السر في كلمة المرور: هكذا تبقى آمناً وتحفظ خصوصيتك على الإنترنت

2017-08-15مروة الاسدي

هل تريد ان تعرف طريقة كتابة كلمة سر لا يمكن اختراقها؟ هل تتعرض حساباتك الى الاختراق بشكل مستمر؟، هل تعتبر كلمة المرور الخاصة بك مُعرضة للخطر؟، ماذا تفعل عند نسيان كود PIN أو كلمة المرور؟، كيف تبقى آمناً وتحفظ خصوصيتك على الإنترنت؟، هذه الأسئلة وغيرها تدور في بال أي مستخدم انترنت وخصوصا مواقع التواصل الاجتماعية والحسابات الشخصية، لأنها قد تعرضهم لخطر الاختراق وانتهاك الخصوصية.

السر هو كلمة المرور ويرجع ذلك إلى مجموعة من المعايير كتبها بيل بير، المدير السابق للمعهد الوطني للمعايير والتقنية والأب الروحي لكلمات المرور الحديثة، في عام 2003، نصح بير جميع الإدارات الحكومية في ذلك الوقت أن كلمة السر يجب أن تكون عشوائية مكونة من الحروف والرموز لا أحد يمكن تخمينها.

لكن اتضح أن الطريقة سهلت للقراصنة عملية اختراق الأجهزة الإلكترونية، حيث استخدم الناس تركيبات عشوائية ما جعلها في الواقع أقل عشوائية، وقال بير لصحيفة "وال ستريت" إنه من الأفضل اختيار كلمة مرور طويلة مكونة من عبارات أو أشياء يمكنك تذكرها بسهولة والتوقف عن تعقيد كلمة السر.

استخدامك لكلمة مرور قوية يضمن لك عدم قدرة المخترقين "الهاكرز" على الوصول لحسابك عبر الأساليب المتبعة لتخمين كلمات المرور الشائعة.

وعلى الرغم من أن أهمية هذه النصيحة إلا أن الكثير من المستخدمين حول العالم لا يزالون يعتمدون على كلمة مرور سهلة التخمين، فمثلاً 123456 كانت كلمة المرور الأكثر استخداماً في عام 2016 الماضي من بين كافة كلمات المرور التي تم تسريبها على أيدي الهاكرز.

كذلك يُنصح عند إنشاء كلمة مرور بتجنب استخدام أي معلومات شخصية مثل تاريخ الميلاد أو الرقم الهاتفي أو الاسم أو أي معلومات يُمكن للآخرين تخمينها.

الاعتماد على كلمة مرور واحد لمختلف حساباتك يعتبر من الأخطاء الشائعة جداً بخصوص كلمات المرور، فهذا الأسلوب في التعاطي مع كلمات المرور يُسهل على الهاكرز الحصول على كلمة المرور الخاصة بحساباتك المهمة بمجرد معرفة كلمة المرور على أي موقع آخر، كما أن إمكانية تعرض أي موقع أو خدمة لعملية تسريب بيانات المستخدمين سيتيح للهاكرز الولوج إلى حساباتك الأخرى باستخدام نفس المعلومات.

الاعتماد على كلمة مرور قوية إلى جانب كلمة مرور فريدة لكل حساب، سيعمل على إرهاق المستخدم نوعاً ما عند حاجته لتذكر هذه الكلمات.

لذا فإن الحل الأمثل لتجاوز هذه المشكلة يكمن بالاعتماد على أحد التطبيقات الموثوقة لإدارة كلمات المرور مثل LastPass أو 1Password والتي لن تحتاج بعدها إلى تذكر هذه الكلمات في كل مرة.

لا تُفكر إطلاقاً بإرسال المعلومات الخاصة بأحد حساباتك لأي شخص على الإنترنت، حتى لو كان من الأشخاص الذين تثق بهم.

فعند إرسال معلومات مهمة على البريد الإلكتروني أو على الشبكات الاجتماعية لهذا الشخص مثل كلمة مرور إحدى حساباتك، فيمكن أن يتعرض هذا الشخص لعملية اختراق وبالتالي الوصول إلى حسابك.

لذا إن كنت بحاجة ماسة لإرسال مثل هذه المعلومات الحساسة، فيفضل إرسالها باستخدام الرسائل السرية ذاتية التدمير على إحدى تطبيقات التواصل الفوري، فمثلاً تطبيق مسنجر يدعم هذه الميزة إلى جانب تيليجرام وكذلك فايبر وغيرها من التطبيقات.

