أوتش! | نيسان (أبريل) ، ٢٠١٥

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

عبارات المرور

تمهيد

أصبحنا في هذه الأيام نستخدم كلمات المرور كل يوم تقريباً، للدخول على البريد الإلكتروني، إستخدام الخدمات المصرفية عبر الإنترنت، أو إستخدام هاتفك الذكي. كلمات المرور تعتبر واحدة من نقاط الضعف، إذا عرف شخص ما كلمة المرور، فذلك يمكنه من سرقة هويتك وأخذ أموالك أو الدخول إلى معلوماتك الشخصية. كلمات المرور القوية ضرورية لحماية نفسك. في هذه النشرة سوف نتحدث عن كيفية إنشاء كلمات مرور قوية ويمكن حفظها بسهولة وذلك باستخدام «عبارات مرور».

المحرر الضيف

قاي برونو مستشار أمني رفيع المستوى مع شركة IPSS، مدرب في معهد سانز ومعني بأمن المعلومات. قاي يحمل شهادة GSE من شركة سانز أنهى برنامج الوصي الرقمي من معهد سانز. يمكنك متابعة قاي على تويتر @GuyBruneau وعلى handlers.sans.org/gbruneau .

عبارات المرور

التحدي الذي نواجهه جميعا هو أن مجرمو الإنترنت لديهم أساليب متطورة لتخمين كلمات المرور، وأن أساليبهم على الدوام فى تطور. هذا يعني أن بإمكانهم إكتشاف كلمة المرور الخاصة بك إذا كانت ضعيفة أو يسهل تخمينها. خطوة هامة لحماية نفسك هي استخدام كلمات مرور قوية. كلما إحتوت كلمة المرور على حروف أكثر، كلما كانت أقوى و كان من الصعب تخمينها. ومع ذلك، فأن مثل هذه الكلمات تكون معقدة و يكون من الصعب تذكرها. ولذلك ننصح باستخدام «عبارات المرور». هذه العبارات أو الجمل البسيطة يسهل تذكرها، ولكن يصعب تخمينها. مثال على تلك العبارات «أين صديقي سامي؟». ما يجعل هذه العبارة قوية ليس فقط أنها طويلة ولكن استخدام حروف ورموز (المسافات وعلامة الترقيم هي الرموز). يمكنك أن تجعل كلمة المرور الخاصة بك أقوى وذلك باستبدال الحروف بأرقام أو رموز، مثل استبدال الحرف أ برقم 1 فتصبح الجملة «1ين صديقي س1مي؟».. إذا كان موقع ويب أو البرنامج الذي تستخدمه لا يسمح لك باستخدام عدد كبير من الأحرف استخدام الحد الأقصى لعدد الأحرف المسموح به.

استخدام عبارت المرور بشكل آمن

يجب عليك أن تكون حذراً عند استخدامك لعبارات المرور،. فلن يكون استخدامها مفيداً إذا تمكن مجرمو الأنترنت من تخمينها أو كشفها بسهولة. لذا نقترح ما يلي:

عبارات المرور

١. تأكد من استخدام عبارة مرور مختلفة لكل حساب أو جهاز لديك. على سبيل المثال، لا تستخدم نفس عبارة المرور للعمل أو حسابك المصرفي كالتي تستخدمها للحسابات الشخصية، مثل الفيسبوك، يوتيوب أو تويتر. بهذه الطريقة، إذا تم اختراق أحد حساباتك، فان الحسابات الأخرى تبقى آمنة. إذا كان لديك الكثير من عبارات المرور، فانظر في استخدام أحد برامج إدارة كلمات المرور (برامج تقوم بتخزين كلمات المرور بشكل آمن.) وبهذه الطريقة، تحتاج أن تتذكرفقط عبارة المرور لجهازك و عبارة المرور لبرنامج مدير كلمات المرور.

٢. لا تكشف عبارة المرور الخاصة بك أو طريقة تكوينها لأي شخص، بما في ذلك زملاء العمل. تذكر أن عبارة المرور يجن أن تحفظ بسريّة. إذا عرف أي شخص آخر عبارة المرور الخاصة بك، فأنها لم تعد آمنة. إذا كشفت عبارة المرور لشخص آخر لأي سبب، أو تعتقد انه قد تم اختراقها أو سرقتها، فغييرها على الفور.

استخدام عبارات المرور هي إحدى الخطوات الأكثر فعالية التي يمكنك اتخاذها لحماية هويتك والمعلومات الخاصة بك.

٣. تماما مثل كلمات المرور، تجنب عبارات المرور التى يسهل تخمينها أو يشيع استخدامها.

٤. لا تستخدم أجهزة الكمبيوتر العامة، مثل تلك الموجودة في الفنادق أو المكتبات، لتسجيل الدخول إلى حساب العمل أو البنك. يمكن لأي شخص استخدام هذه الحواسيب، ولهذا فأنها قد تكون مصابة ببرامج خبيثة و يمكن تسجيل كل ما تتم كتابته باستخدام لوحة المفاتيح. أستخدم فقط أجهزة الكمبيوتر أو الأجهزة النقالة الموثوق بها للدخول الى حسابات عملك أو الحسابات المصرفية.

٥. كن حذرا من المواقع التي تتطلب منك الإجابة على أسئلة شخصية. هذه الأسئلة تستخدم عندما تنسى عبارة المرور وتحتاج إلى إعادة تعيينها. المشكلة هي أن إجابات هذه الأسئلة كثيرا ما يمكن العثور علها فى شبكة الإنترنت أو حتى في صفحة الفيسبوك الخاصة بك. تأكد من أن إجابتك على الأسئلة الشخصية لا تستخدم معلومات متاحة على الأنترنت. يمكن أن يساعدك برنامج مدير كلمات المرور لتخزين المعلومات التى تساعدك على أجابة الأسئلة الشخصية .

عبارات المرور

٦. العديد من الحسابات على الانترنت تقدم ما يسمى «التوثيق بعاملين»، والمعروف أيضا ب «التحقق بخطوتين». في هذه الحالة تحتاج إلى أكثر من مجرد عبارة المرور لتسجيل الدخول. تحتاج الى شئ اخر مثل رمز المرور الذى يتم إرساله إلى هاتفك الذكي. هذا الخيار هو أكثر أمنا من مجرد عبارة المرور. كلما أمكن ذلك، استخدم دائما التوثيق بعاملين

٧. غالباً ما تتطلب الأجهزة النقالة «رمز» لحماية الوصول إليها. تذكر«الرمز» ليس أكثر من كلمة مرور أخرى. كلما كان «الرمز» معقدا، كلما كان أكثر أمنا. العديد من الأجهزة المحمولة تسمح لك بتغيير«الرمز» الى عبارة مرور.

٨. وأخيرا، إذا كنت لم تعد تستخدم أحد حساباتك، تأكد من إغلاقه أو حذفه أو تعطيله.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة

http://www.securingthehuman.org.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة المتخصصين في أمن المعلومات بكلية علوم وهندسة الحاسب الآلي

بجامعة الملك فهد للبترول والمعادن.

مصادر إضافية

عدد أوتش "الهندسة الإجتماعية ":	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_aa.pdf
عدد أوتش " تطبيقات إدارة كلمات المرور":	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_aa.pdf
عدد أوتش " التحقق بخطوتين ":	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_aa.pdf
مصطلحات أمن المعلومات الشائعة (باللغة الانجليزية):	http://www.securingthehuman.org/resources/security-terms

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي
ترجمها إلى العربية: طلال موسى الخروبي، فرج أحمد عز الدين.