصّصين في مجال الهاكرز والقرصنة، بل يُمكن تنفيذ هذه الجريمة عن طريق حسابات مواقع التّواصل الاجتماعيّ عبر انتحال الشّخصيّة والاحتيال عبر غُرف الدّردشة؛ ويُشار إلى الاحتيال عبر الإنترنت على أنّه نوع من أنواع الخداع والحيل التي تتمّ على شبكة الإنترنت، وغالبًا ما تحدث هذه الجرائم في غُرف الدّردشة أو عبر البريد الإلكترونيّ أو على المُنتديات أو مواقع الإنترنت (الويب)، والهدف من هذه الجرائم هو الاحتيال على العُملاء والمُستخدمين عن طريق سرقة الأموال والمعلومات الشّخصيّة المهمّة وغيرها من البيانات؛ وعادةً تكون هجمات الاحتيال عبر الإنترنت بهدف التّجسُّس أو انتحال الشّخصيّة أو الحصول على معلومات حساب المُستخدمين في مراكز مهمّة أو على صلة بأشخاص مهمّين (أي لأسباب شخصيّة)، وقد تكون لسرقة الأموال من الحسابات المصرفيّة وبطاقات الدّفع الإلكترونيّة[1].

حقائق ومعلومات

تتكوّن البصمة الرّقميّة من أنشطة مختلفة على الإنترنت، مثل التّسوُّق والتسجيل في المواقع.

1. Internet Fraud, Australian Federal Police (AFP). on site: https://police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf

وتتمّ عمليّة الاختراق (الاحتيال عبر الإنترنت) عادةً عند زيارة الأفراد للمواقع الإلكترونيّة أو غُرف الدّردشة (الماسنجر) أو المتاجر الإلكترونيّة أو المُدوّنات أو التّطبيقات الذّكيّة، وفي هذه المرحلة يتمّ الإيقاع بالضّحيّة عبر نصب أحد الفخاخ الإلكترونيّة له، ليقوم المُجرم بتنفيذ بقيّة خُطّته غير المشروعة عن طريق الهُجُوم على بيانات الأشخاص وحسابات العُملاء.

تعريف جريمة الاحتيال عبر الإنترنت

تُعرف جريمة الاحتيال عبر الإنترنت بأنّها التّلاعُب العمد بمعلومات وبيانات تُمثّل قيمًا ماديّة يختزنها نظام الحاسب الآليّ أو الإدخال غير المُصرّح به لمعلومات وبيانات صحيحة أو التّلاعُب في الأوامر والتّعليمات من خلال عمليّة البرمجة أو أيّة وسيلة أُخرى، من شأنها التّأثير على الحاسب الآليّ حتّى يقوم بعمليّاته بناءً على هذه الأوامر أو البيانات أو التّعليمات من أجل الحُصُول على ربح غير مشروع وإلحاق ضرر بالآخرين. ويُمكن إدارة العمليّة الإجراميّة من مكان بعيد عن مسرح الجريمة ذاتها، أو من خارج حدود الدّولة مثل جرائم الاحتيال الخاصّة بترويج الموادّ غير المُلائمة وكذلك النّصب الإلكترونيّ[1].

وترتبط بالاحتيال عبر الإنترنت مجموعة من المفاهيم الأخرى، مثل مفهوم الاحتيال المعلوماتي، والذي يُقصد به: الخداع أو الغشّ المعلوماتيّ الذي يقوم على التّلاعُب في نُظُم المُعالجة الآليّة للمعلومات بغرض الحصول دون وجه حقّ على خدمات أو أموال أو أصول مُعيّنة؛ وكذلك مفهوم "الاحتيال أو النّصب الماليّ الإلكترونيّ" ويُقصد به: الاستيلاء على مال الآخرين بوسيلة يشُوبها الخداع؛ ممّا يتسبّب في سرقة هذا المال عن طريق أجهزة الحاسوب.

وهنا يقوم الجاني "المُهاجمُون الإلكترونيُّون" باستخدام تقنيّات حديثة بغرض التّلاعُب في البيانات المصرفيّة والمُستحقّات الماليّة، وكذلك الميزانيّات للشّركات لتحويل المال في أسرع وقت لحسابه الشّخصيّ، بالطّبع هذا النّوع من الهجمات الإلكترونيّة يُؤثّر سلبًا على الاقتصاد الوطنيّ فقد يُؤدّي إلى إفلاس البُنُوك والشّركات.

1. يونس الباشا، فايزة. الجريمة المُنظّمة في ظلّ الاتّفاقيّات الدّوليّة والقوانين الوطنيّة، دار النّهضة العربيّة للطّبع والنّشر والتّوزيع، 2001م، ص 21.

ثانيًا: أسباب الوُقُوع ضحيّةً للاحتيال عبر الإنترنت

تتعدّد الأسباب المُؤدّية إلى جرائم الاحتيال عبر الإنترنت، وغالبًا ما تكون بسبب الاستخدام الخاطئ لوسائل التّواصل الاجتماعيّ وشبكة الإنترنت، وعدم اتّباع قواعد التّعامل الآمِن مع الإنترنت، وعدم الوعي التّامّ بمفاهيم الأمن السّيبرانيّ والسّلامة الرّقميّة.

حقائق ومعلومات

يمكنك حماية بَصْمتك الرّقميّة بالتحقُّق من إعدادات الخصوصية وتجنُّب المواقع غير الآمِنة.

وفيما يلي تبيان لأهمّ العوامل والأسباب التي تُؤدّي إلى وُقُوع مُستخدمي الإنترنت ضحيّةً للاحتيال الإلكترونيّ:

- قلّة الوعي بأهمّيّة قواعد الاستخدام الآمِن للإنترنت.
- التّسرُّع في اتّخاذ القرار عند تصفُّح المواقع الإلكترونيّة، أو عند فتح رسائل البريد الإلكترونيّ، فقد يتسرّع المُستخدم في التّعامل مع أيّ رابط يجدُه أمامه، وهو أسلوب يتّبعه المُحتالون على الإنترنت لعدم إعطاء المُستهدفين الفُرصة للتّفكير أو التّحقُّق من مصداقيّة الرّسالة التي تلقّوها.
- الدُّخُول إلى مواقع إنترنت غير آمِنة، وعندها يتلقّى المُستخدم إشعارات أو رسائل وهميّة، غالبًا ما تكون تُشير إلى أنّ المُستخدم قد ربح أموالًا أو أجهزةً إلكترونيّةً، وتطلُب منه تزويدها ببيانات ومعلومات شخصيّة لتُسلّمه الهديّة، وفور إدخال المُستخدم لأيّ بيانات شخصيّة سيكون قد وقع ضحيّة الاحتيال.