ينصح أيضاً بتغيير كلمة المرور الخاصة بحساباتك المهمة من حين لآخر، وإن كانت هذه النصيحة أقل أهمية من النصائح السابقة إلا أنها تساعدك على إبقاء حسابك بحالة أمنية مستقرة دائماً.

موقع جديد يكشف لك خطر اختراق حساباتك

نشر أحد خبراء البيانات أكثر من 306 ملايين كلمة سر جرى اختراقها مُسبقاً، بهدف مساعدة الناس على حماية أمنهم الإلكتروني، ويمكن لأي شخص أن يتحقق من احتمالية تعرض أمنه الإلكتروني للخطر من خلال استخدام موقع "Pwned Been I Have" الجديد على الإنترنت، بحسب صحيفة The Daily Mail البريطانية.

يتلاعب موقع Pwned بكلمة "Owned"، التي تُستخدم في السياقات غير الرسمية لتشير إلى السخرية من الآخرين أو استغلال، ونشر الخبير الأمني تروي هانت، المُقيم في الساحل الذهبي في أستراليا، أداة للبحث عما إذا كانت كلمة السر الخاصة من بين الكلمات التي جرى اختراقها من قبل، وبالتالي تحتاج إلى تغييرها.

ويمكن قراءة القائمة بأكملها بعد تحميل ملف سعته 5.3 غيغابايت، أو يمكن للمستخدمين اختبار كلمات السر الخاصة بهم عبر هذا الرابط، وقام هانت بتجميع القائمة من عشرات البيانات التي تعرَّضت للاختراق. بحسب هاف بوست عربي.

وكتب في مدونته قائلاً "آمل أن توجد خدمة على الإنترنت يسهل الوصول إليها مثل هذه، تعمل ولو بشكل جزئي على معالجة المطلب القديم، الذي يجبرني على تقديم عنوان البريد الإلكتروني وكلمة السر. وإذا أدت كلمة السر وحدها إلى نتيجة عند استخدام هذه الخدمة فقد يكون ذلك سبباً جيداً في عدم استخدامها مجدداً، بغض النظر عن الحساب الذي ظهرت إلى جانبه".

وأوضح هانت "وبالإضافة إلى الأشخاص الذين يتحققون من كلمات المرور التي من المحتمل أنهم استخدموها من قبل، أتصور أن يقوم المزيد من الأشخاص البارعين في التكنولوجيا باستخدام هذه الخدمة، لتوضيح نقطة ما للأصدقاء والأقارب وزملاء العمل: "أترى، تعرضت كلمة السر هذه

للاختراق من قبل، فلا تستخدمها"!.

ومع ذلك، ينصح هانت المستخدمين أيضاً بألا يتحققوا من كلمات سرٍ يستخدمونها في الوقت الحالي، عبر خدمة الطرف الثالث، مثل البحث الذي صممه على شبكة الإنترنت، وأضاف: "لم أتحقق من هذه الكلمات صراحة، وأنا شخص جدير بالثقة، ولكن لا تجربوا هذا"، وعلاوة على هذا يعتبر هانت وراء مدونة تعقب اختراق البيانات الأصلية "Pwned Been I Have"، التي تسمح للمستخدمين بالتحقق مما إذا تعرضت حسابات البريد الإلكتروني الخاصة بهم للاختراق أم لا.

وعندما دُشِّن الموقع عام 2015، فقد تضمن بيانات من 66 موقعاً "Pwned"، أو مواقع تعرضت لشكل من أشكال الاختراق الأمني، ومن ضمن هذه المواقع VTech, Adobe, Sony, Tesco, الذي الوقت يظهر الموقع اسم على الضغط خلال فمن ،أخرى ومواقع Minecraft Pocket Edition جرى فيه تسريب بيانات المستخدمين، والسبب في ذلك، بالإضافة إلى عدد الحسابات التي تأثرت بذلك.

أفضل كلمات المرور

وفي وقت سابق من هذا العام، اقترحت ميجان سكوايز، أستاذة علوم الحاسب بجامعة إيلون، أن أفضل كلمات المرور تتألف من 16 رمزاً، ومليئة بالأرقام والحروف العشوائية، فعلى الرغم من صعوبة تذكُر كلمات المرور العشوائية، فمن المُستحسن أن يحفظ المستخدمون كلمات المرور التي يمكن تقسيمها.

وبهذه الطريقة يسهل تذكرها، لأنهم إما أن يتوصلوا إلى معنى في تلك الأقسام، أو لأنهم يتمكنون من إضافة المعنى الخاص بهم بسهولة أكثر، وذلك عن طريق أساليب الاستذكار، فعلى سبيل المثال، تبدو كلمة مرور مثل "juNC!9tY!freQ", مُعقدة للغاية في بادئ الأمر. ولكن من خلال تقسيم كلمة المرور إلى أجزاء صغيرة على هذا النحو "freQ!", و"9tY!" و "juNC", يُمكن للمستخدمين تذكُرها على أنها "freak", و "ninety" و"junk".

