خطوة بخطوة كيفية تحمي نفسك من الهجمات الإلكترونية؟

الخميس 16 أكتوبر 2025 06:00 م

تتزايد المخاوف بين مستخدمي شبكة الإنترنت ومنصات التواصل الاجتماعي من انتشار الهجمات الإلكترونية والاستيلاء على بياناتهم الشخصية لاستغلالها بشكل سيء

ويقدم خبراء الأمن السيبراني، مجموعة من النصائح للحماية من مثل هذه الهجمات، على النحو التالي:

1. المكالمات والرسائل العشوائية
كن حذرًا من أي مكالمات أو رسائل نصية واردة من أرقام عشوائية (أو حتى أرقام يُزعم أنها "موثوقة").

يجب عليك تغيير كلمة مرور الحساب الخاص بك إذا شككت أنك مستهدف إذا كنت تستخدم كلمة مرور مماثلة لحسابات أخرى، أو حسابًا مشابهًا، فتأكد من تغييرها أيضًا

فكر في تغيير كلمات المرور الخاصة بك لـ:
حساباتك المصرفية
البريد الإلكتروني
الخدمات الحكومية
حسابات التواصل الاجتماعي
وإذا أدى تغيير كلمة المرور إلى ظهور مطالبة تطلب منك تسجيل الخروج من هذا الحساب على جميع الأجهزة الأخرى، فقل نعم

2. تحقق من قوة كلمات المرور
عند اختيار كلمة مرور، تذكر: كلما كانت أطول، كانت أقوى كلمة المرور القوية لا تقل عن 14 حرفًا ويصعب تخمينها أو قم بترقية تدابير الأمن السيبراني لديك باستخدام عبارة مرور

3. تجنب كلمات المرور السهلة
تعتبر كلمات المرور التالية هي الأكثر شيوعًا والأسهل في الاختراق - لذا إذا كنت تستخدمها، فيجب أن تفكر بجدية في تغييرها بسرعة!

123456 (أو أي أرقام مرتبة ترتيبًا زمنيًا)
987654321
123123
111111

4. استخدم مدير كلمات المرور
هل سئمت من محاولة تذكر جميع كلمات المرور الخاصة بك، أو الاضطرار إلى تغييرها في كل مرة تقوم فيها بتسجيل الدخول؟

اختر مدير كلمات مرور لتخزين كلمات المرور وإنشائها بأمان إذ لن تحتاج سوى إلى تذكر كلمة مرور رئيسة واحدة بعد إعدادها

سيساعدك مدير كلمات المرور على إنشاء كلمات مرور فريدة ومعقدة لحساباتك الشخصية والعملية كما يخزنها مدير الحسابات بأمان داخل نظامه، ويُدخلها في مواقع الويب عند تسجيل الدخول

5. استخدم المصادقة متعددة العوامل
لمزيد من الأمان، ينصح باستخدام المصادقة الثنائية، وهي تُضيف طبقة أمان إضافية لمواقع الويب، ما يُمكّنك من تأكيد هويتك

هناك عدة طرق قد يُطلب منك فيها إثبات هويتك، ولكن هاتفك عادةً ما يكون المفتاح يمكنك تسجيل الدخول إلى حسابك المصرفي، ليُطلب منك إدخال رقم التعريف الشخصي (PIN). أو قد يُطلب منك استخدام تطبيق مصادقة متعددة العوامل (MFA) مثل Microsoft Authenticator للوصول إلى رسائل البريد الإلكتروني الخاصة بالعمل

6. لا تثق بأحد **(عبر البريد الإلكتروني أو الهاتف أو الرسائل النصية)**
احذر دائمًا من رسائل البريد الإلكتروني المُضلِّلة وصفحات الويب المُخترَقة (مثل البريد العشوائي والتصيُّد الاحتيالي). التفاعل مع هذه الرسائل يُعرِّض معلوماتك للخطر، وقد يُؤدِّي إلى تنزيل الفيروسات لذا ينصح بالآتي:
لا تفتح رسائل البريد الإلكتروني من عناوين بريد إلكتروني غير معروفة
مرفقات سلة المهملات في رسائل البريد الإلكتروني غير المتوقعة
تجنب النقرات الخطرة - بدلاً من ذلك اكتب العنوان في متصفحك

احمِ نفسك من الهجمات الإلكترونية بالتنبه لأي رسائل نصية قد تتلقاها، خاصةً إذا طلبت منك إدخال بيانات بطاقتك الائتمانية

على سبيل المثال، إذا اتصل بك أحد موظفي البنك وترك لك رسالة ورقمًا، فتأكد دائمًا من التحقق من الرقم عبر الإنترنت قبل الاتصال مرة أخرى.

ومهما فعلت، لا تُفصح عن أية معلومات شخصية عبر الهاتف أو البريد الإلكتروني، إلا إذا كنت متأكدًا تمامًا من سلامتها.

إذا اتصل بك شخص ما هاتفيًا يطلب معلومات شخصية، فاطلب اسمه ورقم هاتفه، وأخبره أنك ستتصل به لاحقًا.

7. تأمين جهازك
إذا كان جهازك المحمول غير آمن أو مفقودًا أو مسروقًا، فيمكن استخدامه للوصول إلى معلوماتك أو أموالك أو سرقة هويتك والبيانات التي لا يمكن استبدالها مثل الصور أو الرسائل.

تأمين أجهزتك عن طريق:
تثبيت برنامج مكافحة الفيروسات
تعيين كلمة مرور أو إيماءة أو بصمة إصبع يجب إدخالها لفتح القفل
ضبط الجهاز لطلب كلمة مرور قبل تثبيت التطبيقات
ترك البلوتوث مخفيًا عند عدم استخدامه وتعطيل الاتصال التلقائي بالشبكات
تمكين وظائف القفل و/أو المسح عن بعد، إذا كان جهازك يدعمها.

8. تحديث البرامج
تأكد من تحديث نظام البرامج على أجهزتك بانتظام - هاتفك، جهازك اللوحي، وجهاز الكمبيوتر المحمول.

قم بتحديث تطبيقاتك وتصفحك للويب بأحدث إصدار من متصفحك. وايضًا، برنامج مكافحة الفيروسات، الذي يُسهم بشكل كبير في حمايتك من الهجمات الإلكترونية.

9. انتبه جيدًا لعناوين **URL** الخاصة بمواقع الويب
فغالبًا ما تستخدم المواقع الضارة تهجئة مختلفة، أو نطاقًا مختلفًا (مثل .org بدلًا من .com) لخداع مستخدمي الإنترنت.

وقم بتنزيل الملفات من المواقع الموثوقة فقط، وإلا فقد تحتوي على فيروس مصمم للتجسس عليك أو المطالبة بمبلغ مالي للسماح لك مجددًا باستخدام جهاز الكمبيوتر الخاص بك.