- نشر معلومات شخصيّة على مواقع التّواصل الاجتماعيّ، وهذه المعلومات تُشكّل فُرصة للمُحتالين للإيقاع بالمُستخدمين، ومن خلالها وبالاعتماد على البصمة الرّقميّة للمُستخدم يُمكن الإيقاع به والاحتيال عليه.
- التّعامل مع متاجر إلكترونيّة مُزيّفة، تسعى لخداع المُستخدمين وسرقة أموال من بطاقات الدّفع الإلكترونيّة الخاصّة بهم.
- انتشار منصّات تبادُل العُملات الرّقميّة، مثل البيتكوين وغيرها، فحاليًا يوجد العديد من المنصّات لتبادُل هذا النّوع من العُملات، وبعضها يكون منصّات وهميّةً، تحتال على المُستخدمين، وقد تمنحُهم أحيانًا بعض الأموال بهدف كسب ثقتهم، ولاحقًا يتمّ خداعهم وسرقة أموالهم.
- انتحال المُحتالين لشخصيّات رسميّة أو شخصيّات عامّة، وهو ما يجذب أحيانًا بعض المُستخدمين للإنترنت، ولاحقًا يتم خداعهم.
- استغلال التّعاطف الإنسانيّ، قد يقوم بعض المُحتالين بانتحال صفة مُنظّمات أو أفراد يقومون بجمع تبرُّعات لحالات إنسانيّة حادّة، وبعض هذه الحالات تكون غايتها الاحتيال، لذلك لا يجوز دفع أيّ تبرُّعات أو مُساعدات إلّا لمُنظّمات معروفة وذات مواقع رسميّة وبمُوجب إيصالات مُصدّقة أصولًا.

هل تعلم؟

الشبكات العامَّة غير آمِنة، وقد تُعرِّضك لخطر الاختراق.

ثالثًا: أنواع وأشكال الاحتيال عبر الإنترنت

لا توجد أنواع ثابتة أو دائمة للاحتيال الإلكترونيّ، فغالبًا ما يسعى المُحتالون لتطوير أساليبهم، ولكنّه بشكل عامّ يتمّ عبر أدوات ووسائل رئيسة.

وفيما يلي تبيان لأهمّ هذه الأدوات والأنواع:

البريد الإلكترونيّ:

قد يصل إلى البريد الإلكترونيّ رسائل تتضمّن روابط مُسابقات أو جوائز ماليّة وعينيّة مُغريةً مثل: الهواتف الذّكيّة أو الحصول على فرصة قضاء العُطلة في إحدى الدُّول الخارجيّة، وبمُجرّد الضّغط على الرّابط يُطلب من مالك البريد إدخال بعض البيانات الشّخصيّة أو الماليّة مثل رقم بطاقته الائتمانيّة أو رقمه الوطنيّ أو رقم جواز السّفر... وغيرها من بيانات شخصيّة مُهمّة. وقد يُطلب منه أيضًا حوالة ماليّة ولو صغيرة من أجل الحصول على الجائزة. هذا الأمر يُعرّض المعلومات الشّخصيّة للخطر، ويزيد من فُرص سرقة المال من الحسابات الخاصّة.

ومن طُرُق الاحتيال عبر الإنترنت التي تُعدّ أكثر خداعًا ومكرًا، إرسال بريد إلكترونيّ مُزوّر يبدو كأنّه أُرسل من صديق أو جهة رسميّة في حين أنّه ليس سوى عمليّة تصيُّد إلكترونيّ؛ إذ يطلُب من الشّخص معلومات مُعيّنةً وحسّاسةً. على سبيل المثال: قد تُخبرك الرّسالة أنّك في حاجة لتغيير كلمة المرور على حساب "باي بال" لأنّ هناك مُحاولة لاختراقه، وتبدو الرّسالة كأنّها من الموقع الرّسميّ، ما يزيد من احتماليّة تنفيذ المطلوب وإدخال كلمة مُرُور جديدة، وهو ما يسمح باستخدامها من طرف جهة الاحتيال لسرقة المال[1].

1. What is email fraud? Cloudflare. On site: https://www.cloudflare.com/learning/email-security/what-is-email-fraud/

الهاتف الذّكيّ:

يتسبّب تثبيت تطبيقات غير آمِنة وكذلك الضّغط على روابط مجهولة (غير معلوم مصدرها الأصليّ أو مشكوك فيها) في اختراق البيانات الشّخصيّة كالصُّور والملفّات، وأيضًا سرقة بعض المعلومات مثل: كلمات المرور وأرقام البطاقات البنكيّة، ما يُؤدّي إلى وقوع الشّخص ضحيّةً في يد المُجرمين الإلكترونيّين وقد تستخدم بياناته الخاصّة لمصلحة هؤلاء المُجرمين؛ كما يُمكن أن يتمّ الاحتيال عبر الإنترنت عبر انتحال صفة صديق على الإنترنت بنفس الاسم والصُّورة الشّخصيّة، بهدف طلب خدمة ما، مثل تحويل المال إلى رقم الهاتف أو استخدام معلومات شخصيّة[1].

حقائق ومعلومات

التحقُّق من الروابط المجهولة قبل النقر عليها يُقلّل من احتمالية التعرُّض لعمليات احتيال.

الحاسوب:

تتضمّن بعض أجهزة الحاسوب المملوكة للشّركات والمؤسّسات الكبيرة والصّغيرة على حدّ سواء معلومات في غاية الأهمّيّة، لذا يلجأ القراصنة والمُحتالون إلى اختراق الحاسوب بالبرمجيّات والرّوابط الخبيثة، ممّا يُؤدّي إلى توقُّفها عن العمل، بعدها يتمّ التّواصل مع أصحاب تلك الشّركات والمؤسّسات من أجل دفع المال مُقابل استرجاع إمكانيّة الدُّخول إلى الحسابات الخاصّة بهم للوصول إلى المعلومات المُخزّنة عليها[2].

1. Mobile phone fraud, Action Fraud – National Fraud&Cyber Crime Reporting Centre. On site: https://www.actionfraud.police.uk/a-z-of-fraud/mobile-phone-fraud
2. Computer and Internet Fraud, Impact Law. On site: https://www.impactlaw.com/criminal-law/white-collar/computer-internet-fraud/

التّجارة الإلكترونيّة:

مع نُموّ حجم ومكانة التّجارة الإلكترونيّة ظهر شكل جديد من الاحتيال عبر الإنترنت يستهدف الضّحايا من المُتعاملين على المواقع الإلكترونيّة للمحالّ التّجاريّة، أي يُمكن أن يزور المُستخدم موقعًا مُزيّفًا بهدف شراء بعض السّلع إلّا أنّه يُفاجأ بوقوعه ضحيّة للاحتيال والنّصب الإلكترونيّ[1]، وهو ما يعني أنّه سيدفع المال دون الحصول على أيّ مُقابل. كما يُمكن أن تُحوّل بعض المواقع المُزيّفة المُستخدم إلى طُرُق دفع إلكترونيّ غير معروفة، وذلك بهدف سرقة المعلومات البنكيّة.