ويقترح الباحثون أيضاً الاستفادة من البرامج التي يمكن أن تساعد المستخدمين في ابتكار وتذكُّر كلمات مرور مُميزة يصعب اختراقها لكل المواقع والتطبيقات، كما توجد تقنية ستقوم بإرسال شفرة إلى هاتفك المحمول، استخدم ماسح بصمة الإصبع أو رمزاً خاصاً بجهاز الناقل التسلسلي العالمي USB للدخول إلى موقع أو حساب على الإنترنت.

يذكر أنه خلال هذا الشهر، بدأت جوجل بإثناء المستخدمين عن استقبال شيفرات تطبيق التحقق بخطوتين 2SV، عن طريق خدمة الرسائل القصيرة SMS، بحسب موقع Cnet.

وبدأ ذلك خلال الأسبوع الماضي، فعندما تحاول الدخول إلى حسابك الشخصي، قد تتلقى دعوةً من جوجل للبدء في استقبال الرسائل عن طريق تطبيق جوجل، بدلاً من الشيفرات التي تتكون من 6 أرقام عن طريق تطبيق الرسائل النصية، بحسب موقع Cnet المتخصص في أخبار التكنولوجيا.

الخبير الذي نصحنا بوضع كلمات مرور معقدة يعترف بأنَّه كان مخطئاً.. كيف نختارها إذاً؟

قال خبير تكنولوجيا المعلومات، المسؤول عن اقتراح أن يستخدم الناس كلمات مرور مُعقَّدة وتغييرها بصفةٍ منتظمة، إنَّه نادمٌ على تلك النصيحة، قائلاً إنَّ تلك النصيحة "قادت الناس إلى الجنون".

وكان بيل بير، قد كتب إرشادات الأمان الخاصة بكلمات المرور لصالح المعهد الوطني الأميركي للمعايير والتقنية في عام 2003، واقترح حينها أن يغيِّر الناس كلمات مرورهم كل ثلاثة أشهر، وأنَّها يجب أن تتضمن مجموعة من الأرقام والحروف.

إذ تختلف متطلبات اختيار كلمات المرور من موقعٍ لآخر؛ إذ يطلب بعضها استخدام الحروف الإنكليزية الصغيرة والكبيرة في كلمة المرور، بينما يطلب البعض الآخر علامات لا هي حروف ولا أرقام، مثل علامة الاستفهام وعلامة النسبة المئوية.

وقال بير مُتحدِّثاً إلى صحيفة Journa Street Wall The: "أنا نادمٌ الآن على كثير مما فعلتُه، لأنَّ

الأمر قاد الناس إلى الجنون، وهم لا يختارون كلمات مرور جيدة مهما فعلت"، الآن وقد علمنا أنَّ النصيحة التي نتبعها حالياً خاطئة، يبقى السؤال إذن ما الذي يجعل كلمة المرور قوية؟

حسناً، هناك أمران مباشران يمكن أن يُحدِثا فرقاً، كل الفرق. أحدث هاتين النصيحتين هي أن تكون كلمة المرور مكونة من مجموعة من الكلمات العشوائية التي لا يمكن أن يستنتجها إلا إنسان. بحسب هاف بوست عربي.

وإليك مثال جيد: leekeatingrabbitstorm أو "كراث يأكل أرنب عاصفة"، وهي مجموعة كلمات بجانب بعضها البعض لا تعني شيئاً على الإطلاق، وستتطلَّب من جهاز الكمبيوتر ملايين وملايين من التخمينات حتى يصل إليها.

الشيء التالي الذي يجب أن تقوم به إن كان حسابك يدعم ذلك، هو أن تضبط الإعدادات على خاصية التحقُّق بخطوتين، ويعني ذلك أنَّه حتى لو استطاع أحدهم تخمين كلمة مرورك سيظل بحاجة لتجاوز خطوة أخرى تتمثَّل في إدخال شفرة خاصة تُرسَل إلى هاتفك الذكي.

وأخيراً، إن كنت تريد تأمين حساباتك حقاً، قد يستحق الأمر أن تستثمر بعض المال في أحد تطبيقات إدارة كلمات المرور مثل 1password، أو LastPass، أو Security Keeper. ويُعد استخدام تلك التطبيقات غاية في السهولة، وهي تساعدك أيضاً على اختيار كلمات مرور معقدة بإمكانك نسخها من التطبيق ولصقها.

