#أمنك_مسؤوليتك

تعرّف على مهارة إنشاء
كلمات مرور قوية تحصّن حساباتك

كلمة السر هي مفتاح تأمين أغلى ما تملك... فأحسن الاختيار

تعرّف على مهارة إنشاء كلمات مرور قوية تحصّن حساباتك..
كلمة السر هي مفتاح تأمين أغلى ما تملك.. فأحسن الاختيار

المال، الأصدقاء، الأسرار، البيانات الشخصية، المعلومات السرية، هي كنوزنا الثمينة، التي قد يسبب سرقتها ما لا يمكن تعويضه، فضلاً عن أن خسارتها في بعض الأحيان قد يكون سبباً في خسارتنا لحياتنا، خاصة في فترات النزاعات والحروب.

روتيننا اليومي في استعمال الإنترنت قد لا يخلو من الحديث مع أصدقائنا ودائرة علاقاتنا وعملائنا عبر وسائل التواصل الاجتماعي، إلى جانب إنجاز معاملاتنا البنكية، والتسوق وشراء الحاجيات، كل ذلك إضافة لما يجمعه عنا متصفح الإنترنت من خلال زياراتنا العديدة، قد يكون قابلاً للاختراق بسهولة إذا لم نحصّن أنفسنا بكلمات سر قوية.

تخيّل أن شخصاً يتجول في منزلك أو غرفة نومك، ويضطلع على تفاصيل حياتك، ويعرف أماكن تخبئة أموالك ومقتنياتك الثمينة، وأنه تمكّن من ذلك لأنك اعطيته مفاتيحك أو لأنك تركت أبواب منزلك وشبابيكه مشرعةً أمامه.

إن اختيارنا لكلمات مرور ضعيفة وسهلة الاختراق، واستهتارنا بمراعاة حفظها وذكرها أمام أيّ كان، يُعرّضنا لاقتحام الغرباء لحساباتنا وخصوصيتنا، خاصة وأن كلمات السر الضعيفة وسهلة التخمين هي السبب الأول لعمليات الاختراق حول العالم، وفق ما أظهر التقرير السنوي لشركة "فيريزون" الأمريكية للاتصالات والذي بيّن أن 81٪ من اختراق البيانات في عام 2017 كان بسبب كلمات المرور الضعيفة أو المسروقة.[1]

إن أغلب الطرق الشائعة التي يستخدمها المخترقون لسرقة كلمات السر تكون عبر "التصيد الإلكتروني"، والذي يتم من خلال إرسال رسائل إلكترونية زائفة قد تحتوي على روابط تقوم بتوجيه المستخدم إلى مواقع الكترونية مُصمّمة خصيصًا لسرقة معلوماته، أو بتحميل روابط خبيثة على جهاز الضحية، إضافة لاستخدام أحد أساليب الهندسة الاجتماعية عبر خداع الضحية واستدراجه للحصول على ما يرغب

تُعتبر كلمة السر بمثابة المفتاح للوصول إلى كافة معلوماتنا وبياناتنا الشخصية المخزّنة على أجهزتنا، وكما نعتني باختيار مفتاح محكم لمنزلنا أو خزانة أموالنا يجب أخذ الاحتياطات اللازمة لتكون كلمة سرنا قوية تتميز بتشفيرٍ عالٍ ووثوقيةٍ تامة، بحيث يصعب سرقتها واستخدامها في فتح حساباتنا أو انتحال شخصيتنا.

[1] "81% of Company Data Breaches Due to Poor Passwords",tracesecurity,August 14, 2018,https://www.tracesecurity.com/blog/articles/81-of-company-data-breaches-due-to-poor-passwords.

فيه. ومن هنا فإن أفضل وأبسط وسيلة لإحباط محاولات التصيد الإلكتروني، هي تجنب النقر على روابط في رسائل البريد الإلكتروني والتي قد تكون روابط خبيثة، إلى جانب الحذر من الطرق والوسائل المقنعة التي يستخدمها المخترقون للإيقاع بالمستخدمين في الفخ وسرقة كلمة السر الخاصة بهم.

يُعدّ اختيار كلمات سر قوية بمثابة خط الدفاع الأول عن خصوصية أجهزتنا وحماية بياناتنا، وهو ما يدعونا إلى التعرف على كيفية الحصول على كلمات محصنة، واتخاذ الإجراءات الأمنية التي تحمينا من الوقوع ضحايا للمحتالين الإلكترونيين.

كما ينصحنا خبراء الأمن الرقمي بتغيير كلمات السر بشكل دوري "كل ثلاثة أشهر على سبيل المثال"، لما في ذلك من أهمية بالغة من أجل الحفاظ على سرية البيانات، ولتسهيل ذلك يمكن اعتماد تطبيقات إلكترونية يمكنها تغيير كلمات المرور الخاصة بالمواقع الرئيسية على شبكة الإنترنت تلقائياً بشكل دوري ومنها "lastpass" و "dashlane".

حثت شركة "كاسبرسكي لاب" (وهي شركة متخصصة في أمن الحواسيب)، في شهر تشرين الثاني/نوفمبر 2018، الطلبة على توخي الحذر على الإنترنت، بعد اكتشافها وقوع هجمات إلكترونية استهدفت 131 جامعة على الأقل في 16 بلداً حول العالم، اشتملت على ما يقرب من 1000 هجوم تصيد، شُنّت منذ أيلول/سبتمبر 2017، وذلك بهدف سرقة معلومات الجامعة الحساسة.

ويسعى المخترقون وراء الحصول على بيانات اعتماد الدخول الخاصة بالموظفين والطلبة وعناوين بروتوكول الإنترنت (IP) الخاصة بهم وبيانات الموقع، ويُنشؤون في معظم الحالات صفحات ويب احتيالية لإدخال معلومات تسجيل الدخول التي تتضمن كلمة المرور إلى الأنظمة الرقمية في الجامعات، وتكون هذه الصفحات مطابقة بشكل واضح للنظم الأصلية.

وأشارت الشركة إلى أنه على الرغم من اهتمام الجامعات بأمن نظمها التقنية، إلا أن المهاجمين أوجدوا طرقاً لاختراق تلك النظم عبر استهدافهم المستخدمين المهملين بوصفهم الحلقة الأضعف.[2]

كيف يتمكن القراصنة من كشف كلمة السر الخاصة بنا؟

يتحسس القراصنة كلمات سر مستخدمي الإنترنت بواسطة ما يسمونه بـ "هجمات القوة الغاشمة"، وفيها يوظفون برامج حاسوبية تقوم بشكل أوتوماتيكي كامل بتجريب عدد غير محدود من توليفات الحروف والأرقام والرموز، كما تقوم بتجريب كلمات قواميس ومعاجم بأكملها بشكل آلي تام، وذلك بهدف التمكن من سرقة كلمات سر مستخدمي الإنترنت وحساباتهم الإلكترونية.[3]

---

[2] "Scholars beware: phishing fraudsters hunt for university credentials",01 NOVEMBER, 2018,https://www.zawya.com/mena/en/press-releases/story/Scholars_beware_phishing_fraudsters_hunt_for_university_credentials-ZAWYA20181101100442/

[3] "كيف تحمي كلمة السر الخاصة بك من قراصنة الإنترنت؟"،دويتشه فيله، 6 نيسان/أبريل 2015. (آخر زيارة 26 تشرين الثاني/نوفمبر 2018).
https://www.dw.com/ar/%D9%83%D9%8A%D9%81-%D8%AA%D8%AD%D9%85%D9%8A-%D9%83%D9%84%D9%85%D8%A9-%D8%A7%D9%84%D8%B3%D8%B1-

ويوصي الخبراء باستخدام الشبكة الخاصة الافتراضية "VPN" عند استخدام شبكة عامة مفتوحة، حيث يكون من السهل اختراق حسابات المستخدمين وكلمات سرهم، من خلال التنصت على البيانات وتخزينها، إذ تعمل "الشبكة الخاصة الافتراضية" على تشفير البيانات وجعلها مجهولة، عبر إنشاء نفق وهمي بين الجهاز ومزود الخدمة ، مما يعني عدم قدرة أي أحد على اعتراضها، وهو ما يجعل القراصنة غير قادرين على التجسس.

حاول الإبداع في تأليف كلمة السر الخاصة بك، من أجل ابتكار كلمة تجمع بين التعقيد وصعوبة الاختراق، وسهولة الحفظ والتذكّر في الوقت نفسه.

نقاط مهمة عند اختيار كلمة السر:

1. أن تكون طويلة بحدود 14 حرفًا على الأقل، إذ يسهل اختراق كلمات السر القصيرة.
2. أن تكون معقدة أي تحتوي على حروف كبيرة وصغيرة وأرقام ورموز، وهو الأمر الذي يزيد صعوبة اختراقها.
3. أن تكون عشوائية لا تستخدم أنماط معتادة مثل: 1234 أو QWEASD.
4. أن لا تحتوي على أية معلومات عن الهوية الشخصية مثل تاريخ أو مكان الميلاد أو أرقام هواتف أو حتى معلومات متعلقة بصاحب الحساب مثل طعامه المفضل أو المدينة التي يقطنها.
5. أن تكون كلمة سر يمكن تذكرها دون الحاجة لكتابتها على ورقة أو ملف يسهل فتحه، كتخزين كلمة السر في ملف إكسل، مثال: Ig3GaM20bFmRf وهي اختصارات لعبارة بالإنكليزية: I got 3 gifts at my 20th birthday from my friends.
6. أن تكون كلمة سر فريدة لا تُستخدم نفسها لأكثر من حساب وذلك لتقليص حجم الضرر الذي قد يتأتى عن اكتشافها.
7. تغيير كلمة السر بشكل دوري "كل ثلاثة شهور فترة جيدة".
8. التعرّف على كيفية استعادة كلمة السر أثناء إنشاء الحساب، إذ تستخدم مواقع عدة أدوات لاستعادة كلمة السر، وهنا يجب الحرص على أن تكون عملية الاستعادة آمنة، ففي حال استخدام سؤال لاستعادة كلمة السر يجب أن تنطبق على جوابه نقاط اختيار كلمة السر نفسها.
9. عدم كتابة كلمة السر على أجهزة عامة أو أجهزة الأصدقاء، إذ تقوم برامج رصد لوحة المفاتيح بتسجيل أي كلمة يتم طباعتها على الحاسوب، ويصبح بالإمكان سحب كلمات السر بسهولة.
10. استخدام برنامج آمن لإدارة كلمات السر مما يساعد على اختيار كلمات سر قوية دون الحاجة لحفظها جميعاً مثل برنامج "Keepass".

