نشرة توعوية · الأمن السيبراني

دليل أفضل كلمات المرور

كيف تصنع كلمة مرور لا تُكسر، وتحميها من التسريب والتصيّد — في عشر دقائق قراءة.

الإصدار ٠١ · صفر ١٤٤٨هـ

منصة توعية للتوعية بالأمن السيبراني

awareness-ksa.com

في هذه النشرة

لتحديث الأرقام في وورد: اضغط على الفهرس ثم F9.

كلمة المرور هي الباب الأول

أغلب الاختراقات لا تبدأ بثغرة معقّدة، بل بكلمة مرور ضعيفة أو مُعاد استخدامها. الباب الذي تحرسه بنفسك أقوى من أي جدار.

هذه النشرة تختصر لك ما تحتاج معرفته فعلًا: كيف يفكّر المهاجم، وما الذي يجعل كلمة المرور صامدة، وكيف تدير عشرات الحسابات دون أن تحفظ عشرات الكلمات.

٠١ · لماذا تُستهدف كلمات المرور؟

المهاجم لا يبحث عن التحدي، بل عن أقصر مسافة. وكلمة المرور المُعاد استخدامها تمنحه مفتاحًا واحدًا يفتح عدة أبواب دفعة واحدة.

المؤشّر	الدلالة
٨٠٪	من الاختراقات سببها بيانات دخول ضعيفة أو مسروقة
٦٥٪	من المستخدمين يعيدون استخدام الكلمة نفسها
ثانية	هو زمن كسر كلمة من ٦ خانات أرقام فقط

أثر الدومينو

تسريب موقع تسوّق قديم قد يفتح بريدك، وبريدك يفتح كل شيء آخر لأنه بوابة استعادة الحسابات.

ماذا يريد المهاجم؟

- بياناتك الشخصية لبيعها أو لانتحال هويتك.
- بريدك كنقطة انطلاق لاستهداف زملائك وجهات عملك.
- وصولًا إلى أنظمة جهة عملك عبر حسابك الشخصي.

المصدر: تقارير تحليل حوادث الاختراق السنوية — أرقام تقريبية للتوعية.

٠٢ · أربع طرق يُكسر بها حسابك

كل طريقة لها دفاع مختلف. الطول يهزم التخمين، والتفرّد يهزم التسريب، والتحقق بخطوتين يهزم التصيّد.

الطريقة	الدفاع
التخمين الآلي — تجربة ملايين الاحتمالات في الثانية	الطول قبل التعقيد
حشو بيانات التسريب — كلمة مسرّبة تُجرَّب في مواقع أخرى	كلمة مختلفة لكل حساب
التصيّد الاحتيالي — صفحة مزيّفة تطلب بياناتك	تحقّق من الرابط قبل الكتابة
الهندسة الاجتماعية — استدراجك بالثقة أو الاستعجال	لا تشارك رمزًا أو كلمة

علامة تحذير

أي رسالة تستعجلك وتطلب كلمة المرور أو رمز التحقق — هي محاولة احتيال حتى يثبت العكس. الجهات الرسمية لا تطلبها أبدًا.

٠٣ · مواصفات كلمة المرور القوية

1. **الطول أولًا — ١٦ خانة فأكثر**

   كل خانة إضافية تضاعف الجهد على المهاجم أضعافًا. الطول أقوى من الرموز الغريبة.

2. **فريدة لكل حساب**

   كلمة واحدة مكرّرة تعني أن تسريبًا واحدًا يسقط كل حساباتك دفعة واحدة.

3. **بلا معلومات شخصية**

   الاسم، تاريخ الميلاد، اسم النادي أو الأبناء — كلها أول ما يُجرَّب.

4. **بلا أنماط لوحة المفاتيح**

   مثل qwerty أو ١٢٣٤٥٦ أو P@ssw0rd — موجودة في أول قوائم التخمين.

5. **غيّرها عند الاشتباه فقط**

   التغيير الدوري الإجباري يدفع الناس لكلمات أضعف. غيّرها عند التسريب أو الشك.

> «كلمة مرور طويلة يسهل تذكّرها، خير من قصيرة معقّدة تُكتب على ورقة.»

٠٤ · طريقة عبارة المرور

بدل أن تخترع رموزًا لن تتذكّرها، ابنِ جملة من كلمات غير مترابطة — طويلة، سهلة عليك، مستحيلة على الآلة.

1. **اختر أربع كلمات لا رابط بينها**

   مثال: قمر · مفتاح · رمّان · مجداف. كلما قلّ الترابط، زادت القوة.

2. **اربطها بفاصل ثابت**

   استخدم شرطة أو نقطة بينها لزيادة الطول وتسهيل الكتابة.

3. **أضف بصمة الموقع**

   حرفان من اسم الخدمة داخل العبارة يجعلها فريدة لكل حساب دون جهد حفظ إضافي.

النتيجة

Qamar-Miftah7-Rumman-Mijdaf

٢٧ خانة · سهلة التذكّر · لا تحتوي معلومة شخصية · تتغيّر لكل خدمة بتغيير حرفين.

لا تستخدم المثال أعلاه

أي مثال منشور يصبح معروفًا. اصنع عبارتك أنت من كلمات تخصّك وحدك.

٠٥ · افعل ولا تفعل

افعل

- اجعلها ١٦ خانة فأكثر
- كلمة مختلفة لكل حساب
- فعّل التحقق بخطوتين
- استخدم مدير كلمات مرور
- احمِ بريدك بأقوى كلمة

لا تفعل

- لا تكتبها في ورقة أو ملاحظة
- لا تشاركها مع أحد إطلاقًا
- لا تحفظها في متصفّح عام
- لا تدخلها عبر شبكة مفتوحة
- لا تستخدم اسمك أو ميلادك

مقارنة سريعة

نمط كلمة المرور	الطول	التقييم
Bader1990	٩	تُكسر فورًا
P@ssw0rd!	٩	تُكسر فورًا
Tr0ub4dor&3	١١	متوسطة
Sahab-Fanar-Zaytun	١٨	قوية جدًا

٠٦ · التحقق بخطوتين

حتى لو عرف أحدهم كلمتك، لن يدخل بدون الرمز الذي في جهازك. هذه أقوى خطوة واحدة يمكنك اتخاذها اليوم.

أي طريقة أفضل؟

- **مفتاح مادي أو بصمة:** الأقوى — يقاوم التصيّد تمامًا.
- **تطبيق مُوثِّق:** جيد جدًا ويعمل بدون شبكة.
- **رسالة نصية:** أفضل من لا شيء، لكنها الأضعف بينها.

ابدأ بالأهم

فعّلها أولًا على: البريد الإلكتروني، ثم الحسابات البنكية، ثم حسابات العمل، ثم التواصل الاجتماعي.

رمز التحقق سرٌّ لا يُشارك

لا ترسله لأحد مهما كانت صفته، ولا تعتمد إشعار دخول لم تطلبه أنت.

٠٧ · مدير كلمات المرور

مدير كلمات المرور خزنة مشفّرة تولّد كلمة فريدة لكل حساب وتملؤها نيابةً عنك. أنت تحفظ كلمة رئيسية واحدة طويلة، وهو يتكفّل بالباقي.

الميزة	ما تعنيه لك
توليد تلقائي	كلمات عشوائية طويلة بلا جهد ذهني
حماية من التصيّد	لا يملأ بياناتك في موقع مزيّف مختلف العنوان
تنبيه التسريب	يخبرك إن ظهرت كلمتك في تسريب معروف
مزامنة آمنة	نفس الخزنة على الجوال والحاسب بتشفير طرفي

قبل أن تختار

- تأكّد أنه يستخدم تشفيرًا طرفيًا لا يطّلع فيه المزوّد على بياناتك.
- فعّل التحقق بخطوتين على الخزنة نفسها.
- في بيئة العمل، التزم بالحل المعتمد من جهة عملك.

٠٨ · إذا تسرّبت كلمتك

السرعة تصنع الفرق. رتّب خطواتك بهذا الترتيب تحديدًا.

1. **غيّر كلمة الحساب المتأثر فورًا**

   من جهاز تثق به، وبكلمة جديدة تمامًا لا تشبه السابقة.

2. **غيّرها في كل مكان استُخدمت فيه**

   هنا يظهر خطر التكرار. ابدأ بالبريد ثم الحسابات المالية.

3. **أنهِ الجلسات النشطة**

   معظم الخدمات توفّر «تسجيل الخروج من جميع الأجهزة» في الإعدادات.

4. **راجع إعدادات الاسترداد**

   تأكّد أن بريد ورقم الاستعادة وقواعد إعادة التوجيه لم تُغيّر.

5. **أبلغ جهة عملك**

   إن كان للحساب صلة بالعمل، أبلغ فريق الأمن السيبراني مباشرة.

> **لا تؤجّل**
>
> كل ساعة تأخير تمنح المهاجم وقتًا لتوسيع وصوله إلى حسابات أخرى.

٠٩ · قائمة تحقق سريعة

عشر دقائق الآن تكفي لرفع مستوى حمايتك بشكل ملموس.

تم	الإجراء
☐	غيّرت كلمة مرور البريد إلى عبارة من ١٦ خانة فأكثر
☐	فعّلت التحقق بخطوتين على البريد
☐	فعّلته على الحسابات البنكية وحسابات العمل
☐	أزلت الكلمات المكرّرة من الحسابات المهمة
☐	ثبّتت مدير كلمات مرور موثوقًا
☐	راجعت الأجهزة والجلسات النشطة
☐	حدّثت بريد ورقم الاسترداد
☐	حذفت كلمات المرور المكتوبة في الملاحظات

هل تشك في رسالة؟

لا ترد ولا تضغط الرابط. أبلغ فريق الأمن السيبراني في جهة عملك، وتحقّق من الجهة عبر قنواتها الرسمية المعروفة.