وأفضل تطبيقات لإدارة كلمات المرور هي:

يُعد تطبيق 1password هو "الأفضل" في تلك المجموعة؛ فهو يعمل مع أي شيء تقريباً، كما أنَّه من أسهل التطبيقات من ناحية الاستخدام، ويرجع ذلك إلى واجهته البسيطة للغاية.

ويستخدم تطبيق 1password الإضافات في متصفح كروم وفايرفوكس وسفاري بدلاً من استخدام "الملء الآلي - Autofill"، الأمر الذي يسمح لك بالدخول السريع والسهل إلى منصتك الخاصة على أي

جهاز من أجهزة الكمبيوتر الخاصة بك.

أما تطبيق 1password الخاص بأجهزة الآيفون، فيستخدم تقنية ID Touch أو "مُعرِّف اللمس"، وهو عبارة عن مستشعِر بصمة الإصبع. لذلك يُعد هذا التطبيق حلاً شاملاً للمستخدم الواحد الذي يحتاج حلاً متكاملاً، سعر التطبيق 49.99 دولار.

أمَّا Dashlane، فيُعد التطبيق الذي يمكن استخدامه لأكثر من مستخدم واحد من بين التطبيقات الثلاثة في هذه المجموعة، ويتَّسم باحتوائه على واجهة تفاعل شبيهة بتطبيق 1password، بسهولة الاستخدام ويتمتَّع بإمكانات كبيرة.

وإذا كنت تدير مشروعاً صغيراً، أو حتى كبيراً، فقد تكون تلك هي الخدمة المناسبة لك، إذ يمكنك، من خلال اختيارات متنوعة للمشاركة، إرسال كلمات المرور لزملائك الذين لديهم تطبيق Dashlane، الزملاء أولئك من خاصتك المرور كلمة وسرية أمان على الحفاظ مع.

كل ما عليهم فعله هو الموافقة، ومن ثَمَّ سيُدخلهم التطبيق إلى الخدمة (التي يحتاجون فيها استخدام كلمة مرورك، كأن يرغبوا في فتح بريدك الإلكتروني على سبيل المثال أو حسابك في موقع فيسبوك وغيرها)، دون حتى أن يضطروا لرؤية بيانات اعتماد التسجيل الخاصة بك. ويعمل هذا التطبيق على نظام iOS، وأندرويد، وماكنتوش، ووينـدوز، وسعر هذا التطبيق هو 39.99 دولار في العام.

قد يكون تطبيق LastPass الأخير في القائمة، لكنَّه حتماً ليس الأخير في الجودة؛ فهو مدير كلمات المرور العريق، الذي يمتلك أكثر الخصائص التي يمكنك استخدامها، فهو يعمل مع جميع المنصات والمواقع، كما يمكن تخصيصه أو ضبطه وصولاً إلى درجةٍ احترافية، وذلك في ظل دعمه لتكنولوجيا التحقُّق القائمة على القياسات والمؤشرات الحيوية، كالتعرُّف على الوجه أو البصمة أو الصوت على سبيل المثال، وأي تكنولوجيا تحقُّق أخرى يمكن أن تتخيلها تقريباً، قد يكون هذا التطبيق أكثر تعقيداً في استخدامه، لكن بمجرد إعداده، يمكن القول إنَّه يصبح الأكثر مرونة بلا منازع، من حيث القيام بالخدمة التي تريدها، سعر التطبيق 12 دولاراً في العام.

ماذا تفعل عند نسيان كود PIN أو كلمة المرور؟

سرعان ما يفقد المستخدم كود PIN أو نموذج إلغاء القفل أو كلمة مرور لخدمات الويب، ولكنه يتمكن في بعض الأحيان من استعادة بيانات الوصول بسهولة بدون أية مكالمات هاتفية معقدة أو رسائل إلكترونية مع خدمة العملاء.

وفي حال لم يتذكر المستخدم كود PIN اللازم لإلغاء قفل الهاتف الذكي؛ فإنه يمكن الاستعانة بكود خاطئ بشكل مرات ثلاث العادي PIN كود إدخال يتم عندما الكود هذا يعمل حيث ثانٍ؛ كخيار PUK في الهاتف الذكي، وعادةً ما يكون هذا الكود مطبوعًا على غلاف بطاقة SIM من الشركة المقدمة لخدمات الاتصالات الهاتفية الجوالة، كما أشارت مجلة «شيب» الألمانية، وفي حالة عدم العثور على هذا الغلاف؛ فإنه يمكن شراء بطاقة SIM جديدة، والتي يمكن طلبها من مراكز الخدمة التابعة للشركة المقدمة لخدمات الاتصالات الهاتفية الجوالة.

ويمكن لأصحاب بعض أجهزة أندرويد الحديثة، إلغاء القفل عن طريق مدير أجهزة أندرويد، ولكن يشترط أن يتم ربط الهاتف بحساب غوغل الخاص بالمستخدم، ويمكن استدعاء ذلك في المتصفح عبر الرابط، وبعد إدخال بيانات التسجيل الخاصة بحساب غوغل، يتمكن المستخدم من تحديد موقع جهاز أندرويد، وجعله يصدر صوت رنين، بالإضافة إلى إمكانية قفله وتحديد كود جديد، وإذا لم يفلح هذا الحل؛ فإنه يمكن اللجوء إلى خيار استعادة ضبط المصنع، ولكن لا بد من مراعاة أن هذا الإجراء يؤدي إلى فقدان جميع البيانات المخزنة على الهاتف، ومن أجل القيام باستعادة ضبط المصنع، يتعين على المستخدم أن يقوم بإيقاف الهاتف أولاً، وبعد ذلك القيام بالضغط المتزامن على زر خفض شدة الصوت وزر Power، إلى أن يقوم الجهاز بتشغيل وضع استعادة ضبط المصنع، ويمكن أن تختلف تسمية هذا الوضع من شركة إلى أخرى.

وهناك العديد من خدمات الويب تقدم للمستخدم إمكانية إدخال رقم هاتفي أو بريد إلكتروني لكي يتم استعماله عند إعادة تعيين كلمات المرور المنسية، وفي حالة فقدان كلمة المرور الخاصة بحسابات الويب، يتعين على المستخدم البحث عن الزر "نسيت كلمة المرور"، ومن خلال النقر عليه يتم إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني المخزن، وبالتالي يتمكن المستخدم من

تعيين كلمة مرور جديدة.

كيف تبقى آمناً وتحفظ خصوصيتك على الإنترنت؟

اختراق قاعدة بيانات تضم 306 ملايين كلمة مرور

أطلق خبير أمن المعلومات "توري هانت" أداة بحث لتصفح قاعدة بيانات تضم كلمات المرور التي تم اختراقها والقرصنة عليها في وقت سابق.

تستهدف قاعدة البيانات الجديدة مساعدة المستخدمين في معرفة كلمات المرور التي يمكن اختراقها بسهولة، وذلك من خلال تجميع بيانات العشرات من عمليات اختراق قواعد البيانات وسرقة كلمات المرور بهدف مساعدة الأفراد والشركات في تحسين أمن شبكات معلوماتهم.

وأشار موقع "سي نت دوت كوم" المتخصصة في موضوعات التكنولوجيا، إن اختيار كلمات مرور قادرة على مواجهة محاولات القرصنة والاختراق أمر حتمي في ظل تزايد نشاط القرصنة المعلوماتية. ومن الناحية المثالية يجب ألا تقل كلمة المرور عن 16 حرفا وتكون عبارة عن مزيج من الحروف والأرقام والرموز، مع استخدام الحروف الكبيرة والصغيرة. ورغم ذلك فإن أكثر كلمات المرور تعقيدا في العالم ستصبح بلا جدوى إذا كان أحد قراصنة المعلومات قد رصدها واستخدمها في اختراق حساب صاحبها.

يتيح موقع الإنترنت الذي أطلقه "هانتر" للمستخدمين معرفة ما إذا كان عنوان بريدهم الإلكتروني عرضة للاختراق دون الكشف عن كلمة المرور بالتأكيد، ويحذر "هانت" من استخدام قاعدة البيانات الجديدة لاختبار كلمة مرور يستخدمها المستخدم بالفعل في أحد حساباته، حيث يمكن أن ينطوي ذلك على عرض خيار كلمة مرور أخرى أمام طرف ثالث، وكتب "هانت" في تدوينة على الإنترنت يقول " في حين يقوم المستخدمون حسنو النية باختبار كلمات المرور التي يستخدمونها بالفعل، فإن بعض محترفي التكنولوجيا يستخدمون قاعدة البيانات لكي يوضحوا لأصدقائهم وأقاربهم وزملائهم أن كلمة المرور تلك تم اختراقها من قبل ولا يجب استخدامها.. وإذا كان هناك أمر

تعلمته من سنوات عملي في هذه الخدمة، فهو أنه لا يوجد ما هو أكثر إزعاجا من رؤية بياناتك متاحة لآخرين".