%D8%A7%D9%84%D8%AE%D8%A7%D8%B5%D8%A9-%D8%A8%D9%83-%D9%85%D9%86-%D9%82%D8%B1%D8%A7%D8%B5%D9%86%D8%A9-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA/a-18362338

ما هو برنامج Keepass؟

برنامج مجاني مفتوح المصدر وموثوق، يعمل على حفظ وتخزين كلمات المرور الخاصة بالمستخدم بطريقة سهلة وآمنة، وتجميعها في ملف واحد مُشفّر، يمكن تحميله من هنا.

مزايا برنامج كيباس "Keepass":

- يتيح حفظ عدد كبير من الحسابات متضمنة كلمة السر واسم المستخدم لكل حساب.
- يقترح كلمات سر صعبة تتكون من أحرف ورموز وأرقام من خلال مولّد كلمات السر الذي يحتويه.
- ينظم الحسابات وكلمات السر الخاصة بها ضمن مجموعات، على سبيل المثال: مجموعة حسابات الشبكات الاجتماعية، مجموعة حسابات البريد الإلكتروني.
- إمكانية البحث ضمن البرنامج عن حساب معين.
- إمكانية نقل ملف الحسابات وكلمات السر على فلاشة أو حفظها على التخزين السحابي.
- وذلك إلى جانب سهولة الاستخدام، وتوفره بثلاثين لغة.

كيف يمكننا أن نزيد من أمان حساباتنا في حال فقدان كلمة السر أو سرقتها؟

ميزة التحقق بخطوتين: هي من الخاصيات التي تندرج ضمن طرق تعزيز حماية حسابات المستخدم، إذ أنها تطلب التأكيد من خلال وسيلة مختلفة على أن عملية تسجيل الدخول تتم عبر صاحب الحساب، فبعد إدخال كلمة السر يحتاج المستخدم إلى رمز إضافي قد يكون عبر الهاتف أو باستخدام برنامج مولّد الرموز من "غوغل"، الأمر الذي يساهم في تحصين الحساب.

تُقلل خاصية التحقق بخطوتين كثيراً من انتحال هوية المستخدم، والدخول غير المُصرّح به إلى معلوماته الحساسة والاستيلاء عليها.

وقد باتت كافة وسائل التواصل الاجتماعي تستخدم ميزة التحقق بخطوتين، والتي يمكن تفعيلها من خلال عدة طرق منها :

- الرسائل النصية "SMS".
- تطبيق إنشاء الرموز.
- رموز الاسترداد.

المؤسسات المشاركة بالحملة:

منظمة سوريون من أجل الحقيقة والعدالة: منظمة سورية مستقلة، تأسست عام 2015، تعمل على توثيق انتهاكات حقوق الإنسان في سوريا، وقضايا المناصرة في المحافل الدولية.

جريدة عنب بلدي: مؤسسة إعلامية سورية مستقلة تأسست عام 2011 في مدينة داريا بريف دمشق، وتصدر مطبوعة أسبوعية، سياسية، اجتماعية، منوعة.

راديو روزنة: إذاعة سورية انطلقت عام 2013، تقدم نشرات ومواجز إخبارية متعددة وبرامج ثقافية وتوعوية وخدمية متنوعة، وتنشط أيضاً عبر موقعها الإلكتروني.

الشبكة السورية للإعلام المطبوع: تأسست عام 2014، وهي تجمّع لصحف ومجلات سورية مستقلة، تعمل على تنسيق الجهود فيما بينها من خلال تبادل الخبرات الصحفية والمهنية.

منظمة آرتا للإعلام والتنمية: وهي منظمة غير حكومية غير ربحية، مقرها في مدينة عامودا بمحافظة الحسكة، تعمل على تطوير مشاريع إعلامية مستقلة وتدريب ودعم صحفيين.

مشروع سلامتك: تأسس عام 2012، يهدف لنشر التوعية والمساعدة حول الأمن الرقمي، عبر تقديم الدعم التقني للمنظمات السورية، والمساعدة التقنية عبر الإنترنت، والتدريب الميداني.

موقع أنا إنسان: يركز على نشر القصص الإنسانية، وبشكل خاص قصص السوريين، بهدف طرح ومعالجة قضايا متعددة، وتوثيق معاناتهم والانتهاكات التي ارتُكبت بحقهم، إلى جانب عرض تجارب نجاحهم وإنجازاتهم.