كيف نؤمّن على حياتنا وبياناتنا بكلمات مرور قوية؟

أكثر ما يسعى المخترقون للوصول إليه.. كيف تتم سرقة كلمات المرور؟

تعدّ سرقة كلمات المرور واختراق الحسابات المختلفة عبر الإنترنت أسهل مما يمكن توقعه، وهي حوادث شائعة رغم ما نشهده من تطور تكنولوجي، وقد يلجأ المخترقون لأساليب عدة من أجل الوصول لغاياتهم، منها تخمين كلمات المرور والتي قد تكون سهلة ويمكن التنبؤ بها، أو استخدام أداة إعادة تعيين كلمة المرور لإنشاء كلمة مرور جديدة دون معرفة مالك الحساب وموافقته، كما يمكن إيقاع المستخدم في فخ التصيّد الاحتيالي والروابط المشبوهة عبر أساليب الهندسة الاجتماعية.

يمكن تعريف "الهندسة الاجتماعية" في سياق أمن المعلومات على أنها استخدام الخداع للتلاعب بالأفراد من أجل الكشف عن معلوماتهم السرية أو الشخصية والتي يمكن استخدامها لأغراض احتيالية.[1]

[1] للمزيد: انظر: "دليل خطوات عملية في الحماية الرقمية"، سوريون من أجل الحقيقة والعدالة. 5 كانون الأول/ديسمبر 2018. (آخر زيارة للرابط: 8 شباط/فبراير 2020). https://stj-sy.org/ar/1045/.

○ حوادث حول سرقة كلمات المرور:

تعرضت جنى "اسم مستعار لشخصية حقيقية" لسرقة كلمة مرور حساب "الفيس بوك" الخاص بها، مما جعلها عرضة للابتزاز المادي والمعنوي من خلال تهديدات وصلتها بنشر صورها الخاصة ومعلوماتها الشخصية الموجودة في مراسلاتها.

كانت "جنى" تستخدم كلمة مرور سهلة ومعروفة من قبل جميع مقربيها، ولم تكن تكترث لأمانها الرقمي، لأنها كانت تعتقد أنه ما من شيء قيّم يمكن اختراق حساباتها لأجله، وأنه لا يوجد لديها ما يمكن خسارته، ولكن الأمور سارت كما لم تكن تتوقع بل أسوأ بكثير.

بعد عرض قصتها على خبير أمن رقمي، تبيّن أن أحد أقربائها عمد إلى تغيير كلمة مرور حساب "الفيس بوك" الخاص بها عندما تمكن من الوصول إلى هاتفها الشخصي، لكنها لم تكتشف ذلك إلا بعد مرور عدة أشهر لأن التطبيق كان مفتوحاً على هاتفها، وبعد مرور هذه الفترة الزمنية من إعادة تعيين كلمة المرور عمد المخترق نفسه إلى ابتزاز "جنى" بمختلف الوسائل مدعياً أن رسائل الابتزاز تصل إلى حسابه الشخصي.

يقول خبير الأمن الرقمي لسوريون من أجل الحقيقة والعدالة معقباً:

"ارتكبت (جنى) الكثير من الأخطاء دون قصد، مما أوصلها إلى اختراق حسابها وما تلاه من استغلال وابتزاز، فقد استخدمت كلمة مرور سهلة وتحتوي على معلومة يعرفها الكثير من الأشخاص عنها وهي تاريخ ميلادها، كما أنها لم تحافظ على كلمة المرور الخاصة بها بشكل آمن بعيداً عن الأشخاص الذين من الممكن أن يستغلوا مثل هذه الفرص.

إضافة لذلك فإن (جنى) كانت تعتقد أنه لا يوجد لديها شيء لتخسره، رغم ما تحتويه محادثاتها من صور خاصة وبيانات تمسها بشكل شخصي، وهي نقاط حساسة لدى غالبية العائلات في مجتمعاتنا بشكل وصولها إلى أشخاص غرباء الكثير من المشاكل التي قد تنتهي أحياناً بجرائم شرف.. لم تشعر جنى بقيمة هذه الأشياء إلا عندما خسرتها ووقعت بيد من يستغلها لأغراضه الشخصية."