استغلال الكوارث:

في وقت الأزمات مثل الكوارث الطّبيعيّة أو الصّحيّة مثل "جائحة كورونا" التي وقعت قبل سنوات، يلجأ مُرتكبو الجرائم الإلكترونيّة إلى تنظيم حملات وهميّة تدعو إلى التّبرُّع من أجل مساعدة الضّحايا، ما يتسبّب في إعطائهم معلومات خاصّة بالحسابات البنكيّة، وهو ما يقع تحت طائلة الاحتيال عبر الإنترنت.

حقائق ومعلومات

استخدام كلمات مرور فريدة وقوية لكل حساب يمنع القراصنة من الوصول إلى حساباتك الأخرى في حال تسريب كلمة مرور واحدة.

1. Varga, Gergo. 7 Types of Ecommerce Fraud & How to Detect Them, SEON. On site: https://seon.io/resources/ecommerce-fraud-detection-and-prevention/

02

الفصل الثاني

كيفيّة تنفـــــيذ عمليّات الاحتيال عبر الإنترنت

- **أوّلًا:** الثّغرات المُساعدة على عمليّات الاحتيال عبر الإنترنت
- **ثانيًا:** أمن البيانات الشّخصيّة والاحتيال عبر الإنترنت
- **ثالثًا:** البصمة الرّقميّة والاحتيال عبر الإنترنت

أوّلًا: الثّغرات المُساعدة على عمليّات الاحتيال عبر الإنترنت

تُعدّ الثّغرات الرّقميّة من العوامل المُساعدة في الوقوع ضحيّةً للاحتيال الإلكترونيّ، وتُعرف الثّغرة الرّقميّة على أنّها مُصطلح يُطلق على مناطق ضعيفة في أنظمة تشغيل الحاسب، هذه المناطق الضّعيفة يُمكن التّسلُّل عبرها إلى داخل نظام التّشغيل، ومن ثمّ يتمّ التّعديل فيه لتدميره نهائيًّا، أو للتّجسُّس على المعلومات الخاصّة بصاحب الحاسب الآلي المُخترق، أو ما يُعرف بجهاز الضّحيّة[1]؛ كما تظهر الثّغرات الأمنيّة في جميع البرمجيّات أيضًا وليس في أنظمة التّشغيل فقط، وهي بسبب أخطاء برمجيّة أثناء تطويرها ارتكبها المُطوّرون، وتُشكّل خطرًا أمنيًّا بسبب عدم اكتشافها في أغلب الأحيان ممّا يستلزم إصدارًا جديدًا لإيجاد حلّ لها، ويُطلق عليها هنا **الثّغرات غير المُكتشَفَة Zero-day** التي دائمًا ما يستعين بها القراصنة في جرائمهم الإلكترونيّة. وثغرة Zero-day واحدة من هذه العيوب، وهي ثغرة في البرامج يُمكن استغلالها مِن قِبَل المُتسلّلين الذين ليس لديهم تصريح حتّى الآن، حيث لا يعرف مُطوّرو البرامج مكان الضّعف أو يُطوّرون إصلاحًا له، أو أنّهم يتجاهلون ذلك، وتُؤدّي هذه الثّغرة الأمنيّة إلى خرق خطير للأمن السّيبرانيّ[2].

1. What is bug? Neterich. On site: https://netenrich.com/glossary/bug
2. What is a Zero-day Attack? - Definition and Explanation, Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

أمثلة على هجمات Zero-Day

فيما يلي أمثلة على هجمات الثّغرة الأمنيّة التي تكشف عن مخاطر هذه الهجمات على المؤسّسات والأفراد.

سوني:

في عام 2014م، استهدف هُجُوم Zero-Day شركة Sony Pictures، وأدّى الهُجُوم إلى تدمير الشبكة الدّاخليّة لSony، وتسريب بيانات الشّركة الحسّاسة على مواقع مُشاركة الملفّات، بما في ذلك المعلومات الشّخصيّة حول مُوظّفي Sony وعائلاتهم، والمُراسلات الدّاخليّة، ومعلومات حول رواتب المدراء التّنفيذيّين، ونُسخ من أفلام سوني التي لم يتمّ طرحها، وفي هذا الهُجُوم استخدم المُهاجمُون نوعًا مُختلفًا من البرمجيات الضّارّة لمحو أنظمة مُتعدّدة على شبكة شركة سوني[1].

هُجُوم WannaCry:

تسبّب هذا الهُجُوم في تعطيل أكثر من 200,000 جهاز في يوم واحد بجميع أنحاء العالم في مايو 2017م، وقد انتشر هُجُوم برنامج الفدية هذا عبر أجهزة الحاسوب التي تعمل بنظام التّشغيل Microsoft Windows؛ حيث تمّت السّيطرة على ملفّات المُستخدمين وطلب فدية بعُملة بيتكوين Bitcoin لإعادتها؛ والسّبب في هذا الهُجُوم هو استمرار العمل بأنظمة أجهزة الحاسوب القديمة غير المُحدّثة، فقد استغلّ المجرمون الإلكترونيُّون المسؤولون عن الهُجُوم نُقطة ضعف موجودة في نظام التّشغيل Microsoft Windows باستخدام هجمة تسلُّل عُرفت باسم Eternal Blue.

1. VB2018 paper: Since the hacking of Sony Pictures, Minseok (Jacky) Cha, AhnLab, South Korea. On site: https://www.virusbulletin.com/virusbulletin/2018/11/vb2018-paper-hacking-sony-pictures/

فقبل شهرين من الهُجُوم كانت مايكروسوفت Microsoft قد أصدرت تصريحًا أمنيًّا لحماية أنظمة المُستخدمين، لكن مع عدم قيام الكثير من الأفراد بتحديث أنظمة التّشغيل الخاصّة بهم بانتظام كانوا الأكثر استهدافًا في هذا الهُجُوم؛ وقد طلب المُتسلّلون عُملة بيتكوين الرّقميّة bitcoin بقيمة 300 دولار، ثُمّ رفعوا قيمة الفدية إلى 600 دولار لكُلّ فرد، مُقابل إعادة ملفّات المُستخدمين[1].

هل تعلم؟

مشاركة الصُّور والمعلومات الشّخصيّة على الإنترنت تزيد من إمكانية تتبُّعك واستخدام بياناتك بطرق غير آمِنة.

الهجمات غير المُستهدفة لثغرة Zero-day

لا بُدّ من الإشارة هُنا إلى نوع في غاية الأهمّيّة لنا كأفراد؛ هو الهجمات غير المُستهدفة لثغرة Zero-day، فعادةً ما يتمّ شنّ هجمات الثّغرات غير المُكتشَفَة غير المُستهدفة ضدّ عدد كبير من مُستخدمي المنزل (الأفراد العاديّين) الذين يستخدمون نظامًا ضعيفًا، مثل نظام التّشغيل أو المُتصفّح، وغالبًا ما يكون هدف المُهاجم هو اختراق هذه الأنظمة واستخدامها لبناء شبكات روبوت ضخمة لتنفيذ جرائم إلكترونيّة أكبر فيما بعد[2].

