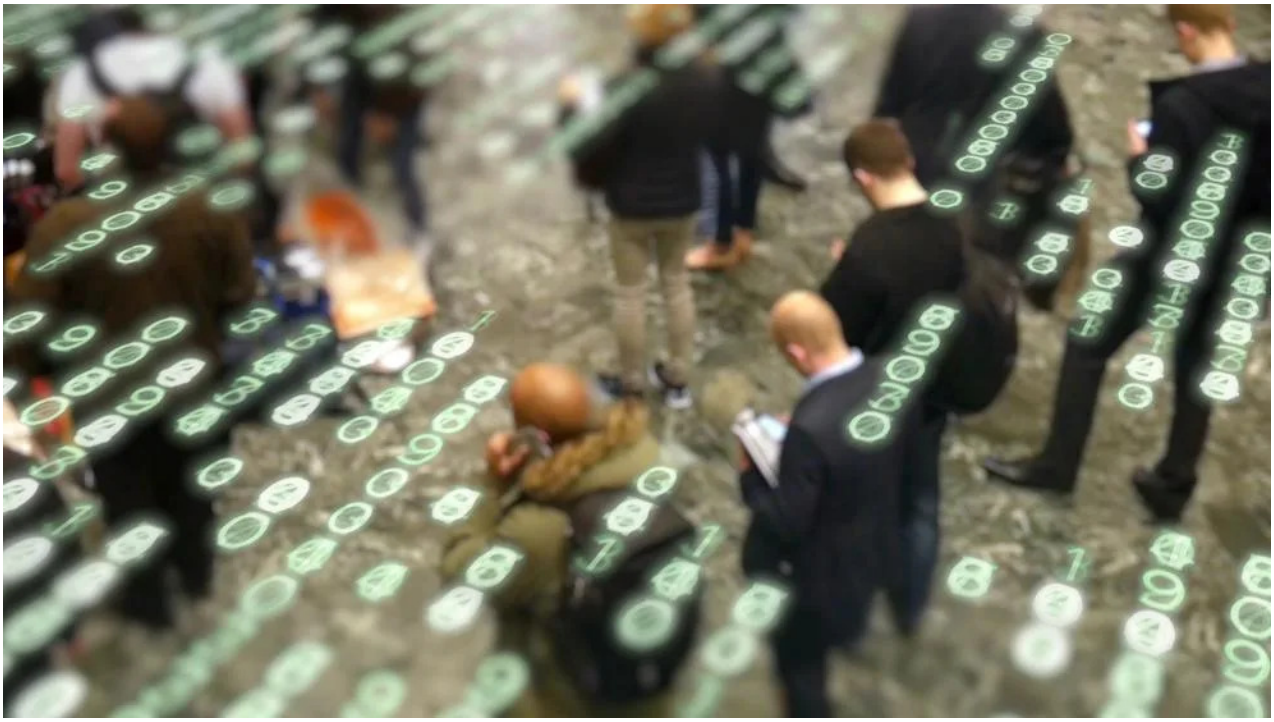
7 حيل إن قمت بها فلن يتمكن أي "هاكر" من اختراق حسابك



ترجمة وتحرير نون بوست

على الرغم من وفاة أندي غروف، وهو المهندس المجري الذي قاد الثورة التكنولوجية لأجهزة الكمبيوتر، والرئيس التنفيذي للشركة متعددة الجنسيات "إنتل" خلال هذه السنة، إلا أن إرثه التكنولوجي لا يزال قائما في عصر يغوص في مجال الابتكار التكنولوجي. وفي نفس الوقت، هو الشخص الذي حثنا على ضرورة الشعور بالارتياب أمام التكنولوجيات الحديثة.

في الحقيقة، لا يعدّ هذا التنبيه الأول الذي يؤكد لنا على ضرورة توخي الحذر أمام ما نقوم بنشره على شبكة الإنترنت. وفي هذا السياق، فإن الشبكات المفتوحة عن طريق الهواتف النقالة يمكن أن تكون، بسهولة تامة، عرضة إلى الاختراق من قبل أي شخص.

بالتالي، حثّ مدير مكتب التحقيقات الفيدرالي، جيمس كومي، الناس على المواظبة على تغطية كاميرا الكومبيوتر أثناء استعماله. وعلى الرغم من محدودية معرفتنا بمختلف البرمجيات التي تساعدنا على ضمان خصوصيتنا على شبكة الإنترنت، إلا أن هذه الحيل البسيطة من شأنها أن تقينا من خطر قرصنة حساباتنا على الانترنت.

1. استخدام كلمة عبور خاصة لكل خدمة

منذ الوهلة الأولى، نعتقد أن استخدام كلمة العبور نفسها لجميع أجهزتنا الإلكترونية الخاصة حلا منطقيا وفعالا. في المقابل، تجعلنا هذه الطريقة هدفا سهل الاختراق. وفي هذا الصدد، تجدر الإشارة إلى أن مارك زوكربيرغ، خلال بداية هذه السنة، قد تعرض للقرصنة بسبب استعماله لنفس كلمة العبور لحساباته على موقع" لينكد إن"، و"تويتر" و"بنترست". وفي هذه الحالة، يكفي أن يتمكن المخترق من قرصنة أحد هذه الحسابات ليتمكن من اختراق بقية الحسابات الأخرى.

بالإضافة إلى ذلك، فإن كلمة السر التي كان يعتمدها زوكربيرغ كانت بسيطة وسهلة جدا، مثل "dadada". حريصين نكون أن المهم من ،مختلفة عبور كلمات استخدام جانب إلى أنه بالذكر والجدير

على عدم استخدام مفاتيح واضحة والجمع بين الأحرف الكبيرة والصغيرة والأرقام.

2. تعديل كلمة العبور الخاصة بالهاتف الجوال

فضلا عن الولوج إلى الهاتف عن طريق بصمة الإصبع، من الضروري أن نقوم بإعادة تعديل كلمة السر التي تتكون من أربعة أرقام فقط، نظرا لأن "الهاكر" لديه فرصة من أصل عشر محاولات لفك تشفير أي كلمة مرور. وبالتالي، إذا كانت كلمة العبور الخاصة بك مطابقة لأي تشكيلة من المجموعات التالية: 1234 ,9999,1111,3333,0000,5555,1212,6666,7777,1313،2000,8888 4444,4321,222 2,2001,6969,1010

فيُستحسن تغييرها في أقرب وقت ممكن.

3. استخدام وسائل "استيقان" مزدوجة للبريد الإلكتروني الخاص بك

من المرجح أن يعتبر البريد الإلكتروني الخاص من أكثر البوابات المتاحة للوصول إلى بياناتك الشخصية. وبهذه الطريقة، فإن المخترق الإلكتروني سيتمكن بسهولة تامة من تغيير كلمات العبور الخاصة بحساباتك المصرفية والشبكات الاجتماعية. وبالتالي، فإن التحسين البسيط لخصوصية بياناتك يكمن في ضبط الإعدادات الخاصة ببريدك الإلكتروني عن طريق عملية "الاستيقان".

4. تشفير القرص الصلب الخاص بك

وهي طريقة بسيطة للغاية، إذ يكفي أن تدخل إلى قائمة "الأمن والخصوصية" في جهاز الحاسوب الخاص بك، سواء كان "ويندوز" أو "ماك"، وتقوم بتفعيل خاصية التشفير "FileVault".

مشهد من فيلم "عدو في الشبكة"

5. استخدام تطبيق "سيجنال" عند إرسال رسائلك الخاصة

من المعلوم أن تطبيق الواتساب يُصنّف من ضمن أكثر التطبيقات استخداما في العالم. ومع ذلك، فإن محتوى الرسائل التي ترسلها من خلال هذا التطبيق ليس مشفرا. وبالتالي، إذا كنت ترغب في إرسال رسائل وصور وأشرطة فيديو دون أن ينتابك قلق من عمليات الاختراق، فيمكنك استخدام هذا التطبيق.

تطبيق المراسلة "سيجنال"

6. الاعتماد على التصفح المتخفي

انطلاقا من فرضية عدم وجود أي نظام آمن بنسبة مائة بالمائة، فإن التصفح المتخفي على "جوجل كروم" أو متصفح "فاير فوكس" السري ليسا بالأنظمة المجانية الأكثر فعالية. لذلك، فإن برنامج التخفي "تور" الذي يعتمد على نظام "التسيير البصلي"، يتيح لمستخدميه فرصة الاتصال دون الكشف عن هوّياتهم على شبكة الإنترنت.

7. إذا لم تكتف بمتصفح "تور"، عليك بمحرك البحث "دك دك غو"

يعتبر "دك دك غو" من ضمن محركات البحث الخاصة الأكثر أمانا، حيث يقوم بمحو جميع آثار البحث الخاصة بك على شبكة الإنترنت.

المصدر: لافانغواردیا