

4 طرق يسيرة للبقاء آمنًا على الإنترنت

فحماية وجودنا على الإنترنت أمر حتمي. فثمة بضع خطوات يسيرة لنا فعلها لضمان أمان معلوماتنا ممن يتمنون سرقتها.



رصد محاولات التّصيّد والإبلاغ عنها

تقع أنجح الاختراقات عبر الإنترنت نتاج تنزيل مستلم ما رسالة "تصيدية" لبرمجية خبيثة أو تقديم بياناته الشخصية لمُرسل البريد العشوائية (سبام). فلا تنقر على رسائل محاولات التصيد هذه أو حتى تتفاعل مع أي منها. إنما، ارصدهم بملاحظة استخدامهم للغة تنبيهية أو تقديمهم لعروض تفوق حد التصديق.

بلّغ عن حالة التصيد واحذف رسائلها.

ضع كلمة مرور قوية

فكلمات المرور الضعيفة يسير تخمينها. كَوّن كلمات مرور حساباتك من 16 رمزًا في الأقل، وعشوائية، وفريدة من حساب لآخر. استعن بِمُنظّم لكلمات المرور، وهو برمجية تأمينية تُنشئ كلمات المرور وتصونها. فهذه البرمجية سهلة الاستخدام ستحتفظ بكلمات مرور حساباتك وتملأ بها الحقول آليًا عند اللزوم.

فَعَلِ المُصادقة متعددة العناصر (MFA)

استعن بـMFA على أي موقع إلكتروني يقدمها. توفر MFA حاجزًا آمنًا زائدًا بالإضافة إلى كلمة المرور عند تسجيل الدخول إلى الحسابات والتطبيقات مثل مسح الوجه أو رمز يُرسل نصًا.

الاستعانة بـMFA سيقلل كثيرًا من احتمالية اختراقك.



حدّث البرمجية

كلما تُرسل لنا الأجهزة أو التطبيقات أو البرمجيات (لا سيما برمجيات مكافحة الفيروسات) إشعارات بتوافر تحديثات، ينبغي لنا تثبيت تلك التحديثات في أقرب فرصة. فالتحديثات تصحح الأخطاء الترميزية الأمنية لتحسين حماية بياناتنا.

فعلّ التحديثات التلقائية لتيسّر الأمر.



تنفيذ تلك الإجراءات يساعد على تأمين عالمنا.



لكل منا مساعدة الآخر على
البقاء أمنين على الإنترنت، فشارك بهذه
النصائح مع أفراد أسرتك وأصدقائك!

cisa.gov/SecureOurWorld