1. What was the WannaCry ransomware attack? cloudflare. On site: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
2. Zero Day Exploit: All You Need to Know, phoenixnap, 2023. On site: https://phoenixnap.com/blog/zero-day-exploit#:~:text=A%20zero%2Dday%20exploit%20is,vendor%20learns%20about%20the%20vulnerability.

ثانيًا: أمن البيانات الشّخصيّة والاحتيال عبر الإنترنت

يُشير أمان المعلومات إلى مجموعة من الإجراءات والأدوات الأمنيّة التي تحمي على نطاق واسع المعلومات الحسّاسة من سُوء الاستخدام أو الوُصُول غير المُصرّح به أو التّعطيل أو الإتلاف. ويشمل أمان المعلومات الأمن المادّيّ والبيئيّ، والتّحكُّم في الوُصُول والأمان عبر الإنترنت[1].

أمّا سرقة البيانات، فهي عمليّة سرقة معلومات رقميّة مُخزّنة على أجهزة الحاسوب أو الهواتف للحصول على معلومات سرّيّة أو انتهاك الخصوصيّة. ويُمكن أن تكون البيانات المسروقة أيّ شيء مثل: معلومات الحساب المصرفيّ، وكلمات المرور على الإنترنت، ورقم جواز السّفر، والسّجلّات الطّبيّة والاشتراكات عبر الإنترنت... وما إلى ذلك. وبمُجرّد وُصُول شخص غير مُصرّح له إلى معلومات شخصيّة يُمكنه حذفها أو تغييرها أو منع الوصول إليها بدون إذن المالك[2].

وتحدُث سرقة البيانات عادةً بسبب رغبة أشخاص في بيع المعلومات أو استخدامها في سرقة الهُويّة. وإذا تمكّن لُصُوص البيانات من سرقة معلومات كافية، يُمكنهم استخدامها للوُصُول إلى حسابات آمِنة أو إصدار بطاقات ائتمان باستخدام اسم الضّحيّة أو استخدام هُويّة الضّحيّة بطريقة أُخرى لصالح أنفسهم؛ ونشير هنا إلى أن كلمة "سرقة" في مُصطلح عالم الإنترنت لا تعني حرفيًّا أخذ معلومات بعيدًا عن الضّحيّة أو نزعها منه، بل ما يحدث عند سرقة البيانات هو أنّ المُهاجم بكُلّ بساطة ينسخ المعلومات كي يستخدمها هو بنفسه. ويُطلق على هذه الجريمة الإلكترونيّة مُصطلح "انتهاك البيانات" أو "تسرُّب البيانات".

حقائق ومعلومات

ضَبْط إعدادات الخصوصيّة على مواقع التواصل الاجتماعي يُقلّل من مشاركة معلوماتك مع أطراف غير معروفة.

1. ما هُو أمان المعلومات؟، مايكروسوفت. مُتاح على الرّابط: https://www.microsoft.com/ar/security/business/security-101/what-is-information-security-infosec
2. ما المقصود بسرقة البيانات وكيفيّة منعها؟، Kaspersky. مُتاح على الرّابط: https://me.kaspersky.com/resource-center/threats/data-theft

والشّكل الأكثر شيوعًا من هذا النّوع من الجرائم هو التّصيُّد الاحتياليّ، ويحدث عندما يتنكّر مُحتال في هيئة جهة موثوقة لخداع الضّحيّة وجعله يفتح رسالة بريد إلكترونيّ أو رسالة نصّيّة أو رسالة فوريّة تحتوي على تطبيق خبيث، والأشخاص الذين يقعُون ضحيّةً لهجمات التّصيُّد الاحتياليّ يتعرّضون لسرقة الهُويّة.

كما يُمكن للأشخاص التّسبُّب في تعرُّضهم للاحتيال الإلكترونيّ بأنفسهم عن طريق تنزيل برامج أو بيانات من مواقع إلكترونية مُخترقة مُصابة بفيروسات مثل الفيروسات المُتنقّلة أو البرمجيّات الضّارّة، ممّا يُعطي المجرمين إمكانيّة وصول غير مُصرّح به إلى أجهزتهم؛ ويُتيح لهم سرقة البيانات.

ثالثًا: البصمة الرّقميّة والاحتيال عبر الإنترنت

"البصمة الرقمية" -أو كما تُسمَّى "الظل الرقمي"- هي الأثر الذي تَتركه بياناتك في أثناء استخدامك للإنترنت، سواءٌ بشكلٍ مقصود أو غير مقصود؛ حيث تشمل هذه البيانات المواقع التي تزورها، والرسائل الإلكترونية التي تُرسِلها أو تستقبلها، والتفاصيل التي تُقدّمها عند التسجيل أو الشراء أو التفاعل على شبكة الإنترنت[1].

وتشمل البصمة الرقمية أيضًا عدَّة أنشطة أخرى، مثل: النشر على وسائل التواصل الاجتماعي، أو الاشتراك في نشرات إخبارية، أو ترك مراجعات إلكترونية، أو التسوق عبر الإنترنت. كما تُسجِّل المواقع نشاط المُستخدِمين عبر ملفات تعريف الارتباط (Cookies)، التي يتمّ تثبيتها على الأجهزة لتَتبُّع السُّلوك الرقمي. في الوقت نفسه، تجمع العديد من التطبيقات بيانات المُستخدِمين أحيانًا دون عِلْمهم الكامل؛ مما يجعل هذه البيانات جزءًا من بصمتهم الرقمية.

وبمُجرَّد السماح لجهةٍ ما بالوصول إلى بياناتك، يمكن استخدامها بطُرق مختلفة، مثل: بيعها لشركات تسويقية، أو مشاركتها مع أطراف أخرى. في بعض الحالات، قد تُستغَلّ هذه البيانات لتقديم إعلانات مُخصَّصة، أو جمع معلومات أكثر عنك، والأسوأ من ذلك أنّ هذه المعلومات قد تُؤدّي إلى تعرُّضك إلى الاختراق أو السرقة؛ ممّا يجعل خصوصيَّتك وأمانك الشخصي في خَطر.

