OUCH!

SANS SECURITY AWARENESS

نشرتك الشهريه للتوعية بأمن المعومات

أنشئ كلمات مرور سهلة

نظرة عامة

تعتبر طريقة اختيارك لكلمات المرور هي المفتاح الرئيسي لحماية حسابك، لذلك فإن الكثير من المقالات تقوم بنصحك باستخدام كلمات المرور المعقدة لحماية حسابك، ولكن نادراً ما يتم إعطاؤك طريقة بسيطة لإنشاء وإدارة جميع كلمات المرور بشكل آمن. سنستعرض ثلاث طرق لتسهيل آلية اختيار كلمات المرور، وتأمين حساباتك وحماية مستقبلك.

عبارات المرور

إن الطريقة التقليدية في اختيار كلمات المرور المعقدة التي ترهقك في تذكرها أو كتابتها قد انتهت، ومع تطور أجهزة الحاسوب فائقة السرعة التي تُمكن المهاجمين عبر الانترنت من اختراقها بسهولة. إن المعيار الأساسي لاختيار كلمات المرور هو أن تتكون من خانات كثيرة أي جعل كلمة المرور طويلة وليس الأساس التعقيد لكلمة المرور فقط. لذلك يمكنك الاستعاضة بكلمة المرور المعقدة وصعبة الكتابة والحفظ بجملة قصيرة أو كلمات عشوائية وبذلك تعتبر كلمة المرور قوية وسهلة الحفظ، وعلى سبيل المثال لعبارات المرور:

«حان وقت القهوة القوية!»
«خسر الحلزون الزحف للشاطئ»

كلاهما قوي مع أكثر من عشرين حرفًا، يسهُل تذكرها، سهلة في الكتابة ولكن يصعب كسرها وهو أمر جيد. تَذكر أن طول كلمات المرور هو الأهم.

إدارة كلمات المرور

تحتاج إلى كلمة مرور فريدة لكل حساب خاص بك. إذا قمت بإعادة استخدام نفس كلمة المرور لحسابات متعددة، فإنك تُعَرِض نفسك لخطر كبير. كل ما يحتاجه المهاجم الإلكتروني هو اختراق موقع الكتروني تستخدمه، وسرقة جميع كلمات المرور بما في ذلك كلمات المرور الخاصة بك، ثم استخدام كلمة المرور لتسجيل الدخول إلى جميع حساباتك الأخرى. وهو ما يحدث في كثير الأحيان وللتأكد من أن حسابك غير مخترق من خلال أحد المواقع التي سجلت بها مسبقا يمكنك التحقق من خلال الموقع التالي www.haveibeenpwned.com .لذلك فلابد لك من استخدام كلمة مرور فريدة لكل حساب وهو ما يُعد أمر مرهق للمستخدم لتَذَكُر كلمات المرور المتعددة. إذن ما الذي يجب عليك فعله؟ استخدم مدير كلمات المرور.

مدير كلمات المرور هو برنامج حاسوبي يقوم بتخزين جميع كلمات المرور الخاصة بك بشكل آمن ومُشَفَر وما عليك إلا أن تتذكر كلمة مرور واحدة وهي كلمة المرور الخاصة ببرنامج مدير كلمات المرور وبعد إدخالها بشكل صحيح يقوم هذا التطبيق باسترداد كلمات المرور الأخرى ويتيحها لكي تستخدمها بسهولة. كما أن لبرنامج إدارة كلمات المرور مميزات أخرى مثل تخزين إجاباتك على الأسئلة السرية، وتحذيرك عند إعادة استخدام كلمات المرور، يضمن لك استخدام كلمات مرور قوية، والعديد من الميزات الأخرى. بالإضافة لأن مديري كلمات المرور تتزامن بشكل آمن عبر أي كمبيوتر أو جهاز تقريبًا، لذلك بغض النظر عن النظام الذي تستخدمه، يكون لديك وصول سهل وآمن إلى جميع كلمات المرور الخاصة بك.

أخيرا .. تأكد من كتابة كلمة المرور لبرنامج إدارة كلمات المرور وتخزينها في مكان آمن في المنزل. إن بعض برامج مديري الكلمات تتيح لك آلية طباعة كلمات المرور الرئيسية لاستعادة الحساب. بهذه الطريقة إذا نسيت كلمة المرور لبرنامج مدير كلمة المرور لديك نسخة احتياطية. كما يتيح لك من خلال زوجتك أو أحد افراد أسرتك الموثوقين استرداد المعلومات نيابة عنك في حال مرضت أو وجدت نفسك في حالة طارئة.

المصادقة الثنائية (التحقق من خطوتين)

يضيف التحقق المكون من خطوتين (غالبًا ما يسمى المصادقة الثنائية أو المصادقة متعددة العوامل) طبقة إضافية من الأمان. حيث يتطلب منك الحصول على شيئين عند تسجيل الدخول إلى حساباتك، كلمة المرور ورمز رقمي يتم إنشاؤه بواسطة هاتفك الذكي أو مكالمة إلى هاتفك. حيث تضمن هذه العملية أنه حتى لو حصل مهاجم الإنترنت على كلمة المرور، فلا يزال غير قادر على الوصول إلى حساباتك. لعدم تمكنه من الحصول على الرمز الرقمي الذي غالباً ما يُرسل إلي هاتفك الذكي. وتعتبر آلية المصادقة الثنائية سهلة الإعدادات وعادة ما تحتاج إلى استخدامه مرة واحدة عند تسجيل الدخول من جهاز كمبيوتر أو جهاز جديد. وينصح باستخدام هذه المصادقة كلما أمكن لا سيِما بالنسبة إلى أهم حساباتك، مثل حساباتك البنكية أو التقاعدية أو الوصول إلى بريدك الإلكتروني. إذا كنت تستخدم برنامج مدير كلمات المرور، فإننا نوصي بشدة بحمايتها باستخدام عبارة مرور قوية والتحقق من خطوتين.

قد يبدو الأمر بسيطاً، لكن هذه الخطوات الثلاث البسيطة تقطع شوطاً طويلاً في حماية وظيفتك وسمعتك ومستقبلك المالي.

الضيف المحرر

Justin Henderson (@SecurityMapper) هو المؤسس المشارك في شركة H & A للحلول الأمنية، بالإضافة لكونه مدرب معتمد في شركة SANS ومؤلف منهاج Cyber Defense and SIEM، كما أنه يحب العمل في مجال الامن السيبراني ، يعمل كمستشار في هذا المجال لأكثر من خمسة عشر عاما.

مصادر إضافية

هل أنا مخترق (باللغة الإنجليزية): https://haveibeenpwned.com/

التحقق بخطوتين: https://twofactorauth.org/

NIST SP800-63B Digital Identity Guidelines: https://pages.nist.gov/800-63-3/sp800-63b.html

بوستر أنت مستهدف (باللغة الإنجليزية): https://www.sans.org/u/OGi