○ اختراق آلاف الحسابات في "دزني بلس" خلال أسبوع:

بعد نحو أسبوع من طرح شركة "دزني" خدمة بث الفيديو "ديزني بلس" تم اختراق آلاف الحسابات من خلال قراصنة الإنترنت، وأبلغ العديد من المستخدمين عن سرقة حساباتهم في "ديزني بلس" على مواقع التواصل الاجتماعي، وفق ما نشر موقع "زد نت" المعني بشؤون التقنية، والذي أشار إلى أن ذلك لا يعني أن الشركة بحد ذاتها اخترقت، بل قد تكون معظم عمليات اختراق الحسابات نجمت بسبب تكرار مالكيها لكلمات مرور يستعملونها في حسابات أخرى، أو نتيجة استخدام برمجيات خبيثة لسرقة كلمات المرور، أو رسائل التصيد، أو الهجمات العنيفة ضد كلمات المرور الضعيفة وأسئلة إعادة تعيين كلمات المرور ذات الإجابات السهلة.[2]

○ كيف تتم سرقة كلمات المرور؟

أ. تخمين كلمة المرور:

يمكن للمخترق توقع كلمة المرور والوصول إليها في حال كانت بسيطة وتعتمد على تفاصيل شخصية معروفة عن المستخدم مثل رقم هاتفه أو تاريخ ميلاده أو عنوانه.

---

[2] "لم يمض أسبوع على طرح الخدمة.. آلاف الحسابات في ديزني بلس باتت مخترقة". الجزيرة نت. 9 تشرين الثاني/نوفمبر 2019. (آخر زيارة للرابط: 7 شباط/فبراير 2020). http://tiny.cc/rjdqjz.

ب. برامج تكوين كلمات السر العشوائية:

قد يعمد المخترقون إلى استخدام كلمات السر العشوائية أو ما يسمونه "هجمات القوة الغاشمة"، والتي تُجرّب بشكل آلي وسرعة فائقة عدد غير محدد من احتمالات توليفات الرموز والأرقام، وكلمات القواميس وتحليل الشيفرات وكسر الخوارزميات، بهدف الوصول إلى كلمة المرور الصحيحة للضحية والتمكن من سرقة حساباته.

ت. خاصية إعادة تعيين كلمة المرور:

إذا كان المخترق على علم بإجابات الأسئلة السرية لحساب الضحية يمكنه إعادة تعيين كلمة المرور، وتسجيل الدخول باستخدام كلمة مرور جديدة.

بعض تطبيقات موقع "فيس بوك"، قد تكون طريقة لكشف كلمة المرور، إذ ينشر الأشخاص عن طريق الإجابة على الأسئلة التي تطلبها تلك التطبيقات معلومات شخصية عنهم، ربما يكون بعضها إجابات على أسئلة أمان استرداد الحساب الشائعة، وبالتالي يقوم المستخدم بتسليم معلوماته الهامة بطريقة غير مباشرة ، مما يجعل من السهل التحايل على أدوات استعادة كلمة المرور.

ث. التصيد الاحتيالي:

ويتم عن طريقها إرسال رسائل خادعة ولكنها تبدو حقيقية أو طبيعية ويُطلب من خلالها إدخال كلمة المرور. كأن يُرسل المخترق رابطاً لخبرٍ مثيرٍ للفضول، أو لعرضٍ مغرٍ من أحد المتاجر وعند فتحه يطلب من المستخدم تسجيل بيانات الدخول في صفحة لها نفس تصميم موقع "فيس بوك"، وبذلك يحصل المخترق بسهولة على كلمة المرور.