1. What is a digital footprint? And how to protect it from hackers, Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

أمثلة على البصمة الرّقميّة

من المُمكن أن يترك مُستخدم الإنترنت وراءه بصمات رقميّة من خلال أيّ نشاط يقوم به على الإنترنت، وفيما يلي تبيان لبعض الأمثلة عن هذه الأنشطة:

- التّسوُّق عبر الإنترنت.
- عمليّات شراء من مواقع التّجارة الإلكترونيّة.
- التّسجيل لإنشاء حساب على موقع ويب مُعيّن.
- تنزيل تطبيقات التّسوُّق واستخدامها.
- التّسجيل من أجل النّشرات الإخباريّة للعلامات التّجاريّة.
- الخدمات البنكيّة عبر الإنترنت.
- استخدام تطبيق الخدمات المصرفيّة للهاتف المحمول.
- الاشتراك في المطبوعات والمُدوّنات.
- فتح حساب بطاقة ائتمان.
- استخدام وسائل التّواصل الاجتماعيّ على الأجهزة الخاصّة بك.
- تسجيل الدُّخول إلى مواقع الويب الأخرى باستخدام بيانات اعتماد وسائل التّواصل الاجتماعيّ.
- التّواصُل مع الأصدقاء وجهات الاتّصال عبر الإنترنت.
- مُشاركة المعلومات والبيانات والصُّور مع معارفك.
- الاشتراك في مصدر إخباريّ عبر الإنترنت.
- إعادة نشر المعلومات التي تقرؤها.
- استخدام أجهزة تتبُّع اللّياقة البدنيّة.

حماية البصمة الرّقميّة

فيما يلي بعض النّصائح لحماية البيانات الشّخصيّة وإدارة السُّمعة الشّخصيّة للأفراد عبر الإنترنت:

التّحقُّق من البصمة الرّقميّة عبر مُحرّكات البحث

يُمكن للفرد عبر إدخال اسمه في مُحرّكات البحث، مراجعة نتائج مُحرّك البحث والمعلومات المُتاحة عنه للاطّلاع العامّ. فإذا كانت أيّ من النّتائج تُظهره بمظهر سلبيّ، يُمكنه الاتّصال بمسؤول الموقع لمعرفة ما إذا كان بإمكانه إزالتها أم لا؛ ويُعدّ إعداد تنبيهات Google إحدى طُرُق مُراقبة اسم المُستخدم[1].

تقليل عدد مصادر المعلومات

تحتوي مواقع الويب على معلومات أكثر ممّا قد يرغب الفرد في عرضه. وغالبًا ما تتضمّن هذه المواقع معلومات شخصيّة، مثل رقم الهاتف والعُنوان والعُمُر، لذا على الفرد إزالة المعلومات الشّخصيّة من هذه المواقع الإلكترونيّة أوّلًا بأوّل.

تقييد كمّيّة البيانات التي يتمّ مُشاركتها

في كل مرّة نُقدّم فيها معلومات شخصيّة لمؤسّسة ما، فإنّنا نصنع بصمتنا الرّقميّة، كما أنّنا نزيد من احتماليّة قيام إحدى المؤسّسات التي تُخزّن بياناتنا بإساءة استخدامها أو تعرُّضها للانتهاك، ما يضع بياناتنا بين الأيدي الخطأ؛ وبناءً على ذلك، علينا التّفكير جيّدًا قبل تقديم أيّ معلومات لأيّ جهة على الإنترنت.

1. How to protect your digital footprint, state farm, 2023. On site: https://www.statefarm.com/simple-insights/family/how-to-reduce-and-protect-your-digital-footprint

التّحقُّق من إعدادات الخُصُوصيّة

تسمح إعدادات الخُصُوصيّة على وسائل التّواصل الاجتماعيّ بالتّحكُّم في من يرى منشوراتنا. لذا يُفضّل مُراجعة هذه الإعدادات، والتّأكُّد من ضبطها على المستوى الذي يُناسبنا. فمثلًا يُتيح **Facebook** قصر المُشاركات على الأصدقاء، وإنشاء قوائم مُخصّصة بالأشخاص الذين يُمكنهم مُشاهدة منشورات مُعيّنة.

التّفكير جيّدًا قبل مُشاركة معلوماتنا على وسائل التّواصل الاجتماعيّ

تُسهّل وسائل التّواصل الاجتماعيّ الاتّصال بالآخرين، ولكن يُمكنها أيضًا أن تُسهّل الإفراط في مُشاركة المعلومات الشّخصيّة عليها، لذا يجب التّفكير جيّدًا قبل الكشف عن موقعنا أو أيّ معلومات شخصيّة أخرى مثل رقم الهاتف أو عُنوان البريد الإلكترونيّ.

تجنُّب المواقع غير الآمِنة

علينا في كُلّ مرّة ندخل فيها إلى الإنترنت التّأكُّد من أنّنا نتعامل مع موقع ويب آمِن يبدأ عنوان URL بـ https:// وليس http://؛ حيث يُشير حرف "s" إلى اللّفظ "آمِن". ويجب أن يكون هناك أيضًا رمز قُفل على يسار شريط العُنوان.

حقائق ومعلومات

إزالة الحسابات القديمة غير المستخدَمة تُقلّل من فُرَص استغلال بياناتك الشخصية.

الحذر عند استخدام شبكة Wi-Fi العامّة

تُعدّ شبكة Wi-Fi العامّة بطبيعتها أقلّ أمانًا من الشبكة الشّخصيّة؛ لأنّنا لا نعرف من قام بإعدادها أو من قد يشاهدها أيضًا. لذا ينبغي تجنُّب إرسال معلومات شخصيّة عند استخدام شبكات Wi-Fi العامّة.

حذف الحسابات القديمة

تتمثّل إحدى طُرُق تقليل بصمتنا الرّقميّة على الإنترنت في حذف الحسابات القديمة، ومن ذلك، على سبيل المثال، الملفّات الشّخصيّة في وسائل التّواصل الاجتماعيّ التي لم نعُد نستخدمها أو اشتراكات الرّسائل الإخباريّة.

إنشاء كلمات مرور قويّة واستخدام Password Manager

يجب أن تكون كلمة المرور القويّة طويلة، أي تتكوّن من 12 حرفًا على الأقلّ، والأمثل أن تكون أكثر من ذلك، وتحتوي على مزيج من الأحرُف الكبيرة والصّغيرة، بالإضافة إلى الرُّموز والأرقام. وكُلّما كانت كلمة المرور أكثر تعقيدًا وصعوبةً، أصبح اختراقها أصعب؛ ويساعد استخدام Password Manager على إنشاء جميع كلمات المرور الخاصّة بنا وتخزينها وإدارتها في حساب واحد آمِن عبر الإنترنت.

عدم تسجيل الدُّخول باستخدام Facebook

يُعدّ تسجيل الدُّخول إلى مواقع الويب والتّطبيقات باستخدام **Facebook** أمرًا سهلًا. لكنّنا، في كُلّ مرّة نقوم فيها بتسجيل الدُّخول إلى موقع ويب تابع لجهة خارجيّة باستخدام بيانات اعتماد **Facebook** الخاصّة بنا، نمنح هذه الشّركة الإذن للاطّلاع والاحتفاظ ببياناتنا الخاصّة، ممّا قد يُعرّض معلوماتنا الشّخصيّة للخطر.

