نشرتك الشهرية للتوعية بأمن المعومات

مدير كلمات المرور

نظرة عامة

من أهم الخطوات التي يمكنك اتخاذها لحماية نفسك هي استخدام كلمة مرور فريدة وقوية لكل من حساباتك وتطبيقاتك. لكن للأسف، يكاد يكون من المستحيل تذكر جميع كلمات المرور المختلفة. بالإضافة إلى ذلك ، نحن نعلم أن الاستمرار بكتابة كلمات المرور المختلفة في المواقع ، وإنشاء كلمات مرور جديدة، وتتبع الإجابات على جميع أسئلة الأمان، والعديد من العوامل الأخرى يستنزف وقتًا طويلاً. ومع ذلك، هناك حل من شأنه أن يجعل حياتك أكثر بساطة وأكثر أمانًا بكثير -برمجيات إدارة كلمات المرور.

كيف تعمل برمجيات اداره كلمات المرور

تعمل برمجيات إدارة كلمات المرور من خلال تخزين جميع كلمات المرور الخاصة بك في قاعدة بيانات والتي تسمى أحيانًا بالخزنة. يقوم مدير كلمات المرور بتشفير محتويات الخزنة وحمايتها بكلمة مرور رئيسية تعرفها أنت فقط. وعندما تحتاج إلى كلمات المرور، مثل تسجيل الدخول إلى البنك عبر الإنترنت أو حساب البريد الإلكتروني، ما عليك سوى كتابة كلمة المرور الرئيسية في مدير كلمات المرور لفتح قفل الخزنة. عندها سيقوم مدير كلمات المرور تلقائيًا باسترداد كلمة المرور الصحيحة وتسجيل الدخول بشكل آمن إلى موقع الويب. هكذا لن تكون بحاجة إلى تذكر كلمات المرور أو تسجيل الدخول يدويًا إلى حساباتك.

بالإضافة إلى ذلك، تتضمن معظم برمجيات إدارة كلمات المرور مزايا تمكنها من المزامنة تلقائيًا عبر أجهزة متعددة. أي أنك وبهذه الخاصية، عند قيامك بتحديث كلمة مرور على حاسوبك، تتم مزامنة هذه التغييرات مع جميع أجهزتك الأخرى. أخيرًا، تكتشف معظم برمجيات إدارة كلمات المرور متى تحاول إنشاء حساب جديد عبر الإنترنت أو متى قمت بتحديث كلمة المرور لحساب موجود، ومن ثم تقوم هي تلقائيًا بتحديث البيانات في الخزنة نيابةً عنك.

مهم للغاية أن تكون كلمة المرور الرئيسية التي تستخدمها لحماية مدير كلمات المرور طويلة وفريدة من نوعها. في الواقع، نوصيك بجعل كلمة مرورك الرئيسية على شكل عبارة مرور – أي انها كلمة مرور طويلة تتكون من عدة كلمات أو عبارات متعددة. وإذا كان مدير كلمات المرور يدعم آليه التحقق بخطوتين، فاستخدمه لكلمة المرور الرئيسية أيضًا. أخيرًا، تأكد من تذكر عبارة المرور الرئيسية. إذا نسيت ذلك، فلن تتمكن من الوصول إلى أي من كلمات المرور الأخرى.

اختيار مدير كلمات المرور

هناك العديد من برمجيات ادارة كلمات المرور للاختيار من بينها. في قسم المصادر، أوردنا رابطًا لمراجعات تستعرض العديد من برمجيات ادارة كلمات المرور. وفي الوقت نفسه، عند محاولتك العثور على الأفضل بالنسبة لك، ضع في اعتبارك ما يلي:

يجب أن يكون مدير كلمات المرور الذي تختار سهل الاستخدام. وإذا وجدت أن الحل معقد للغاية بحيث يتعذر فهمه فابحث عن حل مختلف يناسب أسلوبك وخبرتك بشكل أفضل.

يجب أن يعمل مدير كلمات المرور على جميع الأجهزة التي تحتاج استخدام كلمات المرور عليها. بالاضافة الي ضرورة دعمه لخاصية مزامنة كلمات المرور عبر جميع أجهزتك.

استخدم فقط مديري كلمات المرور المعروفة والموثوق بها. وكن حذرًا من المنتجات التي لم تكن موجودة منذ فترة طويلة أو لا تحتوي على تعليقات إيجابية من المستخدمين. واعلم انه يمكن لمجرمي الإنترنت إنشاء مديري كلمات مرور مزيفة لسرقة معلوماتك. أيضًا ، كن حذرًا جدًا من البائعين الذين يروجون أنهم طوروا انظمة التشفير الخاص بهم.

تجنب أي مدير كلمات مرور يدعي أنه قادر على استعادة كلمة المرور الرئيسية نيابة عنك. هذا يعني أنهم يعرفون كلمة مرورك الرئيسية، الامر الذي سيعرضك لمخاطر كبيرة.

تأكد من أنه ومهما كان الحل الذي تختاره، ان يستمر المطور في تحديث مدير كلمات المرور وتصحيحه بنشاط، وتأكد بشكل خاص من أنك تستخدم دائمًا أحدث إصدار.

يجب أن يمنحك مدير كلمات المرور خيار تخزين البيانات الحساسة الأخرى، مثل الإجابات على أسئلة الأمان السرية الخاصة بك، ومعلومات بطاقة الائتمان، وأرقام النشر المتكررة.

ضع في اعتبارك كتابة عبارة مرورك الرئيسية في مظروف مغلق وتخزينها في خزانة محكمه أو خزنة فولاذ أو صندوق ذو قفل.

تعد برمجيات إدارة كلمات المرور طريقة رائعة لتخزين جميع كلمات المرور والبيانات الحساسة الأخرى بشكل آمن، مثل أرقام بطاقات الائتمان. ومع ذلك، تأكد دائما من استخدام عبارة مرور رئيسية فريدة وقوية واستخدم دائمًا أحدث إصدار من أي برنامج تختاره.

المحرّر الضيف

Russell Eubanks هو خبير لأمن المعلومات من أتلانتا، لديه خبرة تزيد عن 20 عامًا، ويحمل العديد من شهادات امن المعلومات. وهو مسؤول في مركز *SANS Internet Storm Center* وهو أيضا مساهم في عناصر التحكم الأمنية الحرجة. يمكن التواصل مع راسل على russelleubanks @ و https://www.securityeverafter.com .

مصادر إضافية

Making Passwords Simple: http://www.sans.org/u/Y10
الميراث الرقمي: http://www.sans.org/u/Z10G
مراجعة لافضل برامج ادارة كلمات المرور: https://www.wired.com/story/best-password-managers

OUCH! من قبل فريق الوعي الأمني في SANS وتُوزّع بموجب Creative Commons BY-NC-ND 4.0. يسمح بتوزيع هذه النشرة شرط الإشارة للمصدر وعدم تعديل النشرة أو إستخدامها لأغراض تجارية. لترجمة النشرة أو لمزيد من المعلومات، يرجى الإتصال على: www.sans.org/security-awareness/ouch-newsletter. | المجلس التحريري: والت سكريفنز، فِل هوفمان، ألان واجونير، شيريل كوناي | ترجمها إلى العربية: محمد سرور، فؤاد أبو عويمر، درويش الحلو، اسلام الكرد