وأيضاً قد يلجأ المخترق لإرسال رسالة للضحية عبر البريد الإلكتروني على أنها من خدمة العملاء في المصرف الذي يودع به أمواله، يخبره من خلالها بأن كلمة المرور الخاصة بحسابه البنكي ضعيفة وعليه تغييرها، ويطلب منه عن طريق الرسالة النقر على رابط سيقوده إلى موقع إلكتروني مزيف يُشبه في تصميمه الموقع الخاص بالمصرف، ومن ثم سيقوم الضحية بإدخال بريده الإلكتروني وكلمة المرور الخاصة به دون أن يشعر بوجود أي نية احتيالية، وسيحقق المخترق غاياته بالوصول إلى الحساب المصرفي للضحية والتحكم به، كما قد يتلقى الضحية اتصالاً هاتفياً من أحد الأشخاص على أنه عميل للمصرف ويعمل على إقناعه بالحاجة القانونية لحصوله على كلمة المرور، أو غيرها من المعلومات الحساسة.

تزايد عمليات سرقة كلمات المرور عام 2019

أشارت شركة "كاسبرسكي لاب" العالمية للأمن الرقمي، إلى ارتفاع استخدام البرمجيات الخبيثة المصممة لجمع بيانات المستخدمين، والمعروفة بأدوات سرقة كلمات المرور بشكل ملموس في عام 2019.

إذ ارتفع عدد المستخدمين المستهدفين بهذه الأدوات من نحو 600 ألف مستخدم خلال النصف الأول من عام 2018، إلى ما يزيد عن 940 ألف مستخدم خلال الفترة نفسها من عام 2019.

وتلتقط البرمجيات الخبيثة البيانات الحساسة بشكل مباشر من متصفحات الويب على أجهزة المستخدمين عبر طرق مختلفة، وقد تتضمن تلك البيانات تفاصيل الدخول إلى الحسابات عبر الإنترنت، والمعلومات المالية مثل تفاصيل بطاقة الدفع المحفوظة.[3]

[3] "تزايد عمليات سرقة كلمات المرور". البيان الاقتصادي.26 تموز/يوليو 2019. (آخر زيارة للرابط 7 شباط/فبراير 2020). https://www.albayan.ae/economy/last-deal/2019-07-26-1.3613784.

ج. حيلة عملية لإنشاء كلمات مرور قوية بسهولة:

ينصح الخبراء باستخدام عبارة مرور "Passphrase" بحيث يكون من السهل تذكرها ومن الصعب تخمينها. يمكن صياغة العبارة من كلمات عشوائية توضع بشكل ملتصق، ومن ثم يتم أخذ أول حرف من كل كلمة ووضع بعضها بأحرف كبيرة، ويُفضل إضافة أرقام ورموز خاصة.

ينصح الخبراء الألمان بالتفكير في جملة بسيطة يسهل تذكرها، وأن تشمل رقماً على الأقل، مثل:

My favorite food is pizza with 4 ingredients and extra cheese

يُأخذ الحرف الأول من كل كلمة: m,f,f,i,p,w,4,i,a,e,c

كما يُمكن تغيير حرف "a" بعلامة خاصة مثل "@"

وعند جمع هذه الحروف مع الرقم ومع وضع الحرف الأول بالرسم الكبير تصبح كلمة المرور **Mffipw4i@ec**[4] وهي كلمة مرور قوية من الصعب اختراقها أو تخمينها.

أصدرت شركة "NordPass" الأمريكية قائمة بأسوأ مئتي كلمة مرور لعام 2019 وذلك بناء على دراسة ما يزيد عن 500 مليون كلمة مرور سمحت للمخترقين بانتهاك حسابات مستخدمي الإنترنت.