تحديث البرامج باستمرار

يُمكن أن تحتوي البرامج القديمة على ثروة من البصمات الرّقميّة. ومن دُون آخر التّحديثات، يُمكن لمُجرمي الإنترنت الوصول إلى هذه المعلومات. فمُجرمُو الإنترنت قادرون على الوُصُول بسهولة إلى أجهزة وبيانات الضّحيّة من خلال استغلال الثّغرات في البرامج. والحلّ يكمُن في تحديث البرامج باستمرار؛ فقد تكون البرامج الأقدم أكثر عُرضة لهجمات المُتسلّلين.

تعيين كلمة مرور للهاتف المحمول

قُم بتعيين رمز مُرور لجهاز المحمول؛ حتّى لا يتمكّن الآخرون من الوُصُول إليه في حال فقده. وعند تثبيت تطبيق، اقرأ اتّفاقيّة المُستخدم؛ لأنّ العديد من التّطبيقات تكشف عن نوع المعلومات التي تجمعها، وما قد تُستخدم من أجله. وقد تقوم هذه التّطبيقات بحفظ البيانات الشّخصيّة، مثل البريد الإلكترونيّ والموقع والأنشطة عبر الإنترنت.

التّحرُّك بسُرعة بعد انتهاك البيانات

في حال الشّكّ بانتهاك البيانات الخاصّة بنا يجب التّحرُّك فورًا، خاصّةً إذا كان الأمر يشمل خسارة ماليّة، وأُولى الخُطُوات هي تغيير أيّ كلمات مرور رُبّما تمّ كشفها. وإذا كنت قد استخدمت كلمة المرور ذاتها لحسابات أخرى، فقُم بتحديثها في جميع الحسابات [1] .

استخدام شبكة VPN

يُمكن أن يساعد استخدام شبكة افتراضيّة خاصّة أو شبكة VPN على حماية بصمتنا الرّقميّة؛ وهذا لأنّ شبكات VPN تُخفي عنوان IP الخاصّ بنا، ممّا يجعل تصرُّفاتنا عبر الإنترنت غير قابلة للتّتبُّع فعليًّا. وهذا يحمي خُصُوصيّتنا عبر الإنترنت، ويمنع مواقع الويب من تثبيت ملفّات تعريف الارتباط التي تتتبّع سجلّ تصفُّح الإنترنت الخاصّ بنا.

1. How to Map, Monitor and Manage Your Digital Footprint, Bitdefender. On site: https://www.bitdefender.com/en-us/cyberpedia/how-to-protect-your-digital-footprint

03

الفصل الثّالث

كيفيّة التّصــرُّف في حال التّعرُّض للاحتيال عبر الإنترنت

- **أوّلًا:** إرشادات الحماية من الاحتيال عبر الإنترنت
- **ثانيًا:** حماية البيانات من الاحتيال عبر الإنترنت

أوّلًا: إرشادات الحماية من الاحتيال عبر الإنترنت

يبتكر المُحتالون طرقًا وآليّات جديدةً لتنفيذ جرائمهم الإلكترونيّة، غير أنّ اتّخاذ بعض الإجراءات البسيطة كفيل بتعزيز أمن المعلومات، وفيما يلي تبيان لأهمّها:

تحميل التّطبيقات من المتاجر المعروفة

ينبغي تحميل كُلّ التّطبيقات من المتاجر المعروفة، فعمليّة تحميل أيّ تطبيق من مصادر مجهولة قد تُعرّض البيانات والخُصُوصيّة للسّرقة.

تحديث تطبيقات الهاتف

لا بُدّ من تثبيت التّحديثات الجديدة الخاصّة بنظام الهاتف، فهي دائمًا تتضمّن ملفّات تُعزّز من حماية الهاتف من أشكال الاختراق المُختلفة.

تجنُّب الرّوابط مجهولة المصدر

حتّى ولو أُرسلت من الأصدقاء، فبمُجرّد الضّغط عليها قد تتعرّض للاختراق، أو تثبيت برمجيّات خبيثة على هاتفك دون معرفتك، وكذلك لا تفتح رسائل البريد الإلكترونيّ المجهولة.

الحذر من المُعاملات التي تتضمّن أطرافًا ثالثة

يجب الحذر عند طلب استقبال أيّ تحويلات ماليّة ثمّ تحويلها إلى طرف ثالث، فقد يكون ذلك عمليّة نصب أو غسيل أموال.

الاستعانة ببرامج مُكافحة الفيروسات

سواء على الهاتف الذّكيّ أو جهاز الحاسوب، يجب تثبيت مُكافح فيروسات معروف، ويحظى بسُمعة جيّدة؛ من أجل تعزيز مُستوى الحماية على الأجهزة الخاصّة.

استخدم كلمات مُرُور مُعقّدة

يُفضّل أن تتضمّن حروفًا ورموزًا وأرقامًا، كما يجب تغييرها فورًا كُلّما أدركت أنّ هناك ما يدعو للشّكّ.

هل تعلم؟

أنَّ استخدام كلمات مرور مُعقّدة وفريدة يُقلِّل من فُرَص اختراق حساباتك الشخصية.

عدم التّسوُّق من المواقع المجهولة

لا تقم بأيّ عمليّة شراء عبر الإنترنت إلّا من المواقع المشهورة والمتاجر الإلكترونيّة ذات السُّمعة الطّيّبة، وإن راودك بعض الشّكّ حول مصداقيّة بعض المواقع، فينبغي البحث عنها أكثر للتّأكُّد من وضعها.

ثانيًا: حماية البيانات من الاحتيال عبر الإنترنت

إنّ حماية البيانات الشّخصيّة والماليّة من الاحتيال أمر مُمكن، ويُمكن تحقيق هذه الحماية من خلال عدّة إجراءات، فيما يلي تبيان لأهمّها:

- التّيقُّظ لعمليّات الاحتيال عند التّعامل مع اتّصالات مُتطفّلة مِن قِبَل أشخاص أو أيّ جهة؛ سواء كانت عبر الهاتف، البريد، الرّسالة الإلكترونيّة، أو على موقع لشبكات التّواصل الاجتماعيّ، فقد تكون عمليّة احتيال.
- إذا كنت قد التقيت بشخص ما عبر الإنترنت، عليك أخذ الوقت الكافي للبحث عنه، مثل البحث عن الصُّور في مُحرّك **Google** للصُّور، أو ابحث عبر الإنترنت عن أشخاص آخرين من المُحتمل أن يكونوا قد تعاملُوا معه.
- لا تفتح نصوصًا أو نوافذ تظهر أمامك أو رسائل إلكترونيّة مشبوهة، مع ضرورة التّأكُّد من هُويّة المُتّصل عبر مصدر مُستقلّ مثل البحث على الإنترنت. وكذلك لا تفتح رسائل البريد الإلكترونيّ المجهولة.
- احتفظ بتفاصيلك الشّخصيّة بشكل آمِن، مثل وضع قُفل على صندوق بريدك، مع الاحتفاظ بكلمات السّرّ والأرقام السّرّيّة الخاصّة بك في مكان آمِن، مع الحذر من المعلومات الشّخصيّة التي تُشاركها على مواقع التّواصل الاجتماعيّ.
- تحديث أنظمة أجهزة هاتفك والحاسوب الخاصّ بك باستمرار، والاحتفاظ بنُسخة احتياطيّة للمحتوى.
- ضع كلمة سرّ لشبكتك الخاصّة بالـWiFi وتجنّب استخدام أجهزة حاسوب عامّة أو النّقاط السّاخنة في الـ WiFi .
- راجع ترتيباتك المُتعلّقة بالخُصُوصيّة والأمن على مواقع التّواصل الاجتماعيّ.

