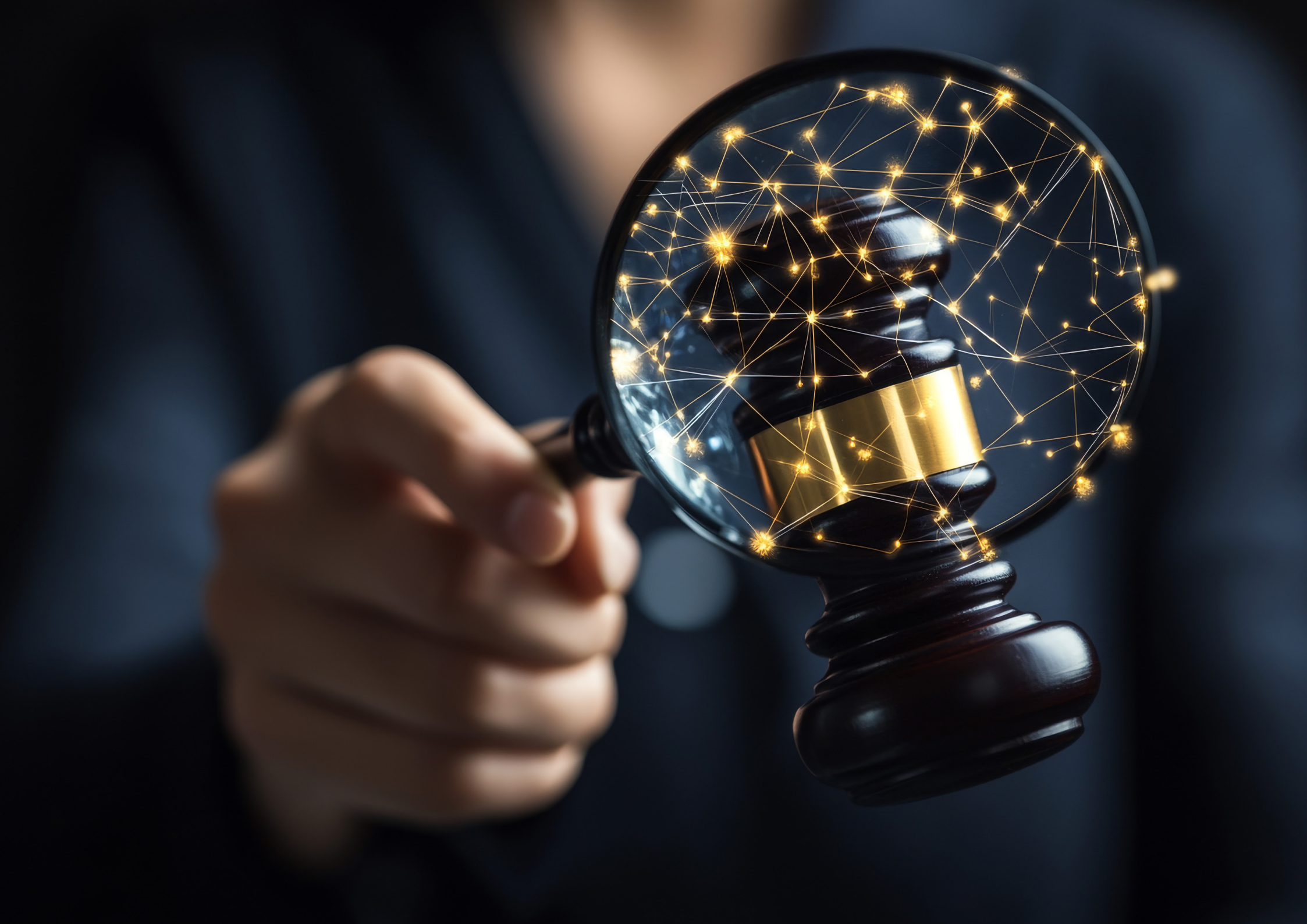
سرقة الهُويَّة عبـر الإنترنت

الفئة المستهدَفة
ذوو الاحتياجات الخاصة

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

سرقة الهُويَّة عبر الإنترنت

الفئة المُستهدَفة: ذوو الاحتياجات الخاصة



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.

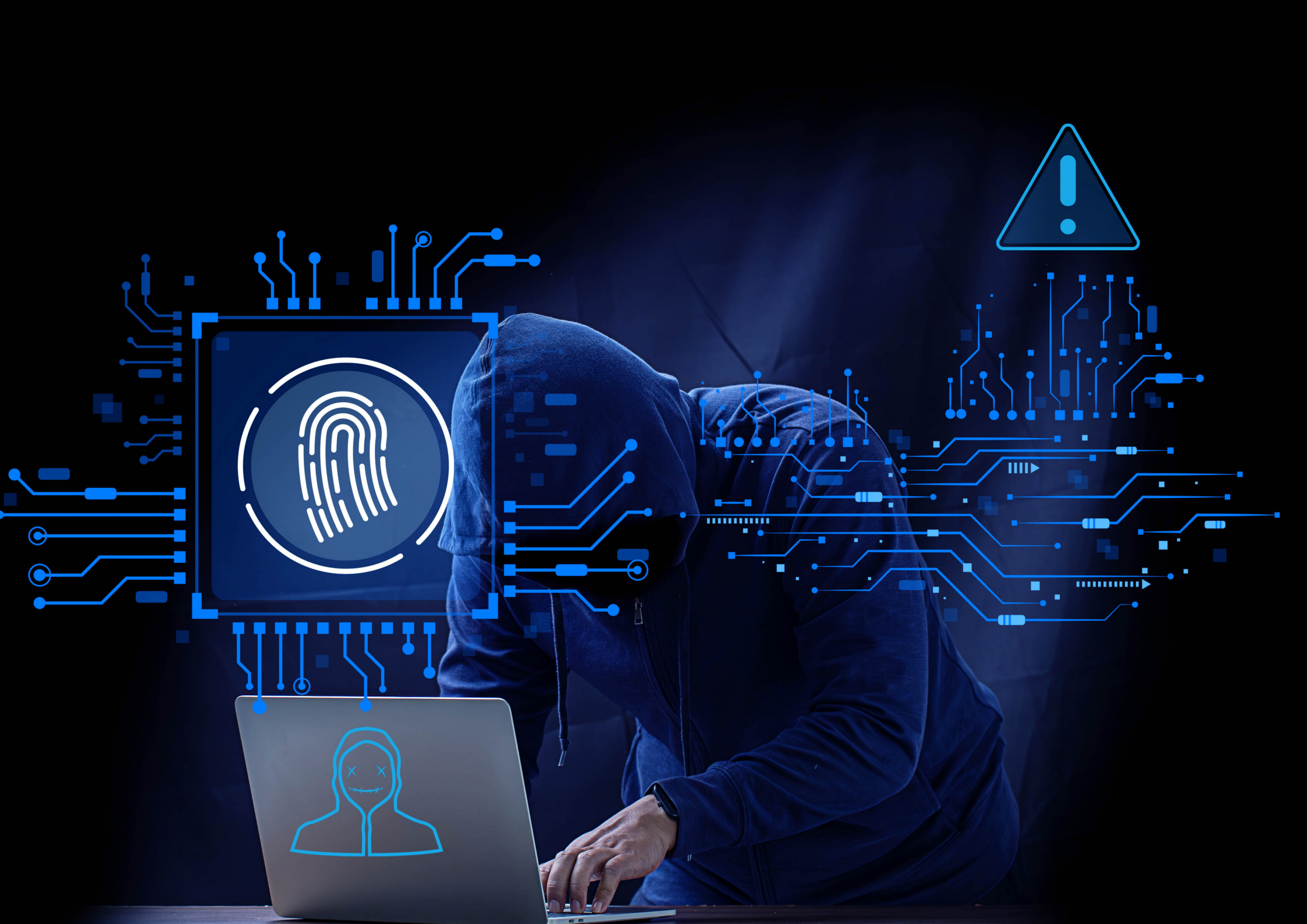
مُقـــدّمة

سرقة الهُويَّة عبر الإنترنت هي إحدى أبرز الجرائم السيبرانية التي تتزايد بشكلٍ مستمرّ مع تطوُّر التكنولوجيا واعتماد الأفراد المتزايد على الإنترنت في حياتهم اليومية. هذا النوع من الجرائم لا يستهدف فئةً معينةً، بل يمكن أن يقع ضحيَّته أي شخص، بغَضّ النظر عن عُمره أو خبرته التقنية؛ حيث يعتمد المجرمون في هذا النوع من الاحتيال على تقنيات الهندسة الاجتماعية، وهي أدوات مُتقدّمة لخداع الأفراد عبر التلاعب النفسي، من خلال إثارة مشاعر الخوف أو الاستعجال لدى الضحايا، مما يدفعهم إلى اتّخاذ قرارات مُتهوّرة مثل: تقديم معلومات شخصية أو مالية دون تفكير كافٍ.

كما يتنكَّر المجرمون في هيئة جهات موثوقة، مثل: البنوك، والمؤسسات المالية، أو حتى الجهات الحكومية؛ وذلك لجعل الضحايا يعتقدون أنهم يتعاملون مع كيان شرعيّ؛ حيث يستخدم هؤلاء المجرمون أساليب متعددة للوصول إلى ضحاياهم، مثل إرسال رسائل بريد إلكتروني مزيَّفة، أو استخدام مواقع وهمية تبدو مشابهة للمواقع الأصلية، أو حتى إجراء مكالمات هاتفية تبدو مُقنِعة. وبمجرَّد أن يتمكَّنوا من خداع الضحايا للحصول على بياناتهم الشخصية -مثل كلمات المرور أو أرقام الحسابات البنكية- يصبح بإمكانهم استغلال هذه المعلومات لتنفيذ عمليات مالية غير قانونية، أو سرقة الهُويَّة، أو الوصول إلى الحسابات الخاصة.

ولا تقتصر سرقة الهُويَّة على سرقة المعلومات الشخصية فقط، بل يمكن أن تؤدي إلى تحويل الأجهزة المخترقة إلى أدوات للهجوم على أشخاص أو شركات أخرى. في بعض الحالات، تُستخدَم أجهزة الحاسوب أو الهواتف المصابة لتنفيذ هجمات أوسع مثل هجمات حجب الخدمة (DDoS)؛ من خلال توجيه عدد كبير من الطلبات الوهمية نحو موقع إلكتروني معيَّن بهدف تعطيله. هذه الهجمات تبرز مدى تعقيد التهديدات السيبرانية في العصر الحالي، وحقيقة أن سرقة الهُويَّة عبر الإنترنت يمكن أن تكون مُقدّمة لسلسلة من الجرائم الأخرى التي تهدّد الأمن الرقمي على نطاق واسع.

مع ازدياد اعتماد الأفراد والشركات على الإنترنت لإدارة شؤونهم المالية والشخصية، أصبحت حماية الهُويَّة الرقمية أكثر أهميةً من أيّ وقتٍ مضى، ولذلك ينبغي توعية المستخدِمين بخطورة سرقة الهُويَّة وكيفية الوقاية منها، بالإضافة إلى اعتماد تقنيات مُتقدّمة للحماية، مثل: التشفير والمصادقة متعددة العوامل؛ وذلك من أجل الحفاظ على الأمن السيبراني.



01

الفصل الأول

مفهوم سرقة الهُوِيَّة

- أولاً: **هجمات سرقة الهُوِيَّة وأنواعها.**
- ثانياً: **أسباب سرقة الهُوِيَّة عبر الإنترنت.**
- ثالثاً: **تأثيرات سرقة الهُوِيَّة.**

مفهوم سرقة الهُويَّة

سرقة الهُويَّة تُعدّ من أخطر الجرائم الإلكترونية التي تهدّد الأفراد والشركات على حدٍّ سواء في العالَم الرقمي اليوم؛ حيث يشير مصطلح "سرقة الهُويَّة" إلى الاستيلاء غير القانوني على المعلومات الشخصية لشخصٍ ما، مثل: الاسم، رقم الهُويَّة، الحسابات البنكية، أو بيانات بطاقة الائتمان، بهدف استخدامها في أغراض احتيالية. أمَّا "تزوير الهُويَّة"، فهو عملية استخدام هذه المعلومات لتمثيل شخص آخر أو ادّعاء هُويَّة مُزيَّفة بهدف خداع الضحايا أو المؤسسات لتحقيق مكاسب مالية أو اجتماعية.

ومع التطوُّر السريع للتكنولوجيا وزيادة الاعتماد على الإنترنت في إنجاز المعاملات الشخصية والمالية، أصبح من السهل على المجرمين الإلكترونيّين الوصول إلى معلومات حسَّاسة واستغلالها. وغالباً ما يحدث ذلك من خلال تقنيات مُتقدّمة مثل الهندسة الاجتماعية، والتصيد عبر الإنترنت (phishing)، أو اختراق الحسابات عبر الإنترنت. وفي حالاتٍ أخرى، قد يستهدف المجرمون البيانات عبر البرمجيات الخبيثة التي تجمع المعلومات الشخصية من الأجهزة المخترَقة.

كما لا تقتصر تبعات تزوير الهُويَّة على الأضرار المالية فقط، بل قد تؤدي أيضاً إلى تداعيات قانونية واجتماعية خطيرة؛ حيث يمكن استخدامها في ارتكاب جرائم أخرى مثل فتح حسابات مصرفية وهمية، أو تقديم طلبات للحصول على قروض، أو حتى تنفيذ عمليات احتيال تحت اسم الضحية.

أصبح التصدي لهذه الجرائم تحدياً كبيراً للحكومات والمؤسسات الأمنية؛ حيث تتطلَّب الحماية من سرقة الهُويَّة وانتحال الشخصية جهوداً متعددة الجوانب، تشمل التوعية بأفضل ممارسات السلامة الرقمية، وتطبيق تقنيات التشفير المتقدّمة، وتطوير قوانين صارمة تُجرِّم هذه الأنشطة وتردع المجرمين.

أولاً: هجمات سرقة الهُويَّة وأنواعها

يُعدّ هجوم سرقة الهُويَّة أحد أنواع هجمات التصيد الاحتيالي التي يتظاهر خلالها مُجرِمو الإنترنت بأنهم أشخاص حقيقيُّون أو كيانات شرعية؛ لسرقة البيانات الشخصية الحسَّاسة للأفراد والموظفين العاملين بالمؤسسات بواسطة تقنيات الهندسة الاجتماعية؛ حيث يحاولون خداع الضحية لتحويل الأموال أو تقديم معلومات حسَّاسة أو تقديم بيانات تسجيل الدخول الخاصة بالحسابات المصرفية والرقمية، وغيرها من المعلومات غير المصرَّح بالوصول إليها لأهميَّتها[1].

ومن الأمثلة على هجوم انتحال الشخصية الناجح: عندما يستخدم المجرمون بريداً إلكترونياً مزيّفاً لمدير تنفيذي رفيع المستوى أو كيان تجاري مهم، وهو ما يُطلَق عليه اختراق البريد الإلكتروني التجاري (BEC)؛ حيث يخدع المجرم ضحاياه لإجراء تحويل مالي أو تقديم معلومات مهمة تساعده في الوصول غير المصرَّح به إلى الأنظمة والشبكات، وقد تكون السرقة خطوةً أوَّليةً وتمهيدية لجريمة إلكترونية أخرى، مثل: تثبيت البرمجيات الضّارَّة على الأجهزة الخاصة بالضحية لسرقة البيانات الحساسة، وتهديد الضحية؛ أو لتكون بوَّابته للوصول إلى الأجهزة المتصلة على الشبكة نفسها والأنظمة، خاصةً في أماكن العمل.

هل تعلم؟

رسالة من كل 3226 رسالة بريد إلكتروني تُرسَل مرة واحدة شهرياً تقريباً يتلقَّاها موظف رفيع المستوى؛ هي محاولة سرقة هُويَّة أو تصيد احتيالي[2].

1. What is Impersonation in Cybersecurity? Zero Fox, on site: https://www.zerofox.com/glossary/impersonation-in-cybersecurity/
2. Kyle Chin, What is an Impersonation Attack?, september 2024. on site: https://www.upguard.com/blog/impersonation-attack#:~:text=An%20impersonation%20attack%20is%20a%20type%20of%20targeted%20phishing%20attack

أنواع هجمات سرقة الهُويَّة

يحاول مُجرِمو الإنترنت انتحال شخصية ما بطُرقٍ مختلفة بواسطة أساليب التصيد الاحتيالي، وهناك عدَّة أنواع من هجمات سرقة الهُويَّة، وهي كالآتي:

هجمات سرقة الهُويَّة عبر البريد الإلكتروني Email Impersonation Attacks

من وسائل هجمات سرقة الهُويَّة هي تظاهر مُجرِمي الإنترنت بأنهم زملاء عمل أو مدراء تنفيذيُّون باستخدام حساب بريد إلكتروني مزيَّف أو مسروق، علماً أن هجمات سرقة الهُويَّة أو هجمات التصيد الاحتيالي المباشر تُعدّ هجمات متطورة للغاية ومُستهدفة، على عكس هجمات التصيد الجماعي عبر البريد الإلكتروني التي تنتهي في مجلد البريد العشوائي.

وغالباً ما تحتوي هجمات سرقة الهُويَّة عبر البريد الإلكتروني على روابط أو مرفقات ضارة تنقل المستخدِم بمجرَّد الضغط عليها إلى مواقع ويب تحتوي على برمجيات ضارة، كما تستخدم هجمات أخرى، مثل هجمات الهندسة الاجتماعية؛ لخداع الضحية وإقناعه بالكشف عن بيانات مهمة أو تحويل الأموال مباشرةً إلى المجرم[1].

1. Email Impersonation Attacks, Proof Point, on site: https://www.proofpoint.com/us/threat-reference/impersonation-attack

ومن العلامات الشائعة لهجمات سرقة الهُويَّة عبر البريد الإلكتروني:

- الطلبات العاجلة التي تتضمّن إلحاحاً لتحويل الأموال أو الإفصاح عن المعلومات الحساسة مثل بيانات الحساب المصرفي، أو بيانات تسجيل الدخول.
- طلب الموظفين إجراء تعديلات على معلومات الإيداع المباشر بشكلٍ مفاجئ.
- وجود أخطاء إملائية ونحوية في رسائل البريد الإلكتروني، مثل: كتابة الحرف "m" على هيئة "rn".
- اعتماد لغة تثير الشعور بالإلحاح والخوف والتوتر.
- عادةً تكون رسالة البريد الإلكتروني المزيَّفة نسخة معدَّلة قليلاً من عنوان البريد الإلكتروني الأصلي، كما لا تتطابق الروابط الفعلية لعناوين URL داخل البريد الإلكتروني مع النص الموجود في الروابط التشعبية في نص نسخة البريد الإلكتروني[1].

1. Impersonation Attack. follow link: https://www.mimecast.com/content/impersonation-attack/

ثانياً: أسباب سرقة الهُويَّة عبر الإنترنت

سرقة الهُويَّة هي واحدة من أكثر الجرائم الإلكترونية انتشاراً، والتي تتسبَّب في أضرار جسيمة للأفراد والشركات على حَدٍّ سواء؛ حيث تتنوّع أشكال سرقة الهُويَّة، من سرقة المعلومات المالية إلى انتحال الشخصية على وسائل التواصل الاجتماعي. ومن أبرز أسباب سرقة الهُويَّة عبر الإنترنت:

الإفراط في استخدام الإنترنت والتواصل الرقمي

أحد الأسباب الرئيسية وراء زيادة حالات سرقة الهُويَّة: استخدام الإنترنت بشكلٍ كبيرٍ. فمع تحوُّل معظم الأنشطة الحياتية إلى العالَم الرقمي، من التسوق الإلكتروني إلى المعاملات البنكية، أصبح من السهل على المجرمين استغلال هذه البيئة المفتوحة للوصول إلى المعلومات الشخصية.

كما أن الحياة اليومية للكثيرين أصبحت مرتبطة بشدة بالإنترنت؛ حيث يعتمد الأفراد على التطبيقات والمنصات الرقمية للتواصل، والتسوق، وإجراء المعاملات المالية. ومع هذا الاعتماد الكبير، زادت الفرص أمام مُجرِمي الإنترنت لاستغلال أي ثغرة للوصول إلى البيانات الحساسة، سواء أكانت هذه البيانات مالية أَم شخصية. إضافة إلى أن الكثير من الأفراد يقومون بإجراء تعاملاتهم عبر الإنترنت دون التأكد من أمان المواقع أو التطبيقات التي يستخدمونها؛ حيث يمكن للمهاجمين استغلال هذه التعاملات غير المؤمَّنة للحصول على معلومات حساسة، مثل: أرقام البطاقات الائتمانية، أو بيانات تسجيل الدخول.

ضعف الوعي بأساسيات السلامة الرقمية بين المستخدِمين

الوعي بالسلامة الرقمية هو خط الدفاع الأول ضد الجرائم الإلكترونية. وللأسف، يعاني الكثير من المُستخدِمين من نقصٍ في المعرفة بأساليب الحماية اللازمة؛ مما يجعلهم عرضة للاختراق وسرقة بياناتهم، كما أن الكثير من المُستخدِمين يعتمدون على كلمات مرور ضعيفة وسهلة التوقُّع، مثل: "123456" أو"password". هذه العادة تجعل من السهل على المهاجمين تنفيذ هجمات تخمين كلمات المرور أو استخدام برمجيات القرصنة للوصول إلى الحسابات.

هل تعلم؟

80% من حالات الاختراقات الإلكترونية تكون بسبب استخدام كلمات مرور ضعيفة أو مُعاد استخدامها في أكثر من حساب[1].

1. Stouffer, Clare. 139 password statistics to help you stay safe in 2024 Norton, june 2023, on site: https://us.norton.com/blog/privacy/password-statistics

زيادة الثغرات الأمنية في الأنظمة والتطبيقات

مع تزايد تعقيد الأنظمة والتطبيقات، تزداد احتمالية وجود ثغرات أمنية فيها. لذا يتم اكتشاف ثغرات جديدة باستمرار، ويعمل مُطوّرو البرمجيات على معالجتها من خلال التحديثات الدورية. ومع ذلك، عدم التزام المُستخدِمين بتنزيل هذه التحديثات يزيد من فرص نجاح الجرائم الإلكترونية. وفي الوقت ذاته، تتطوَّر تقنيات القرصنة باستمرار مع تطوُّر التكنولوجيا، فقد أصبحت أساليب مثل التصيد الاحتيالي، وهجمات البرمجيات الخبيثة، والبرمجيات التجسُّسية أكثر تعقيداً؛ مما يعزّز من فرص المجرمين الإلكترونيّين في استهداف الأفراد والشركات بنجاح. ومن بين أكثر الأهداف جاذبيةً لهؤلاء المجرمين: التطبيقات المصرفية والمالية على الإنترنت؛ حيث تُشكّل الثغرات في هذه التطبيقات خطورةً كبيرةً، إذ يمكن للمهاجمين، عند استغلال هذه الثغرات، الوصول إلى حسابات المستخدِمين وسرقة أموالهم أو معلوماتهم المالية بكُلّ سهولة.

الهجمات التصيدية وانتشار البرمجيات الخبيثة

يُعدّ التصيد الاحتيالي (phishing) من أكثر الأساليب شيوعاً في سرقة الهُويَّة؛ حيث يعتمد المهاجمون على إرسال رسائل بريد إلكتروني أو رسائل نصية تبدو وكأنها من جهات موثوقة، مثل البنوك أو الشركات الكبرى؛ بهدف خداع المستخدِمين للحصول على معلوماتهم الحسَّاسة، وغالباً ما تحتوي هذه الرسائل المزيَّفة على روابط تقود المُستخدِم إلى مواقع وهمية مصمَّمة بدقَّة لتُشبه المواقع الرسمية للجهة المُدعى أنها أرسلت الرسالة. فإذا أَدخَل المُستخدِم بياناته الشخصية في هذا الموقع، تنتقل هذه المعلومات مباشرةً إلى المهاجمين.

بالإضافة إلى التصيد الاحتيالي، تؤدي البرمجيات الخبيثة (malware) دوراً كبيراً في هجمات القرصنة، وتُعدّ هذه البرمجيات من أخطر الوسائل التي يعتمد عليها المهاجمون لاختراق الأجهزة وسرقة البيانات، فهي تتضمَّن برمجيات تجسُّسية قادرة على مراقبة جميع أنشطة المُستخدِم على جهازه، بما في ذلك تسجيل كلمات المرور والمعلومات الشخصية؛ مما يزيد من خطورة سرقة الهُويَّة وانتهاك الخصوصية[1].

هل تعلم؟

حوالي 20% من المُستخدِمين يتعرضون لمحاولات تصيد احتيالي سنوياً.

1. Kinza. Yasar, What is malware? Prevention, detection and how attacks work, Tech Target, july 2024, on site: https://www.techtarget.com/searchsecurity/definition/malware

شبكات Wi-Fi العامة

يعتمد العديد من المُستخدِمين على شبكات الإنترنت العامة في أماكن مثل المقاهي أو المطارات، لكن هذه الشبكات غالباً ما تكون غير مؤمَّنة بما يكفي، مما يجعلها بيئةً مثاليةً للمجرمين لاستغلال الأجهزة المتصلة بها. فعند الاتصال بشبكة لاسلكية غير محميَّة بشكلٍ كافٍ، يصبح من السهل على المهاجمين مراقبة حركة البيانات بين الجهاز والشبكة. وإذا كانت هذه البيانات غير مشفَّرة، يمكنهم الوصول إلى معلومات حسَّاسة مثل كلمات المرور، وأرقام البطاقات الائتمانية، وأي بيانات أخرى تُرسَل عبر الإنترنت.

ولمواجهة هذه المخاطر، يُعدّ استخدام شبكة افتراضية خاصة (VPN) من أفضل الطرق لحماية البيانات عند الاتصال بشبكات غير مؤمَّنة؛ حيث تعمل الـ VPN على تشفير حركة البيانات بين الجهاز والشبكة، مما يجعل من الصعب على المهاجمين التجسُّس عليها أو الوصول إليها؛ مما يوفّر مستوًى إضافياً من الأمان للمُستخدِمين في مثل هذه البيئات[1].

1. What is a VPN service?, Microsoft. On site: https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-vpn

الاستغلال النفسي والاجتماعي (الهندسة الاجتماعية)

الهندسة الاجتماعية نوع من الاحتيال يعتمد بشكل أساسي على استغلال الطبيعة البشرية وخداع الأفراد لتقديم معلومات حساسة دون أن يدركوا الخطر؛ حيث يستند المهاجمون في هذا الأسلوب إلى دراسة سلوكيات الضحايا والنواحي النفسية لإقناعهم بالكشف عن بياناتهم الشخصية. ومن أبرز الطرق التي يعتمدون عليها: انتحال الهُويَّة؛ حيث يتظاهر المجرمون بأنهم شخصيات موثوقة، مثل: موظفين في البنوك أو مسؤولين في شركات، ويستخدمون هذه الصفة لإقناع الأفراد بتسليم معلوماتهم. هذا الأسلوب يستغل الثقة والعلاقات الاجتماعية لتخطّي الحواجز الأمنية التقنية التي قد تكون موجودة.

بالإضافة إلى ذلك، يلجأ المهاجمون إلى إثارة الخوف أو الإيحاء بوجود حالة طارئة لجعل الضحايا يتصرَّفون بسرعة ودون تفكير، فقد يتلقَّى الشخص مكالمةً هاتفيةً تزعم أن حسابه المصرفي يتعرض لهجوم وأنه بحاجة لتقديم معلوماته على الفور لحمايته. تحت ضغط هذه الحالة الطارئة، يكون الضحايا أكثر عرضةً لاتخاذ قرارات غير مدروسة؛ مما يسهل على المهاجمين الوصول إلى بياناتهم الشخصية.

حقائق ومعلومات

الهندسة الاجتماعية مسؤولة عن 30% من الهجمات الإلكترونية الناجحة عالمياً.

ثالثاً: تأثيرات سرقة الهُويَّة

سرقة الهُويَّة هي جريمة تنطوي على عواقب خطيرة تتجاوز مجرد فقدان المعلومات الشخصية. فالتأثيرات المترتبة على سرقة الهُويَّة تشمل الجوانب المالية والنفسية والقانونية، وتتسبَّب في إلحاق أضرار طويلة الأمد بالأفراد والشركات على حَدٍّ سواء.

الأضرار المالية

تُعدّ الأضرار المالية أُولَى النتائج المباشرة لسرقة الهُويَّة؛ حيث يستغل المجرمون المعلومات المالية المسروقة -مثل بيانات الحسابات البنكية أو بطاقات الائتمان- لتحقيق مكاسب غير مشروعة. هذه الأضرار تتجلَّى في أشكال مختلفة، لكن أكثرها شيوعاً سرقة الأموال بشكل مباشر من حسابات الضحايا. فعندما يتمكَّن المجرمون من الوصول إلى بيانات الحسابات، يمكنهم سحب الأموال أو إجراء تحويلات مالية غير مصرَّح بها؛ مما يتسبَّب في نقص مفاجئ في الرصيد البنكي أو سرقة مبالغ كبيرة دون أي إنذار مُسبَق، وغالباً ما يكون من الصعب استعادة هذه الأموال بسرعة، إن لم يكن هذا مستحيلاً في بعض الحالات.

إلى جانب سرقة الأموال المباشرة، يتعرض الضحايا أيضاً لخطر تراكم الديون بسبب استخدام المجرِمين لهويَّتهم في فتح حسابات جديدة أو التقدم بطلبات للحصول على قروض أو بطاقات ائتمان. هذه الديون، التي لا يكون للضحايا أيّ علم بها، قد تؤدي إلى حدوث مشكلات مالية جسيمة؛ حيث يجد الضحايا أنفسهم مطالبين بسداد قروض لم يحصلوا عليها، أو محاصرين بديون تراكمت دون أي تدخُّل منهم. وهذه العواقب قد تستمر لفترات طويلة؛ حيث تتطلب الإجراءات القانونية والمالية وقتاً لحَلّها، مما يؤثر على السّجل الائتماني للضحايا ويعرّضهم لصعوبات مالية طويلة الأمد.

التأثيرات النفسية

لا تقتصر تأثيرات سرقة الهُويَّة على الأضرار المالية فحسب؛ بل تتجاوزها لتشمل تأثيرات نفسية عميقة وطويلة الأمد على الضحايا، فالتعامل مع عواقب هذه الجريمة يمكن أن يكون مرهقاً على المستوى النفسي؛ مما يترك أثراً دائماً على الصحة العقلية للمُتضرّرين.