أسوأ 10 كلمات مرور استُخدمت عام 2019:

1. 12345
2. 123456
3. 123456789
4. test1
5. password
6. 12345678
7. zinch
8. g_czechout
9. asdf
10. qwerty

كما يستخدم كثيرون أسماء النساء ككلمات مرور، ومن أكثرها شعبية نيكول وجيسيكا وهانا.[5]

○ تطبيقات إدارة كلمات المرور:

تقوم هذه التطبيقات بإنشاء كلمات مرور قوية وعشوائية، وتخزينها بطريقة آمنة وسهلة. يكفي أن يحفظ المستخدم كلمة المرور الرئيسية للبرنامج، إذ إنه سيتكفل بحفظ بقية كلمات المرور لجميع الحسابات في قاعدة بيانات مشفرة، وبذلك سيحصل المستخدم على كلمة مرور قوية لكل حساب، إضافة إلى توفيره الوقت.[6]

---

[4] "حيلة ينصح بها الخبراء الألمان لإنشاء كلمات سر قوية بسهولة"، الجزيرة نت، آخر تحديث 15 آذار/مارس 2019.

[5] "Here are the most popular passwords of 2019". NordPass. December 11, 2019. Last visited February 8, 2020. https://nordpass.com/blog/top-worst-passwords-2019/.

[6] "كيف تخلق عبارات مرور قوية واستخدام برامج إدارة كلمات المرور"، سايبر آرابس، آخر تحديث 31 كانون الأول/ديسمبر 2018.

✓ **برنامج كيباس "Keepass"**

هو برنامج مفتوح المصدر وموثوق يعمل على حفظ وتخزين كلمات المرور الخاصة بالمستخدم بطريقة سهلة وآمنة، وتجميعها في ملف واحد مُشفّر.

يُتيح هذا البرنامج حفظ عدد كبير من الحسابات متضمنة كلمة المرور واسم المستخدم لكل حساب، كما يقترح كلمات سر صعبة تتكون من أحرف ورموز وأرقام من خلال مولّد كلمات السر الذي يحتويه، بالإضافة إلى أنه يُنظم الحسابات وكلمات السر الخاصة بها ضمن مجموعات، على سبيل المثال: مجموعة حسابات الشبكات الاجتماعية، مجموعة حسابات البريد الإلكتروني وغيرها[7].

○ نصائح لحماية كلمات المرور:

1. استخدام كلمة مرور قوية، طويلة، معقدة، عشوائية، فريدة.
2. تغيير كلمة المرور بشكل دوري، وعدم استخدام كلمة مرور واحدة لأكثر من حساب.
3. تجنب فتح ملفات أو مرفقات البريد الإلكتروني المُرسَل من أشخاص غير معروفين، ويمكن التأكد من أن الروابط المُرسلة ليست روابط خبيثة من خلال فتحها عبر استخدام موقع_فيروس_توتال.
4. تجنب ربط الحساب برقم هاتف لا يُستخدم، أو مر على استخدامه فترة طويلة، وذلك حتى لا يتمكن من يقوم بشراء الخط الجديد من اختراق الحسابات، أما في حال ضياع الهاتف أو سرقته يتوجب تغيير الشريحة الـ "SIM" بشكل فوري ووقف الشريحة القديمة[8].
5. استخدام طرق تعزيز الأمان، ومن أهمها: استخدام بريد بديل، والتحقق بخطوتين.

أ. استخدام بريد بديل:

إن إضافة بريد إلكتروني بديل عند إنشاء الحساب يرفع من مستوى الأمان، وهو ما يؤمن عند محاولة أي مخترق تسجيل الدخول على الحساب من جهاز آخر، وصول رسالة تحذيرية على بريد المستخدم البديل تمكّنه من تأمين حسابه، وتغيير كلمة المرور إن اقتضى الأمر ذلك.

ب. التحقق بخطوتين:

تستلزم استخدام أكثر من نموذج تحقق للوصول إلى الحساب، فبعد إدخال كلمة المرور يحتاج المستخدم إلى رمز إضافي، الأمر الذي يساهم في تحصين الحساب.

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.

---

[7] للمزيد: "دليل خطوات عملية في الحماية الرقمية"، سوريون من أجل الحقيقة والعدالة"، 2018.

[8] "Protect Your Passwords From Hackers". Life Wire. January 24, 2020. Last visited, February 11, 2020. https://www.lifewire.com/stealing-a-password-1164408.