- احذر من أيّ طلبات تتعلّق بتفاصيلك أو مالك.
- كُن حذرًا عندما تتسوّق على الإنترنت، وخاصّة العروض التي تبدو مُغرية جدًّا.
- عند مُراجعة نُبذة تعارُف جديدة، لاحظ أيّ شيء غير عاديّ في خيارات الشّخص الآخر مثل: (**الصُّورة، أو المكان، أو الاهتمامات، أو تطابُق المهارات اللُّغويّة مع الخلفيّة**)؛ فغالبًا ما يستعمل المُحتالون صُورًا مُزوّرة وجدُوها على الإنترنت. لذا قُم بعمليّة بحث عن صورة الشّخص المُعجب بك لمساعدتك على التّثبُّت من أنّه فعلًا الشّخص الذي يقول إنّه هو، ويُمكن الاستعانة بخدمات البحث عن الصُّور مثل **Google**.
- غيّر كلمات السّرّ الخاصّة بك على الإنترنت إذا كنت تعتقد بأنّ الحاسوب الخاصّ بك أو الهاتف قد تعرّض للقرصنة، فيجب إجراء فحص شامل لنظامك الإلكترونيّ بواسطة برامج مضادات الفيروسات المُعتمدة، ثمّ قُم بتغيير كلمة السّرّ. وكذلك الأمر بالنّسبة للحسابات على الإنترنت، سواء على مواقع التّواصل الاجتماعيّ أو مواقع التّسوُّق .... وغيرها، يجب تغيير كلمة السّرّ فورًا.
- ضع إشارةً مرجعيّةً للمواقع المهمّة، عبر إضافة جميع المواقع التي تقوم بزيارتها باستمرار إلى الإشارات المرجعيّة الخاصّة بك، وافتحها فقط من هناك، وبهذا تقضي على خطر فتح صفحات وهميّة بطريق الخطأ.
- هناك عدّة علامات تحذيريّة لاكتشاف الوثائق المُزوّرة؛ مثل "بيانات الحسابات المصرفيّة" أو "رحلات الطّيران" التي قد تكون فخًّا مِن قِبَل المُتسلّلين في صورة هدايا وهميّة لمعرفة البيانات الشّخصيّة من الأفراد، مثل: التّحيّات العامّة بدلًا من التّحيّات الشّخصيّة، استخدام أسماء مُنظّمات غير موجودة، ركاكة في المظهر، ضعف في القواعد والتّهجئة، مُبالغة في الرّسميّات.
- تذكّر أنّ رسائل الخطأ الحقيقيّة من **Microsoft** أو شركات تقنيّة كبيرة أخرى، لا تتضمّن أبدًا أرقام هواتف لكي تتّصل بها.

لن تتّصل بك مايكروسوفت Microsoft وشركات التّقنيّة الشّرعيّة الأخرى أبدًا لتُخبرك بأنّ هناك مشكلة في جهازك. ما لم تتّصل بهم أوّلًا، ولن يحتاج وكلاء الدّعم التّقنيّ أبدًا إلى أن يطلبوا منك رقم الضّمان الاجتماعيّ الخاصّ بك أو أيّ معلومات شخصيّة أخرى غير مُرتبطة. إذا حصلت على مُكالمة من شخص ما يعرض دعمًا تقنيًّا غير مرغوب فيه، فقُم بإنهاء المكالمة معه.

إذا كانت شاشتك تمتلئ بشكل مُفاجئ بالنّوافذ المُنبثقة المُخيفة؛ يجب إغلاق المُستعرض على الفور (**حاول الضّغط على ALT+F4 إذا لم تتمكّن من القيام بذلك باستخدام الماوس**)، وإذا لم تتمكّن من إغلاق المُستعرض، فحاول إعادة تشغيل الحاسوب[1].

هل تعلم؟

أنّ تجنُّب تسجيل الدخول باستخدام بيانات الفيسبوك يحمي بَصْمتك الرقميَّة من الانتشار غير الضروري.

1. Protect yourself from online scams and attacks, Microsoft, on site: https://support.microsoft.com/en-gb/office/protect-yourself-from-online-scams-and-attacks-0109ae3f-fe61-4262-8dce-2ee3cd43bac7

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

التمرين الأول

- **اختر الإجابة الصحيحة**

1. أيّ ممّا يلي يُعتبر من الأمثلة على البصمة الرّقميّة النّشطة:

1. المنشورات على منصّات التّواصل الاجتماعيّ.
2. التّطبيقات التي تُستخدم لتحديد الموقع الجغرافيّ.
3. مواقع الويب التي تُثبّت ملفّات الارتباط دون إخطار المُستخدم.

2. من أسباب الاحتيال عبر الإنترنت:

1. الاستخدام الخاطئ لمواقع الإنترنت.
2. انتشار المتاجر الإلكترونيّة المُزيّفة.
3. استغلال مشاعر التّعاطُف.
4. جميع ما سبق.

3. كلمة "سرقة" في عالم الإنترنت يُطلق عليها .... .

1 انتهاك البيانات.

2 تسريب البيانات.

3 جميع ما سبق.

4. يُمكن استخدام ..... لتتبُّع أنشطة أيّ شخص على الإنترنت.

1 بصمة الوجه.

2 بصمة اليد.

3 البصمة الرّقميّة.

التمرين الثاني

اكتب الكلمة أو العبارة المُرادفة للجُمل التّالية:

1. هُجُوم نتعرّض له ويُعطّل حساباتنا على الإنترنت، ومُقابل إعادة استخدامها علينا أن ندفع مبلغًا ماليًّا.
2. رسائل بجوائز ماليّة وهدايا مُزيّفة تصل إلينا عبر البريد الإلكترونيّ أو الماسنجر هدفها خداعنا وسرقة بياناتنا.
3. مناطق ضعيفة تتسبّب في اختراق أجهزتنا، سواء الحاسوب أو الهاتف، وتُعرّضنا للخطر.
4. أدوات تحمي معلوماتنا الحسّاسة من الوُصُول إليها أو تعطيلها أو إتلافها.
5. سرقة من نوع خاصّ تستهدف بياناتنا الشّخصيّة على الإنترنت، ويُعاقب القانون فاعلها.

