النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

تطبيقات إدارة كلمات المرور

مقدمة

المحرر الضيف

كريس كريستيانسون Chris Christianson مستشار أمن المعلومات في ولاية كاليفورنيا، لديه 20 عاماً من الخبرة والعديد من الشهادات التقنية. شارك في مؤتمرات عديدة وساهم في العديد من المقالات العلمية. يمكن التواصل مع كريس عن طريق **@cchristianson** أو **https://ismellpackets.com**.

من أهم الخطوات التي يمكنك اتخاذها لحماية نفسك عبر الإنترنت استخدام كلمة مرور فريدة وقوية لكل حساب من حساباتك وتطبيقاتك. لكن الكثير من الناس لا يستطيع تذكر كلمات المرور المختلفة الخاصة بحساباته المختلفة. لهذا السبب يقوم الكثير من الناس باستخدام نفس كلمة المرور لحسابات متعددة. للأسف، إعادة استخدام كلمة المرور نفسها لحسابات مختلفة أمر خطير لأنه بمجرد أن يحصل شخص ما على كلمة المرور الخاصة بأحد حساباتك، فبإمكانه الآن الوصول إلى جميع الحسابات التي استخدمت لها نفس كلمة المرور.

هنا يأتي دور تطبيق إدارة كلمات المرور. هذا التطبيق يقوم بتخزن جميع كلمات المرور الخاصة بك بشكل آمن ، مما يجعل من السهل أن تخصص كلمة مرور مختلفة لكل حساب، لأنه بدلا من أن تتذكر جميع كلمات المرور الخاصة بك، تحتاج فقط لتذكر كلمة المرور الرئيسية لتطبيق إدارة كلمات المرور.

كيف يعمل تطبيق إدارة كلمات المرور

يقوم تطبيق إدارة كلمات المرور بتخزين جميع كلمات المرور الخاصة بك في قاعدة بيانات، ويقوم بتشفيرها ويحميها بواسطة كلمة المرور التي تختارها لاستخدام التطبيق. عندما تحتاج إلى استرداد كلمة المرور الخاصة بأحد حساباتك، مثلاً حساب البنك عبر الإنترنت أو بريدك الإلكتروني ، يمكنك ببساطة كتابة كلمة المرور الرئيسية الخاصة بتطبيق إدارة كلمات المرور وسيقوم التطبيق بعرض كلمات المرور المخزنة. توفر بعض تطبيقات إدارة كلمات المرور خاصية التسجيل التلقائي لكلمات المرور وتخزينها بشكل آمن. هذا يجعل من السهل أن يكون لك العديد (ربما المئات) من كلمات المرور المختلفة والقوية، دون أن تحتاج لتذكرها.

تقوم بعض تطبيقات إدارة كلمات المرور بحفظ كلمات المرور على جهاز المستخدم، في حين أن بعض التطبيقات الأخرى تقوم بتخزينه على الحوسبة السحابية. وبالإضافة إلى ذلك، فإن معظم تطبيقات ادارة كلمات المرور لديها ميزات التزامن التلقائي على جميع الاجهزة الخاصة بك. بهذه الطريقة عند تحديث كلمة مرور على جهازك المحمول، تتم مزامنة تلك التغييرات إلى جميع الأجهزة الأخرى الخاصة بك. بغض النظر عن مكان التخزين، تحتاج إلى تثبيت تطبيق إدارة كلمات المرور على جميع تلك الأجهزة.

تطبيقات إدارة كلمات المرور

عند إعداد تطبيق إدارة كلمات المرور لأول مرة، تحتاج إلى إدخال أو تسجيل بيانات الدخول وكلمات المرور يدويا. بعد ذلك، عندما ترغب في إنشاء حساب جديد أو تغيير كلمة المرور لأحد حساباتك المسجلة في التطبيق يمكن للتطبيق تلقائيا تخزين بيانات الحساب الجديد أو تحديث كلمة المرور التي قمت بتغييرها. هذا ممكن لأن معظم تطبيقات ادارة كلمات المرور تعمل بتوافق مع متصفح الويب الخاص بك. مما يمكِّن التطبيق من تسجيل الدخول تلقائيا إلى مواقع الانترنت عندما ترغب في ذلك.

من المهم أن تكون كلمة المرور الرئيسية التي تستخدمها لحماية تطبيق إدارة كلمات المرور قوية وصعبة جداً وغير قابلة للتخمين. في الواقع نوصي بجعل كلمة المرور الرئيسية عبارة مرور، واحدة من أقوى أنواع كلمات المرور الممكنة. إذا كان تطبيق إدارة كلمات المرور الذي تستخدمه يدعم عملية التحقق بخطوتين قم بتفعيل هذه الخاصية للدخول إلى التطبيق. وأخيرا، تأكد من تذكر كلمة المرور الرئيسية حيث أنك إن نسيتها، فلن تتمكن من الوصول إلى أي من كلمات المرور المخزنة في التطبيق.

تطبيقات إدارة كلمات المرور وسيلة سهلة لتخزين آمن لكل كلمات المرور الخاصة بك.

اختيار التطبيق المناسب

هناك العديد من تطبيقات إدارة كلمات المرور للاختيار من بينها. ستجد رابط لأفضل تطبيقات إدارة كلمات المرور ضمن المصادر الإضافية في آخر هذه النشرة. في ما يلي نسرد أهم معايير اختيار التطبيق الأفضل بالنسبة لك:

- يفضل ان يكون التطبيق سهل الاستخدام. إذا وجدت تطبيقاً معقداً جدا ويصعب فهمه، اختر تطبيقا يناسب بشكل أفضل خبراتك واحتياجاتك.
- عليك اختيار تطبيق يمكن تثبيته على جميع الأجهزة التي ترغب في استخدام كلمات المرور علها. بالاضافة الي توفر خاصية المزامنة بين تلك الاجهزة.
- استخدم تطبيق إدارة كلمات المرور من مصدر موثوق. كن حذرا من البرمجيات الجديدة. يمكن لمخترقي الإنترنت إنشاء برامج إدارة كلمات مرور وهمية لسرقة المعلومات الخاصة بك. أيضا كن حذرا من مطوري البرمجيات الذين يدَّعون أنهم طوروا حلول تشفير خاصة بهم.
- تجنب أي تطبيق يدعي أنه قادر على استعادة كلمة المرور الخاصة بالتطبيق. هذا يعني أن هناك من يعرف كلمة المرور الرئيسية الخاصة بك، وهذا سيعرضك للكثير من المخاطر!.

تطبيقـات إدارة كلمـات المـرور

- تأكد من أن التطبيق الذي اخترته يتم تحدثه باستمرار واحرص على متابعة التحديثات وتثبيتها على جميع اجهزتك باستمرار.
- يجب أن يتضمن التطبيق القدرة على إنشاء كلمات مرور قوية تلقائياً كما يوفر خاصية تحديد قوة كلمات المرور التي اخترتها.
- توفـر بعـض تطبيقـات إدارة كلمـات المـرور خاصيـة تخزيـن بيانـات حساسـة أخـرى، مثـل الأجوبـة عـلى الأسـئلة الأمنيـة السريـة، وأرقـام بطاقـات الائتمـان.

تطبيقـات إدارة كلمـات المـرور وسـيلة رائعـة لتخزيـن آمـن لـكل كلمـات المـرور الخاصـة بـك وغيرهـا مـن البيانـات الحساسـة. ومـع ذلـك، بمـا أن الهـدف حمايـة هـذه المعلومـات الهامـة، تأكـد مـن اسـتخدام كلمـة مـرور رئيسـية قويـة و فريـدة مـن نوعهـا و مـن الصعـب عـلى مجرمـي الشـبكة تخمينهـا، ولكـن مـن السـهل لـك أن تتذكرهـا.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة securingthehuman.sans.org/ouch/archives.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة و المتخصصين في أمن المعلومات.

مصادر إضافية

أفضل برامج كلمات المرور لعام 2017 (باللغة الإنجليزية):	https://www.pcmag.com/article2/0,2817,2407168,00.asp
عدد أوتش حول عِبَارات المُرور:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_aa.pdf
عدد أوتش حول التحقق باستخدام خطوتين:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_aa.pdf
كيف تحافظ على بيانات الدخول (باللغة الإنجليزية):	https://www.lockdownyourlogin.org/
نصيحة اليوم للأمن الإلكتروني من سانز (باللغة الإنجليزية):	https://www.sans.org/tip-of-the-day

مجلس التحرير: والت سكريفن، فيل هوفمان، كاثي كليك، شيريل كونلي
ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور