الوقاية من القرصنة وانتحال الشخصية

من بالغ الأهمية أن يكون الوصول إلى حساباتك آمناً للوقاية من القرصنة، وانتحال الشخصية، وغيرها من أشكال سرقة الهوية.

قد تتفاجأ/ين إذا علمت إلى أي مدى تساهم القواعد السليمة المتعلقة بكلمات المرور في الحفاظ على أمنك. أما إذا كنت تتلقى/ين نصائح في الأمن السيبراني من كل حدب وصوب، فلا بأس إن شعرت بالخوف والارتباك. في هذا الإطار، يُقصد بالنصائح الواردة أدناه أن تبدّد الغموض المتعلق بهذه العملية. يمكنك العمل بها كلها معاً أو تطبيقها بشكل تدريجي. ولكل تفصيل بسيط أهميته في تعزيز أمنك. فإذا كنت بحاجة إلى مساعدة لتطبيق أيّ من التوجيهات الواردة أدناه، أو كنت تريد/ين التعمّق أكثر في هذا الموضوع، راجع/ي هذه الكتيّبات التدريبية والقوائم المرجعية ، التي أعدّها الفريق التقني في منظمة الحماية الرقمية.

- **اختر/اختاري كلمات مرور صعبة.** بحسب شروط إنشاء كلمات المرور التي تعتمدها الكثير من المواقع الإلكترونية اليوم، يجب أن تتألّف كلمة المرور القوية من ستة عشر حرفاً على الأقل، وأن تتضمّن مزيجاً من الأحرف الكبيرة والصغيرة، والرموز، والأرقام. قد تشعر/ين بتمييل إلى استخدام أسماء وأماكن معروفة في كلمات المرور الخاصة بك، أو إلى استبدال أحرف برموز تشبهها مثل "@" بدل حرف " a"، أو "3" بدل "E". لكن *قاوم/ي هذا الشعور*. عوضاً عن ذلك، نزّل/ي برنامجاً لإدارة كلمات المرور (راجع/ي أدناه).

- **حاول/ي اتّباع قاعدة واحدة بواحدة.** تشدّد منظمة الدفاع عن النفس ضد الرقابة، في دليلها إلى الأمان على الإنترنت، على أهمية اختيار كلمة مرور مختلفة لكل حساب. لا تنس/ي كمّ الحسابات المختلفة الموجودة لديك مثل البريد الإلكتروني، وحسابات مواقع التواصل الاجتماعي، و حسابك المصرفي ، وبطاقات الائتمان، والتأمين الصحي، واشتراكات التلفزيون وقنوات الأفلام، واشتراكات المبيع بالتجزئة، والأعمال الخيرية و التطوعي. بطبيعة الحال، من الصعب أن تتذكّر/ي كلمات المرور الخاصة بكل من هذه الحسابات، لذا فكّر/ي في استخدام برنامج آمن لإدارة كلمات المرور (راجع/ي أدناه). تذكّر/ي أنّ كل تفصيل مهمّ: ابدأ/ي بوضع كلمات مرور جديدة ومميّزة لأهم حساباتك وأكثرها حساسية (مثل بريدك الإلكتروني، و حساباتك المالية، وحسابات وسائل التواصل الاجتماعي)، ثم انطلق/ي من هناك. نوصيك بتحديث كلمات المرور كل ستة

أشهر. للحصول على المزيد من المعلومات والتوجيهات المعمّقة، يمكنك متابعة دورات مجانية حول تقنيات الأمن الرقمي من خلال مشروع توتم.

- **استخدم/ي برنامجاً آمناً لإدارة كلمات المرور.** قد يُخيّل إليك أنّ وضع كلمة مرور مميّزة لكلّ حساب، وتذكّرها، أشبه بمهمّة لا تنتهي أبداً. لذلك، تساعد برامج إدارة كلمات المرور على توليد كلمات مرور عشوائية، تكون على درجة عالية من الأمان، كما تقوم بحفظها في مكان آمن، لتخفيف هذا العبء عن ذاكرتك. وتتولى ملحقات متصفحات الويب والتطبيقات الهاتفية تبسيط هذه العملية برمّتها، من خلال ملء أسماء المستخدم وكلمات المرور بشكل تلقائي بمجرّد تسجيل دخولك. من المنطقي تماماً أن تبدي تحفظك بشأن تخزين كل كلمات المرور الخاصة بك في مكان واحد، لذا من الضروري أن تفهم/ي أنّ برامج إدارة كلمات المرور ليست كلها متساوية. فالجيّد منها يشفّر كلمات المرور، بحيث تظهر كرموز مبعثرة إذا تعرّضت مؤسستك لانتهاك أمني. من الأدوات المجانية التي يمكنك استخدامها لتخزين كلمات المرور وإدارتها بأمان "Bitwarden" و"keepassxc".

- **استخدم/ي المصادقة الثنائية** عادةً ما تقدّم مواقع البريد الإلكتروني ووسائل التواصل الاجتماعي وغيرها، توفر للمستخدم خيار تشغيل خاصية التحقق بخطوتين. هذه الخاصية هي طبقة من الأمن تتطلب منك استلام رمز، أو المصادقة على وصولك انطلاقاً من جهاز آخر، وذلك قبل تسجيل الدخول إلى حسابك. فإذا حاول شخصاً ما بالدخول إلى حسابك، لن يتمكّن من اجتياز عملية التحقق إذا لم يكن بوسعه الوصول إلى جهازك الثاني، الذي يكون في معظم الحالات هاتفك المحمول- وهو جهاز يكون من حولك في جميع الأوقات. لتجنّب أي مخاطر أمنية يمكن أن يتعرّض لها هاتفك المحمول، استخدم/ي تطبيقاً للمصادقة، مثل أداة المصادقة من غوغل أو ديو موبايل (Duo Mobile)، عوضاً عن استخدام رقم هاتفك المحمول، بهدف المصادقة على الدخول. في ما يلي قائمة بالأدلة التي يمكنك استخدامها لربط حساباتك المختلفة بتطبيق للمصادقة:
  - جيميل
  - فايبسوك
  - تويتر
  - إنستاغرام
  - هوتميل
  - سنابتشات

- **ابتكر/ي إجابات جديدة عن سؤال الأمان.** تشترط الكثير من المواقع الإلكترونية أن تختار/ي سؤال أمان للإجابة عنه في حال نسيت كلمة المرور. تميل الأسئلة إلى أن تكون بسيطة وشخصية، مما يعني أنه قد يكون من السهل على المهاجم أن يجد الإجابة من خلال البحث في محرّك غوغل. حاول/ي أن تصعّب/ي الإجابات عن هذه الأسئلة، أو اختر/اختاري سؤالاً لا يمكن البحث عن إجابته عبر غوغل. في هذا الإطار، توصيك صفحة "Security Box" بتخزين إجاباتك من خلال برنامج إدارة كلمات المرور، حتى وإن كنت تتمتع/ين بذاكرة قوية. فالإجابة عن أسئلة عامة مثل "ما هي فاكهتك المفضّلة" أو "اسم المدرسة الابتدائية التي التحقت بها" سيجعلك أكثر عرضة للانتهاكات الأمنية.
- **تحقّق/ي إذا كانت البيانات المتعلقة بحساباتك قد تعرّضت للاختراق.** عندما تفتح/ين حساباً بغية استخدام منتج، فأنت لا تكتفي/ن بإنشاء اسم مستخدم وكلمة مرور، بل تُدخل/ين مجموعةً متنوّعةً من المعلومات الشخصية الأخرى. فإذا تعرّضت بيانات تلك الشركة للاختراق، قد ينكشف أمر كلمة المرور الخاصة بك، ويتمّ تسريب معلوماتك على الويب. استخدم/ ي أدوات مثل "Have I Been Pwned" أو "Firefox Monitor"، ثم أدخل/ي عناوين البريد الإلكتروني الخاصة بك، لتتبيّن/ي إذا بياناتك تعرّضت للاختراق. فإذا حدث ذلك، ستتمكّن/ين من رؤية أيّ حسابات تعرّضت للانتهاك. عليك إذاً بتغيير كلمات المرور الخاصة بهذه الحسابات فوراً، وعدم استخدامها في أي مكان آخر مجدّداً.
- **تنبّه/ي من البريد المزعج والتصيّد.** كن/ كوني حذراً/ة عند فتح الرسائل الإلكترونية غير المتوقعة أو غير المرغوب فيها. لا تفتح/ي أي مستندات مرفقة أو روابط غير مرغوب فيها من دون أن تتحقّق/ي من المرسل أولاً. إذا تلقّيت رسالةً إلكترونيةً تتضمّن مستنداً مرفقاً أو رابطاً من أصدقاء لم تتوقع منهم شيأ"، من المفيد أن ترسل إليهم رسالةً نصيةً سريعة للتأكّد من قد أرسلهافعلاً. يمكنك استخدام هذا الاختبار كأداة للتعرّف على البريد المزعج والضارّ بشكل أفضل.
- **اطلب/ي من المؤسسة حيث تعمل/ين، أو الجامعة، أو المنظمة التي تتطوّع/ين فيها عدم نشر معلومات الاتصال بك في أدلتها الإلكترونية.** راجع/ي هذا الدليل الميداني الذي يقدّم توجيهات حول كيفية التحدّث إلى أصحاب العمل وزملاء المهنة إذا كنت بحاجة إلى نصائح لمناقشة التحرّش الإلكتروني بصفة رسمية.

تمّ تعديل التوجيهات الواردة أعلاه بالتشاور مع خبراء في مجال الأمن السيبراني من ومؤسسة حرية الصحافة و"نادي القلم أميركا".