أحد التأثيرات الرئيسية: القلق المستمر؛ حيث يعاني الضحايا من خوف دائم بشأن سلامة معلوماتهم الشخصية والمصرفية، ويبقى هذا القلق حاضراً حتى بعد اكتشاف السرقة، إذ يظل الخوف من تكرار الحادثة أو احتمال وقوع معلومات إضافية في أيدي المجرِمين مصدراً للتوتر المستمر. كما يشعر الضحايا بأنهم غير قادرين على حماية خصوصيَّتهم الرقمية؛ مما يزيد من مشاعر التوتر والارتياب في كل تعاملاتهم المُستقبَلية.

إضافة إلى ذلك، يعاني الضحايا من الشعور بفقدان السيطرة؛ حيث يواجهون إحساساً بالعجز حيال التحكم في معلوماتهم الشخصية. فإدراك أن شخصاً ما يمكنه استخدام هويَّتهم أو معلوماتهم المالية دون إذنٍ يجعل الضحايا يشعرون بفقدان التحكم في جوانب حياتهم. هذا الإحساس بالعجز قد يتفاقم ليؤدي إلى مشاعر الإحباط واليأس؛ مما يؤثّر بشكلٍ سلبيّ على الحياة اليومية للضحايا.

في بعض الحالات، يمكن أن يؤدي الضغط النفسي الناجم عن سرقة الهُويَّة إلى الاكتئاب والعزلة الاجتماعية. فيشعر الضحايا بأنهم مُستهدَفون ومُعرَّضون للخطر؛ مما يدفعهم إلى تجنُّب الأنشطة الرقمية والمصرفية التي قد تعرّضهم مرةً أخرى للسرقة، ويصبحون أكثر عزلة؛ حيث يتراجعون عن الانخراط في الحياة الاجتماعية أو التعامل مع التكنولوجيا بشكلٍ عام، مما يعمّق لديهم مشاعر الحزن واليأس.

التأثيرات على العمل والحياة المهنية

تُعدّ سرقة الهُويَّة من الجرائم التي لا تقتصر آثارها على الجوانب المالية أو النفسية فحسب، بل تمتد لتؤثّر بشكلٍ كبيرٍ على الحياة المهنية للضحايا. فعندما تُستخدَم هُويَّة شخصٍ ما في أنشطة غير قانونية أو احتيالية، يمكن أن تتسبَّب في تشويه سُمعته في مكان العمل؛ مما يؤدي إلى تعرُّضه لعواقب وخيمة في مسيرته المهنية.

ومن أحد الآثار الرئيسية لسرقة الهُويَّة: فقدان فُرَص العمل، فقد يواجه الضحايا صعوبةً في العثور على عمل إذا ارتبطت معلوماتهم الشخصية بقضايا قانونية تؤثّر على سُمعتهم المهنية. وفي حالات معينة، قد يتم استبعادهم من الوظائف عندما يتبيَّن للمسؤولين عن التوظيف أن سِجلّهم يحتوي على أنشطة مشبوهة. هذا الاستبعاد يمكن أن يكون مُحبِطاً للضحايا كَوْنهم غير مؤهَّلين بسبب أفعال لم يرتكبوها.

علاوةً على ذلك، فإن التأثيرات السلبية على التوظيف المستقبلي تُشكّل تحدياً آخر للضحايا، كما أنّ سرقة الهُويَّة قد تؤدّي إلى تدهور سِجلّهم الائتماني والقانوني؛ مما يجعل من الصعب الحصول على وظائف مستقبلية تتطلب فحص السجل الجنائي أو الائتماني. وفي العديد من الصناعات، تُعدّ هذه الفحوص جزءاً أساسياً من عملية التوظيف. وبالتالي، فإن وجود معلومات سلبية في السِّجل قد يؤدي إلى فقدان فرص وظيفية مهمّة.

هذا الأمر يُعقّد قدرة الضحايا على بناء مسار مهنيّ مُستقرّ؛ حيث يجدون أنفسهم عالقين بين تداعيات سرقة الهُويَّة والعواقب القانونية والاجتماعية الناتجة عنها. وفي ظل هذه الظروف، يتطلب الأمر جهداً كبيراً منهم لتجاوز هذه التحديات وإعادة بناء سُمعتهم المهنية، مما يجعل من الضروري تعزيز الوعي حول أهمية حماية الهُويَّة الشخصية، وكيفية التصدّي لتلك الجرائم.

02

الفصل الثاني

طرق الحـــــــــماية والإجراءات بعد سرقة الهُويَّة

- أولاً: **طرق الحماية من سرقة الهُويَّة.**
- ثانياً: **الإجراءات الواجب اتّخاذها بعد سرقة الهُويَّة.**

طرق الحماية والإجراءات بعد سرقة الهُوِيَّة

تُعدّ سرقة الهُوِيَّة من أخطر الجرائم الإلكترونية التي تهدّد الأفراد والمؤسسات على حَدٍّ سواء؛ حيث تؤدّي إلى أضرار مالية ونفسية وقانونية جسيمة. لذلك، يصبح من الضروري اتخاذ تدابير حماية استباقية لتقليل فرص الوقوع ضحيةً لهذا النوع من الجرائم. تشمل هذه التدابير الحفاظ على سرية المعلومات الشخصية، واستخدام كلمات مرور قوية ومتنوّعة، وتفعيل التحقق الثنائي للحسابات الحساسة. بالإضافة إلى ذلك، يجب على الأفراد الحرص على تحديث برامج الحماية بانتظام، وعدم مشاركة البيانات الشخصية عبر الإنترنت إلا مع جهات موثوقة.

أولاً: طرق الحماية من سرقة الهُوِيَّة

سرقة الهُوِيَّة تُمثّل أحد أبرز التهديدات في العصر الرقمي. ومع تزايد الاعتماد على الإنترنت في التعاملات المالية والشخصية، أصبح الحفاظ على هُوِيَّة الفرد الرقمية ضرورةً مُلحَّةً، إذ قد يتسبَّب الوصول غير المصرح به إلى البيانات الشخصية في أضرار مالية ونفسية جسيمة. لحُسْن الحظ، هناك مجموعة من الخطوات التي يمكن اتّخاذها لتعزيز مؤشرات السلامة الرقمية وتقليل خطر التعرض لسرقة الهُوِيَّة، وهي كالآتي:

استخدام كلمات مرور قوية ومُعقَّدة

تُعدّ كلمات المرور أول حاجز أمني أمام محاولات سرقة الهُويَّة، لذلك ينبغي الاهتمام بها بشكل كبير؛ حيث إنّ استخدام كلمات مرور ضعيفة أو متكرّرة يزيد من فرص تعرُّض الحسابات للاختراق[1].

مُتطلَّبات كلمة المرور القوية

يجب أن تتكوَّن كلمة المرور المثالية من مجموعة مُتنوّعة من الأحرف الكبيرة والصغيرة، والأرقام، والرموز الخاصة. فكلما كانت الكلمة أكثر تعقيداً، كان من الصعب على القراصنة اختراقها. كما يُفضَّل أن تكون كلمة المرور مكوَّنة من 12 حرفاً على الأقل؛ وذلك لتقليل احتمالية كشفها باستخدام أدوات التشفير العشوائي.

عدم تكرار كلمات المرور

يُعدّ استخدام كلمة المرور نفسها في أكثر من حساب خطأً شائعاً يقع فيه العديد من الأشخاص. فإذا تم اختراق أحد الحسابات، قد يتمكَّن المخترِق من الوصول إلى بقية الحسابات التي تستخدم كلمة المرور نفسها. لذلك، يُنصَح بإنشاء كلمات مرور فريدة لكل حساب أو خدمة.

استخدام أدوات إدارة كلمات المرور

لتجنُّب مشكلة نسيان كلمات المرور المعقَّدة، يمكن استخدام برامج إدارة كلمات المرور، التي تحفظ كلمات المرور بشكلٍ آمنٍ، وتُتيح للمُستخدِم إنشاء كلمات مرور جديدة معقَّدة لكل حساب. هذه الأدوات توفّر الحماية من خلال تشفير البيانات وإضافة طبقة حماية إضافية.

1. What Is Password Protection?, Proof Point, on site: https://www.proofpoint.com/au/threat-reference/password-protection

هل تعلم؟

أظهرت الدراسات أن 81% من حالات اختراق البيانات تعود إلى استخدام كلمات مرور ضعيفة أو مُعاد استخدامها[1].

تفعيل المصادقة الثنائية (Two-Factor Authentication)

من الوسائل المساعدة على تعزيز أمان الحسابات: تفعيل خاصية التحقُّق الثنائي، وهي نظام أمني يُضيف طبقة حماية إضافية بجانب كلمة المرور. حتى إذا تمكَّن المخترِق من معرفة كلمة المرور، فإن هذه الخاصية تَطلب منه خطوةً أخرى للتأكُّد من هُويَّة المُستخدِم.

كما يتطلَّب التحقق الثنائي إضافة خطوة ثانية لتسجيل الدخول، مثل إرسال رمز مؤقّت إلى الهاتف المحمول أو البريد الإلكتروني. وبالتالي، حتى إذا تم اختراق كلمة المرور، لن يتمكَّن المهاجم من الوصول إلى الحساب دون الوصول إلى الجهاز الآخر المستخدَم في التحقُّق.

1. Rob Sobers, Must-Know Data Breach Statistics, Varoni, September 2024, on site: https://www.varonis.com/blog/data-breach-statistics

أنواع التحقُّق الثُّنَائي

تتنوَّع أساليب التحقُّق الثُّنائي، وتشمل ما يلي:

- **الرسائل النصية القصيرة (SMS):** إرسال رمز مؤقّت إلى رقم هاتف المُستخدِم.
- **التطبيقات المخصَّصة:** مثل Google Authenticator أو Authy، التي تُولّد رموزاً مؤقّتة للمصادقة.
- **المصادقة البيومترية:** مثل استخدام بصمة الإصبع أو التعرُّف على الوجه؛ لتأكيد الهُويَّة.

إن تفعيل التحقق الثنائي يجعل من الصعب للغاية على القراصنة الوصول إلى الحسابات؛ حيث يضيف طبقةً إضافيةً من الأمان. كما أنّ العديد من الخدمات المصرفية، والشبكات الاجتماعية، وخدمات البريد الإلكتروني تدعم هذه الميزة، وينبغي تفعيلها في جميع الحسابات الممكنة[1].

هل تعلم؟

إضافة طبقة التحقق الثنائي يمكن أن تقلّل من احتمالية تعرُّض الحسابات للاختراق بنسبة تصل إلى 99%.

1. Biometric Verification, Login TC, on site: https://www.logintc.com/types-of-authentication/biometric-authentication/

تحديث البرامج وأنظمة الأمان

تُعدّ تحديثات البرامج وأنظمة الأمان من أهم الإجراءات الوقائية لحماية الهُويَّة الرقمية، والحفاظ على أمان الأجهزة والمعلومات الشخصية، فكثيراً ما تحتوي هذه التحديثات على تصحيحات للثغرات الأمنية التي يمكن للمهاجمين استغلالها لاختراق الأنظمة وسرقة البيانات.

إنّ أهمية تحديث البرامج تكمن في معالجة الثغرات التي قد تُكتشَف بمرور الوقت. فالبرامج القديمة، وخاصةً تلك التي لم تتلق تحديثات لفترات طويلة، غالباً ما تحتوي على ثغرات تجعلها عرضةً للهجمات الإلكترونية؛ حيث إن الشركات المطوّرة تعمل على إصدار تحديثات دورية لسَدّ تلك الفجوات الأمنية. فإذا تَجاهَل المُستخدِم تحديث برامجه وأنظمته، فإنه يظل عرضةً لهجمات قد يستغلّها القراصنة؛ مما يزيد من خطر سرقة الهُويَّة أو المعلومات الحسَّاسة.

أما بالنسبة لتحديثات أنظمة التشغيل، مثل Windows & macOS، فهي ضرورية لضمان الحماية من أحدث التهديدات الإلكترونية، ويُنصَح بتفعيل خاصية التحديثات التلقائية حتى يتم تثبيت التحديثات الأمنية على الفَوْر دون الحاجة لتدخُّل المستخدِم، وبذلك يتم تعزيز حماية النظام ضد التهديدات المتطورة.

إلى جانب أنظمة التشغيل، يجب تحديث التطبيقات والأدوات الأمنية بانتظام، والتطبيقات التي تتعامل مع البيانات الحساسة، مثل تطبيقات البنوك والتجارة الإلكترونية، تحتاج إلى التحديث بشكلٍ مستمرّ لضمان سد الثغرات الأمنية المحتملة. كما أن برامج الحماية من الفيروسات وجدران الحماية تحتاج إلى تحديثات دورية لتظل قادرةً على رصد ومكافحة أحدث التهديدات والبرمجيات الخبيثة[1].

بالمحصِّلة، تحديث البرامج بشكلٍ دوري يُعدّ أحد أهم التدابير الوقائية للحفاظ على أمان الهُويَّة الرقمية، وحمايتها من المخاطر المتزايدة.

هل تعلم؟

وفقاً للدراسات، 60% من حوادث الاختراق تعود إلى استغلال ثغرات في البرامج التي لم يتم تحديثها بشكلٍ صحيحٍ.

1. Application Security Tools – How and when to use them, jit, on site: https://www.jit.io/resources/appsec-tools

تجنُّب مشاركة المعلومات الشخصية بشكلٍ غير آمِن

إنّ مشاركة المعلومات الشخصية عبر الإنترنت أحد العوامل الرئيسية التي تؤدّي إلى سرقة الهُويَّة. ففي عصر التوسع الرقمي، يتعيَّن على المستخدِمين التعامل بحذرٍ مع أي طلب لمعلومات حساسة، والتأكد من أن الجهة أو الموقع الذي يطلب هذه المعلومات موثوق وآمِن، لضمان حماية البيانات من الاختراق.

ويُعدّ التحقق من المواقع الآمِنة خطوةً أساسيةً عند تقديم المعلومات الشخصية عبر الإنترنت، لذلك يجب التأكد من أن الموقع يستخدم بروتوكول HTTPS بدلاً من HTTP؛ حيث إن بروتوكول HTTPS يُوفّر اتصالاً مشفراً بين المُستخدِم والموقع، مما يقلل من احتمالية اعتراض القراصنة للبيانات. كما يمكن التحقق من هذا البروتوكول عن طريق البحث عن رمز القفل في شريط العناوين بجانب عنوان الموقع[1].

أيضاً، تجنُّب مشاركة المعلومات الحساسة عبر الرسائل غير الآمِنة هو أمر بالغ الأهمية، فالمعلومات -مثل أرقام الحسابات البنكية أو كلمات المرور- لا ينبغي مشاركتها عبر الرسائل النصية أو البريد الإلكتروني العادي؛ لأنها تكون عرضة للاختراق بسهولة. وفي حال الضرورة، يُفضَّل استخدام وسائل آمِنة ومشفَّرة مثل تطبيقات المحادثات المشفرة لتقليل مخاطر التسريب.

1. Use HTTPS across your website, on site: https://www.ownyouronline.govt.nz/business/get-protected/guides/benefits-of-using-https-across-your-website/

استخدام تقنيات التشفير

التَّشفير يُعدّ من أكثر الأساليب الفعّالة لحماية البيانات الشخصية والمعلومات الحساسة في أثناء نقلها عبر الإنترنت؛ حيث تعتمد هذه التقنية على تحويل البيانات إلى صيغة غير مفهومة؛ ممّا يجعلها عديمة الفائدة لأيّ طرف غير مُصرَّح له بالوصول إليها. حتى إذا تمكَّن القراصنة من اختراق البيانات المشفَّرة؛ فإنَّهم سيجدون صعوبةً كبيرةً في فَكّ تشفيرها وقراءتها[1].

وفي ظل التهديدات السيبرانية المتزايدة؛ أصبح التشفير أداةً أساسيةً لضمان حماية البيانات. على سبيل المثال، عند إرسال رسائل بريد إلكتروني تحتوي على معلومات حساسة، أو عند تخزين مستندات مُهمَّة على جهاز الحاسوب، يُوصَى بتطبيق تقنيات التشفير المناسبة لحماية تلك البيانات من الوصول غير المُصرَّح به.

بالإضافة إلى ذلك، تتبنَّى العديد من المنصات الرقمية أنظمة تشفير لضمان أمان الاتصالات والمعلومات، فضلًا عن خدمات البريد الإلكتروني -على سبيل المثال- التي تُتيح خيارات لتشفير الرسائل؛ ممّا يضمن أن محتواها يظلّ غير قابل للوصول إلا للأطراف المعنيَّة. كما أنّ تطبيقات المراسلة الحديثة تستخدم التشفير من طرف إلى آخر؛ ممّا يضمن أن الرسائل تظل مُشفّرةً من لحظة إرسالها حتى استلامها.

إنّ التشفير يُمثِّل حجر الزاوية في إستراتيجيات الأمن الرقمي الحديثة؛ حيث يُوفّر حمايةً فعّالةً ضد الهجمات الإلكترونية، ويضمن خصوصية البيانات في عالَم يزداد اعتماداً على التكنولوجيا.

1. Zoran Cocoara, Data Encryption: Protecting Sensitive Information in the Digital Age, End Point Protector, November 2023, on site: https://www.endpointprotector.com/blog/data-encryption-protecting-sensitive-information/

ثانياً: الإجراءات الواجب اتّخاذها بعد سرقة الهُويَّة

سرقة الهُويَّة يمكن أن تكون تجربة مُدمّرة تؤثّر على الجوانب المالية والشخصية. فعند تعرُّض الشخص لسرقة هُويَّته، من الضروري اتخاذ إجراءات سريعة لحماية المعلومات الشخصية والحد من الأضرار المحتملة. ولذلك هناك عدَّة خطوات يمكن اتّباعها في حال تعرُّضك لسرقة الهُويَّة:

1 الإبلاغ عن الجريمة

أوَّل خطوة يجب اتّخاذها عند اكتشاف سرقة الهُويَّة هي الإبلاغ عن الجريمة لوحدة إدارة مُكافَحة الجرائم الإلكترونية بوزارة الداخلية؛ فالإبلاغ السريع يمكن أن يمنع تفاقم المشكلة ويحمي الضحية من المزيد من الأضرار.

2 إبلاغ المؤسسات المالية

بعد الإبلاغ، يجب التواصل فوراً مع المصارف والمؤسسات المالية التي تدير الحسابات المتضررة؛ حيث يساعد الإبلاغ المبكّر على حماية الحسابات من أي عمليات غير مصرَّح بها. كما يجب على الضحية طلب تجميد أو إغلاق الحسابات المتأثّرة لتجنُّب أي استخدام غير قانوني لها.

3 إبلاغ مكاتب الائتمان

يجب أيضًا إبلاغ مكاتب الائتمان؛ حيث تستطيع هذه المكاتب وضع تنبيه على تقرير الائتمان الخاص بك، مما يعني أنه سيتم تنبيه أي مؤسسة ترغب في فتح حساب جديد باسمك بأنك ضحية لسرقة الهُويَّة. هذا الإجراء يساعد على تقليل فرص استغلال معلوماتك الشخصية في المستقبل.

4 تجميد الائتمان

تجميد الائتمان يُعدّ خطوةً أساسيةً لمنع الجناة من فتح حسابات جديدة أو إجراء معاملات باسمك باستخدام المعلومات المسروقة. هذا الإجراء يمنع أي شخص آخر من الوصول إلى تقريرك الائتماني دون موافقتك، وهو ما يجعل من الصعب على المجرمين الاستفادة من هويَّتك المسروقة.

احذر!

تجنَّب مشاركة معلوماتك على الشبكات العامة: إنّ الاتصال بشبكات Wi-Fi العامة غير المؤمَّنة يُعرّض بياناتك للسرقة. استخدِمْ شبكة افتراضية خاصة (VPN) لحماية بياناتك أثناء تصفُّح الإنترنت في الأماكن العامة[1].

5 مراقبة الائتمان

بعد الإبلاغ عن الجريمة وتجميد الائتمان، ينبغي مراقبة الائتمان لضمان عدم وجود أي أنشطة غير مشروعة مرتبطة بمعلوماتك الشخصية. فمِن خلال مراقبة حساباتك وتقارير الائتمان، يمكنك اكتشاف أي أنشطة مشبوهة في الوقت المناسب، واتخاذ الإجراءات اللازمة بسرعة.

6 المراقبة الذاتية

يمكنك أيضاً مراقبة تقريرك الائتماني بشكلٍ دوريّ من خلال الحصول على نسخة من التقرير من مكاتب الائتمان الكبرى. في بعض الدُّوَل، يحق للمستهلِكين الحصول على تقرير ائتماني مجاني مرة واحدة سنوياً. ومن خلال مراجعة التقرير بانتظام، يمكن اكتشاف أي أنشطة غير مألوفة والتصرف بناءً على ذلك.

7 التحذيرات المُبكّرة

مراقبة الائتمان تساعد في اكتشاف الجرائم في وقت مُبكّر قبل أن تتفاقم الأمور. إذا لاحظت أي نشاط غير معتاد مثل زيادة كبيرة في الرصيد المستحق أو فتح حسابات جديدة دون إذنك، يجب عليك الإبلاغ عن هذه الأنشطة فوراً للمصارف المعنية، واتخاذ الإجراءات اللازمة.

1. Andra Zaharia, The Dangers of Using Public Wi-Fi, Aura , January 2023, on site: https://www.aura.com/learn/dangers-of-public-wi-fi.

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

التمرين الأول

اكتب كلمة (صحيح) أمام العبارة الصحيحة، وكلمة (خطأ) أمام العبارة الخطأ، مع تصحيح الخطأ إن وُجِدَ

1. سرقة الهُويَّة تحدث عند استخدام بيانات شخص آخر لأغراض قانونية.
2. استخدام كلمات مرور قوية ومُعقَّدة يمكن أن يُقلّل من احتمالية سرقة الهُويَّة.
3. الاتصال بشبكات Wi-Fi العامة لا يُشكِّل خطراً على سرقة الهُويَّة.
4. التصيد الاحتيالي هو أسلوب يستخدمه المحتالون للحصول على بيانات شخصية من خلال التنكر في صورة جهات موثوقة.

5. برامج إدارة كلمات المرور يمكنها حفظ كلمات المرور بشكل آمِنٍ وتشفيرها.

6. المجرمون الإلكترونيون يعتمدون بشكلٍ أساسي على الثغرات التقنية، ولا يستغلون الجانب النفسي للضحايا.

7. استخدام كلمة مرور واحدة لجميع الحسابات يُعزّز الأمان.

8. التشفير لا يُعدّ وسيلةً فعالةً لحماية البيانات أثناء نقلها عبر الإنترنت.