6 آثار على الإنترنت يستخدمها المُهاجمُون لاستغلال ما بها من معلومات وبيانات حسّاسة في خداعنا وكذلك خداع الآخرين.

7 تتكوّن من 12 حرفًا ورمزًا ورقمًا وهدفها حمايتنا على الإنترنت.

التمرين الثالث

أكمل العبارات الآتية

1. البصمات الرّقميّة ..... يُقصد بها مُشاركة المُستخدم معلومات عن نفسه عمدًا.
2. البصمة الرّقميّة ..... يُقصد بها جمع معلومات حول المُستخدم دون أن يُدرك أن هذا يحدث.
3. يستطيع مُجرمو الإنترنت استغلال ..... لأغراض مثل الانتحال الإلكترونيّ.
4. من بين الطُّرُق التي يضيف بها المُستخدمون إلى بصمتهم الرّقميّة تنزيل .....
5. من طُرُق حماية البصمة الرّقميّة تقييد.....
6. التّحقُّق من إعدادات الخُصُوصيّة من طُرُق حماية .....
7. من إرشادات الحماية من الاحتيال عبر الإنترنت تجنُّب الضّغط على الرّوابط .....
8. يُفضّل أن تستخدم كلمات مرور مُكوّنةً من ..... للحماية من الاحتيال عبر الإنترنت.

9 في حال التّعرُّض لجريمة احتيال إلكترونيّ نلجأ إلى إبلاغ .....

10 إذا كانت شاشتك تمتلئ بشكل مُفاجئ بالنّوافذ المُنبثقة المُخيفة، يجب .....


حلّ التمارين
والتدريبات

السؤال

التمرين الأول: اختر الإجابة الصحيحة

الإجابة

1. المنشورات على منصّات التّواصل الاجتماعيّ.
2. جميع ما سبق.
3. جميع ما سبق.
4. البصمة الرّقميّة.

السؤال

التمرين الثاني: اكتب الكلمة أو العبارة المُرادفة للجُمل التّالية

الإجابة

1. هُجُوم الفدية.
2. الاحتيال عبر الإنترنت.
3. الثّغرات الأمنيّة.
4. أمان المعلومات.
5. انتهاك البيانات.
6. البصمة الرّقميّة.
7. كلمة المرور.

السؤال

التمرين الثالث: أكمل الجُمل التّالية بالإجابة الصّحيحة

الإجابة

1. البصمات الرّقميّة **النّشطة** يُقصد بها مُشاركة المُستخدم معلومات عن نفسه عمدًا.
2. البصمة الرّقميّة **غير النّشطة** يُقصد بها جمع معلومات حول المُستخدم دون أن يُدرك أن هذا يحدث.
3. يستطيع مُجرمو الإنترنت استغلال **البصمة الرّقميّة** لأغراض مثل الانتحال الإلكترونيّ.
4. من بين الطُّرُق التي يضيف بها المُستخدمون إلى بصمتهم الرّقميّة تنزيل **التّطبيقات**.
5. من طُرُق حماية البصمة الرّقميّة تقييد **كمّيّة البيانات التي يتمّ مُشاركتها.**
6. التّحقُّق من إعدادات الخُصُوصيّة من طُرُق حماية **البصمة الرّقميّة.**
7. من إرشادات الحماية من الاحتيال عبر الإنترنت تجنُّب الضّغط على الرّوابط **مجهولة المصدر.**
8. يُفضّل أن تستخدم كلمات مرور مُكوّنةً من **الحُرُوف والرُّموز والأرقام** للحماية من الاحتيال عبر الإنترنت.
9. في حال التّعرُّض لجريمة احتيال إلكترونيّ نلجأ إلى إبلاغ **شخص ثقة مثل الوالدين.**
10. إذا كانت شاشتك تمتلئ بشكل مُفاجئ بالنّوافذ المُنبثقة المُخيفة، يجب **غلقها على الفور.**

المراجع

1. يونس الباشا، فايزة. الجريمة المُنظَّمة في ظلّ الاتفاقيات الدّولية والقوانين الوطنيّة، دار النّهضة العربية للطبع والنشر والتوزيع، 2001م، ص 21.
2. ما هو أمان المعلومات؟، مايكروسوفت. مُتاح على الرّابط: https://www.microsoft.com/ar/security/business/security-101/what-is-information-security-infosec
3. ما المقصود بسرقة البيانات وكيفيّة منعها؟، Kaspersky. مُتاح على الرّابط: https://me.kaspersky.com/resource-center/threats/data-theft
4. How aligning security and the business creates cyber resilience, State of Cybersecurity Resilience 2021. On site: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-165/accenture-state-of-cybersecurity-2021.pdf
5. Report: The 2021 Identity Fraud Study, BY ALEX ROLFE, April 2021, on site: https://www.paymentscardsandmobile.com/report-the-2021-identity-fraud-study/
6. Internet Fraud, Australian Federal Police (AFP). on site: https://police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf

7. What is email fraud? Cloudflare. On site: https://www.cloudflare.com/learning/email-security/what-is-email-fraud/

8. Mobile phone fraud, Action Fraud – National Fraud&Cyber Crime Reporting Centre. On site: https://www.actionfraud.police.uk/a-z-of-fraud/mobile-phone-fraud

9. Computer and Internet Fraud, Impact Law. On site: https://www.impactlaw.com/criminal-law/white-collar/computer-internet-fraud/

10. Varga, Gergo. 7 Types of Ecommerce Fraud & How to Detect Them, SEON. On site: https://seon.io/resources/ecommerce-fraud-detection-and-prevention/

11. What is bug? Neterich. On site: https://netenrich.com/glossary/bug

12. What is a Zero-day Attack? - Definition and Explanation, Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

13. VB2018 paper: Since the hacking of Sony Pictures, Minseok (Jacky) Cha, AhnLab, South Korea. On site: https://www.virusbulletin.com/virusbulletin/2018/11/vb2018-paper-hacking-sony-pictures/

14. What was the WannaCry ransomware attack? cloudflare. On site: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

15. Zero Day Exploit: All You Need to Know, phoenixnap, 2023. On site: https://phoenixnap.com/blog/zero-day-exploit#:~:text=A%20zero%2Dday%20exploit%20is,vendor%20learns%20about%20the%20vulnerability.

16. What is a digital footprint? And how to protect it from hackers, Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

17. How to protect your digital footprint, state farm, 2023. On site: https://www.statefarm.com/simple-insights/family/how-to-reduce-and-protect-your-digital-footprint

18. How to Map, Monitor and Manage Your Digital Footprint, Bitdefender. On site: https://www.bitdefender.com/en-us/cyberpedia/how-to-protect-your-digital-footprint

19. Protect yourself from online scams and attacks, Microsoft, on site: https://support.microsoft.com/en-gb/office/protect-yourself-from-online-scams-and-attacks-0109ae3f-fe61-4262-8dce-2ee3cd43bac7

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative