wearedigital

delivering digital inclusion training

الدليل الاساسي للسلامة على الإنترنت

دليل التعلم

الدليل الأساسي للسلامة على الإنترنت

تعد **كلمات المرور** خط الحماية الأول. فأنت *تستخدمها في كل مكان*: البريد الإلكتروني وeBay وAmazon والحسابات المصرفية وما إلى ذلك.

يُنشِئ الكثير من مستخدمي الكمبيوتر كلمات مرور بسيطة للغاية، فقط لأنه يسهل عليهم تذكُّرها.

كلما كان من السهل تذكُّر كلمة المرور، كان من الأسهل للآخرين تخمينها.

إن "اسمك" و"كلمة مرور" و"123456" من الأمثلة التقليدية السيئة.

أنشئ كلمة مرور تكون عبارة عن مزيج من الأحرف الكبيرة، والأحرف الصغيرة والأرقام. أضف بعض "الرموز" من لوحة المفاتيح. (مثل: $ * ! @ £ # وما إلى ذلك)؛ مثال: **!2019WeAre&Digital£**

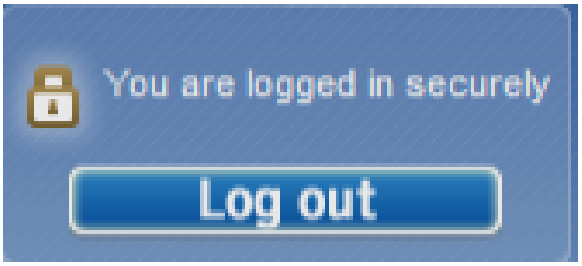
لا تستخدم كلمات أو أسماء يمكن تخمينها بسهولة - على سبيل المثال، اسم شريكك.

حاول استخدام كلمات مرور مختصرة ولا تُنسى.
مثال: تاريخ ميلاد ابنتي هو 7 سبتمبر 1987.
فتصبح كلمة المرور مثلاً: 87tpe$7sbd'Md

ضع كلمة المرور الجديدة في passwordmeter.com للتحقق من قوتها. يجب أن تحقق كلمة مرورك نسبة 100%؛ أي "قوية للغاية".

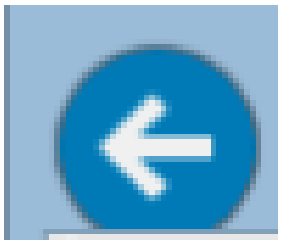
Test Your Password		Minimum Requirements
Password:	Md'sbd7$ept87	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

دليل التعلم

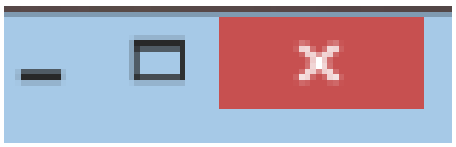


تعد **الخدمات المصرفية على الإنترنت** آمنة للغاية

اختَر تفاصيل تسجيل دخولك بعناية - يجب اختيار "بيانات لا تنسى" أو "معلومات لا تنسى" بنفس الاهتمام الذي توليه لكلمة المرور.

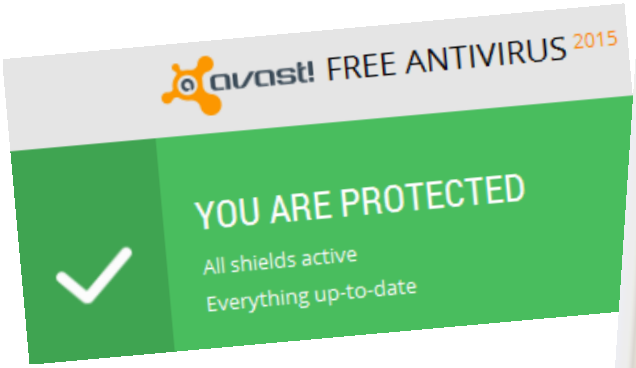


قم دائمًا "بتسجيل الخروج" بشكل صحيح و لا تستخدم زر "الرجوع" في المتصفح.



لا "تغلق" المتصفح بالنقر فوق علامة "X" الحمراء في أعلى يمين الصفحة.

إذا كنت متأكدًا دائمًا من أنك:
(أ) تحافظ على برامج الأمان لديك محدَّثة؛
(ب) تحافظ على سرية بيانات تسجيل الدخول الخاصة بك و
(ج) تقوم دائمًا بتسجيل الخروج بشكل صحيح
ستقوم البنوك وجمعيات البناء بتعويض أي خسائر قد تلحق بك.



ملاحظة: رغم أننا نعتقد بأن المعلومات الواردة في هذا الكتيب دقيقة وتُقدم نصيحة جيدة، فإن الإنترنت هدف متغير باستمرار. ومن ثمَّ فإننا لا نتحمل أي مسؤولية عن أي فيروسات/برامج ضارة قد تصيب جهاز الكمبيوتر لديك أو أي خسائر قد تتكبدها.

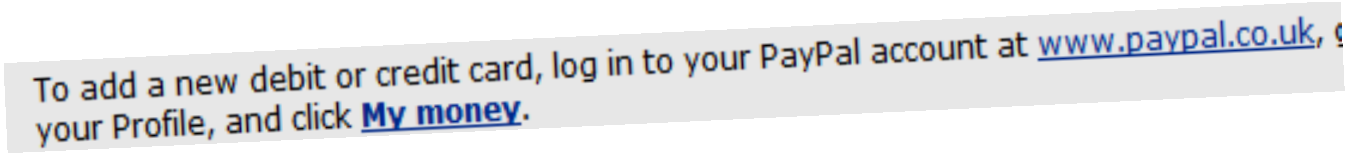
دليل التعلم

الدليل الأساسي للسلامة على الإنترنت

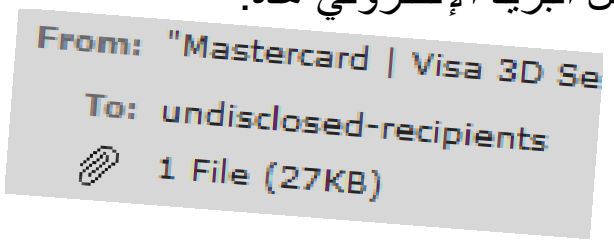
التصيد الاحتيالي

هذا أسلوب يستخدمه المجرمون لمحاولة الحصول على بياناتك الشخصية، لأنه لا يمكنهم مهاجمة البنوك مباشرة.

تجاهل رسائل البريد الإلكتروني التي يبدو أنها تأتي من شركات حسنة السمعة تطلب بياناتك الشخصية. لن تقوم أي شركة جديرة بالثقة بطلب هذه المعلومات. رسائل البريد الإلكتروني غير الموجهة لك شخصيًا ("عزيزي مقدم الطلب") وضعف اللغة المكتوبة بها علامات أخرى على **رسالة بريد إلكتروني** تنطوي على **تصيد احتيالي**.



لا تتبع مطلقًا روابط الويب المتضمنة في رسائل البريد الإلكتروني هذه.



لا تقم أبدًا بفتح (أو "تنزيل") مرفق برسالة بريد إلكتروني من أي مصدر إلا إذا كان موثوقًا به 100%

إذا كنت تريد زيارة بنك/جمعية بناء، فاكتب عنوان الويب بنفسك او اتبع رابطًا يوفره أحد محركات البحث. (Google وBing وما إلى ذلك)

تحقق من عنوان URL - عنوان موقع الويب الحقيقي في الجزء العلوي من المتصفح.