التمرين الثاني

- **اختر الإجابة الصحيحة**

1. من أحد أساليب حماية الهُويَّة الرقمية:

1. استخدام كلمة المرور نفسها لكل حساب.
2. استخدام كلمات مرور مُعقَّدة.
3. عدم تحديث البرامج.

2. أيّ من الآتي هو مثال على هجوم التصيد الاحتيالي؟

1. رسالة بريد إلكتروني من صديق.
2. رسالة بريد إلكتروني تبدو من بنك تطلب معلوماتك المالية.
3. زيارة موقع ويب حكومي.

3. ما هو الهدف الأساسي من سرقة الهُويَّة؟

1. الحصول على بيانات مالية.
2. التعرف على معلومات شخصية فقط.
3. فتح حسابات قانونية.

4. ما هي الطريقة الأكثر أماناً لاستخدام شبكة Wi-Fi عامة؟

1. الاتصال مباشرةً بالشبكة.
2. استخدام VPN.
3. عدم استخدام الشبكة مطلقاً.

5. ما هو بروتوكول الأمان الذي يجب التأكد من وجوده عند استخدام موقع ويب؟

1. HTTP
2. HTTPS
3. FTP

6. ما الذي يساعد في منع سرقة الهُويّة؟

1. عدم مراقبة الحسابات المالية.
2. مراقبة الحسابات الائتمانية بانتظام.
3. فتح حسابات جديدة باستمرار.

7. أيّ من الآتي يُعبّر عن "الهندسة الاجتماعية"؟

1. اختراق نظام بنكي.
2. إقناع الضحايا بتقديم معلوماتهم الشخصية.
3. تحديث الأنظمة الأمنية.

التمرين الثالث

أكمل العبارات الآتية

1. التحقق الثنائي يضيف ..... إضافية لحماية الحسابات من سرقة الهُويَّة.
2. استخدام ..... يساعد في حماية البيانات عند الاتصال بشبكات Wi-Fi العامة.
3. يُعد ..... من أهم وسائل الحماية ضد سرقة الهُويَّة عبر الإنترنت.
4. يجب تجنُّب استخدام ..... في أكثر من حساب واحد لتقليل خطر الاختراق.
5. عند استلام رسالة بريد إلكتروني تطلب معلومات شخصية، يجب التحقق من ..... للتأكد من صحته.
6. التصيد الاحتيالي يتم من خلال إرسال ..... تبدو من جهات موثوقة لخداع الضحية.
7. برامج إدارة كلمات المرور تحفظ كلمات المرور وتقوم ..... بتشفيرها.
8. تحديثات البرامج تساعد على سَدّ ..... الأمنية.

حلّ التمارين والتدريبات

السؤال

التمرين الأول: اكتب كلمة (صحيح) أمام العبارة الصحيحة، وكلمة (خطأ) أمام العبارة الخطأ، مع تصحيح الخطأ إن وُجِدَ

الإجابة

1. **خطأ:** سرقة الهُويَّة تحدث لأغراض احتيالية أو غير قانونية.
2. **صحيح.**
3. **خطأ:** الاتصال بشبكات Wi-Fi العامة يُعرّض البيانات للسرقة إذا لم يتم استخدام شبكة VPN.
4. **صحيح.**
5. **صحيح.**
6. **خطأ:** يعتمدون أيضًا على الهندسة الاجتماعية واستغلال الثقة والخوف.
7. **خطأ:** استخدام كلمة مرور واحدة يُعرّض جميع الحسابات للخطر إذا تم اختراق أحدها.
8. **خطأ:** التشفير هو من أكثر الوسائل فعالية لحماية البيانات.

السؤال

التمرين الثاني: اختر الإجابة الصحيحة

الإجابة

1. من أحد أساليب حماية الهُويَّة الرقمية:

   الإجابة: استخدام كلمات مرور مُعقَّدة.

2. أي من الآتي هو مثال على هجوم التصيد الاحتيالي؟

   الإجابة: رسالة بريد إلكتروني تبدو من بنك تطلب معلوماتك المالية.

3. ما هو الهدف الأساسي من سرقة الهُويَّة؟

   الإجابة: الحصول على بيانات مالية.

4. ما هي الطريقة الأكثر أماناً لاستخدام شبكة Wi-Fi عامة؟

   الإجابة: استخدام VPN

5. ما هو بروتوكول الأمان الذي يجب التأكد من وجوده عند استخدام موقع ويب؟

   الإجابة: HTTPS

6. ما الذي يساعد في منع سرقة الهُويَّة؟

   الإجابة: مراقبة الحسابات الائتمانية بانتظام.

7. أيّ من الآتي يُعبّر عن "الهندسة الاجتماعية"؟

   الإجابة: إقناع الضحايا بتقديم معلوماتهم الشخصية.

السؤال

التمرين الثالث: أكمل العبارات الآتية

الإجابة

1. التحقق الثنائي يضيف **طبقة أمان** إضافية لحماية الحسابات من سرقة الهُويَّة.
2. استخدام **VPN** يساعد في حماية البيانات عند الاتصال بشبكات Wi-Fi العامة.
3. يُعدّ **التشفير** من أهم وسائل الحماية ضد سرقة الهُويَّة عبر الإنترنت.
4. يجب تجنُّب استخدام **نفس كلمة المرور** في أكثر من حساب واحد لتقليل خطر الاختراق.

5 عند استلام رسالة بريد إلكتروني تطلب معلومات شخصية، يجب التحقق من **المصدر** للتأكد من صحته.

6 التصيد الاحتيالي يتم من خلال إرسال **رسائل بريد إلكتروني** تبدو من جهات موثوقة لخداع الضحية.

7 برامج إدارة كلمات المرور تحفظ كلمات المرور وتقوم **آلياً** بتشفيرها.

8 تحديثات البرامج تساعد على سد **الثغرات** الأمنية.

المراجع

1. What is Impersonation in Cybersecurity? Zero Fox, on site: https://www.zerofox.com/glossary/impersonation-in-cybersecurity/
2. Kyle Chin, What is an Impersonation Attack?, september 2024. on site: https://www.upguard.com/blog/impersonation-attack#:~:text=An%20impersonation%20attack%20is%20a%20type%20of%20targeted%20phishing%20attack
3. Email Impersonation Attacks, Proof Point, on site: https://www.proofpoint.com/us/threat-reference/impersonation-attack
4. Impersonation Attack. follow link: https://www.mimecast.com/content/impersonation-attack/
5. Stouffer, Clare. 139 password statistics to help you stay safe in 2024 Norton, june 2023, on site: https://us.norton.com/blog/privacy/password-statistics
6. Kinza. Yasar, What is malware? Prevention, detection and how attacks work, Tech Target, july 2024, on site: https://www.techtarget.com/searchsecurity/definition/malware

7. What is a VPN service?, Microsoft. On site: https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-vpn

8. What Is Password Protection?, Proof Point, on site: https://www.proofpoint.com/au/threat-reference/password-protection

9. Rob Sobers, Must-Know Data Breach Statistics, Varoni, September 2024, on site: https://www.varonis.com/blog/data-breach-statistics

10. Biometric Verification, Login TC, on site: https://www.logintc.com/types-of-authentication/biometric-authentication/

11. Application Security Tools – How and when to use them, jit, on site: https://www.jit.io/resources/appsec-tools

12. Use HTTPS across your website, on site: https://www.ownyouronline.govt.nz/business/get-protected/guides/benefits-of-using-https-across-your-website/

13. Zoran Cocoara, Data Encryption: Protecting Sensitive Information in the Digital Age, End Point Protector, November 2023, on site: https://www.endpointprotector.com/blog/data-encryption-protecting-sensitive-information/

14. Andra Zaharia, The Dangers of Using Public Wi-Fi, Aura , January 2023, on site: https://www.aura.com/learn/dangers-of-public-wi-fi


الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency
الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy
المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative