



كلمة المرور

إرشادات لإختيار كلمة المرور القوية



المحتوى

- أهمية كلمة المرور
- مزايا كلمة المرور الجيدة
- كيف تكتب كلمة مرور قوية
- إرشادات كلمة المرور
- الأخطاء المتكررة بكلمة المرور
- طرق اختراق كلمة المرور



أهمية كلمة المرور

كل من لديه حاسب آلي أو حساب على الإنترنت هو عرضة للاختراق، والفيروسات، وسرقة الهوية، فعليه أن يحرصن جهازه وحساباته بكلمات مرور قوية.



مزايا كلمة المرور الجيدة

- سهولة الحفظ.
- لا يلزمك أن تدونها على الورق.
- يمكن طباعتها بيسر.
- خليط من الأحرف والأرقام والرموز.



كيف تكتب كلمة مرور قوية

- استخدم ٦ رموز على الأقل.
- امزج بها ثلاثة من الأربعة التالية:
 - الأحرف الكبيرة (A-Z)
 - الأحرف الصغيرة (a-z)
 - الأرقام (0-9)
 - الرموز (!@#\$%^&*()_+)=)
- أدخل أخطاءً إملائية متعددة لكل كلمة معجمية تستخدمها.



إرشادات كلمة المرور

- كلمة المرور سرية للغاية.
- لا تدون كلمة المرور ولا ترسلها ببريد.
- لا تشارك أحدا في كلمة المرور.
- لا تستخدم كلمة مرور تكون اسماً أو تاريخاً.
- اختر كلمة مرور تستطيع تذكرها.
- كلمة المرور السيئة هي التي تكون أقل من ٦ أحرف، وتكون من كلمات معجمية.
- كلمة المرور الجيدة هي التي تتكون من ٦ أحرف وزيادة وتحوي خلطة من الأرقام والحروف وعلامات الترقيم والأشكال والأحرف الكبيرة والصغيرة.
- استخدم كلمات مرور مختلفة لحساباتك.
- لا تختار "تذكر كلمة مروري" على الحواسيب المشتركة.
- لا تدخل كلمة المرور وهناك من يراقبك.
- غير كلمة المرور دورياً (كل ثلاثة أشهر مثلاً).
- إذا شعرت أن حاسبك أو حسابك قد تم العبث به فغير كلمة المرور مباشرة.
- لا تعد استخدام كلمات المرور القديمة.



الأخطاء المتكررة بكلمة المرور

- الاختيار السيء لكلمة المرور.
- سوء المحافظة على كلمة المرور.
- ترك الحاسب يعمل بلا مراقبة.

هل تعلم؟

- إن الذي يحصل على كلمة مرورك يمكنه:
 - بعث رسائل تهديد باسمك أو مواد تضر بسمعتك.
 - نشر الفيروسات وبرامج التخريب باسمك.
 - الدخول إلى مواقع أعطيتها بياناتك فيشتري على حسابك.
 - التصرف بملفاتك كيفما شاء.



طرق اختراق كلمة المرور

- الطريقة السهلة لكسر كلمات المرور أن يقوم المخترق بتخمينها، لأن الكثير من الناس يستخدمون معلومات شخصية كالأسماء العائلية وتواريخ الميلاد ونحوه.
- والطريقة الثانية باستخدام برامج تستطيع فك تشفير كلمات المرور بحسابها معجماً بلغات مختلفة، وحساب الاحتمالات الممكنة لكلمة المرور بخلط الأحرف والأرقام والرموز.
- قد يتبين من هذا بأنه من المستحيل إيجاد كلمة مرور لا تكسر وهذا صحيح إلا أن الصحيح أيضاً أن كلمة المرور القوية تجعل عملية تخمينها على برامج الاختراق طويلة ومملة إلى درجة قد تؤدي بالمخترق إلى الإحجام عن العملية، والتركيز على غيرها.



إفعل ولا تفعل

إفعل:

- استخدم ٦ حروف أو أكثر لكتابة كلمات المرور.
- ادمج الأرقام والرموز والأحرف الصغيرة والكبيرة مع بعضها للحصول على كلمة مرور قوية.
- أدخل أخطاءً إملائية متعمدة لكل كلمة معجمية تستخدمها.
- استخدم الرموز (!@#\$%^&*_) في موقع بعض الحروف الشبيهة بها.
- غير كلمة المرور بشكل دوري.
- استخدم كلمات مرور مختلفة لحساباتك المختلفة.
- غير كلمة المرور مباشرة، إذا شعرت أن حاسبك أو حسابك قد تم العبث به.
- أقفل الجهاز في حالة أردت تركه، ولو لوقت قصير.



إفعل ولا تفعل

لا تفعل:

- لا تستخدم بياناتك الشخصية وكلمة المستخدم في كتابة كلمات المرور.
- لا تعط كلمة المرور لأي أحد.
- لا تكتب كلمة المرور تحت أنظار الآخرين.
- لا تدون كلمة المرور ولا ترسلها بالبريد.
- لا تشارك أحدا في كلمة المرور.
- لا تختار "تذكر كلمة مروري" على الحواسيب المشتركة.
- لا تترك الحاسب يعمل بلا مراقبة إذا أردت الذهاب لقضاء حاجة ما.