

## هذا ما يمكن للقراصنة فعله إذا حصلوا على بريدك الإلكتروني



ترجمة وتحرير نون بوست

قالت الكاتبة، ميغان جونز، في تقريرها الذي نشرته مجلة "ريدرز دايجست"، إنه بمجرد وصول المخترق إلى بريدك الإلكتروني، سيتمكن عندها من كشف الكثير من المعلومات الخاصة بك. وفيما يلي بعض الأشياء التي يستطيع قراصنة الإنترنت القيام بها وكيفية الحفاظ على سلامتك.

إرسال رسائل البريد الإلكتروني من عنوانك

أوردت المجلة أنه بمجرد حصول المخترقين على عنوان بريدك الإلكتروني، يمكنهم استخدامه لاستهداف أكبر عدد من الأشخاص الموجودين ضمن قائمة الاتصال الخاصة بك، ونشر البرامج الضارة وعمليات الاحتيال وطلبات المال. وعلى الرغم من أن هذه الأعمال غير ضارة في الغالب، إلا أنها قد تسبب مشكلة في بعض الحالات. وقال جايسون غلاسبرغ، المؤسس المشارك في "كازابا سيكيوريتي" والمدير التنفيذي السابق للأمن السيبراني لدى أرنست أند يونغ أند ليهمان براترز إن "المجرم يستطيع يسبب لشخص ما مشكلة في عمله، أو حتى التسبب في عدد من المشكلات في حياته الشخصية أو المهنية عن طريق انتحال شخصيته".

إرسال رسائل التصيد الاحتمالي

وأضافت المجلة أن غريغ كيلبي من شركة فيستيغ ديجيتال إنفاستيغيشن يحذر أنه "عندما يعرف المتسلل عنوان بريدك الإلكتروني، فإنه يصبح لديه نصف معلوماتك السرية وكل ما يحتاجه الآن هو كلمة المرور". ويستخدم المتسللون عدة طرق مختلفة لتحقيق ذلك، والأكثر شيوعًا هو بريد التصيد الإحتيالي الإلكتروني المخادع. ويتمثل ذلك في تصميم بريد إلكتروني يبدو في ظاهره شرعياً مثل أمازون

وإيبي وبايبال، لكنه مصمم لخداعك. وما أن يقوم الأشخاص بتسجيل الدخول على موقع الويب المزيف هذا، فإن المتسلل يتلقى على الفور بيانات الاعتماد وكلمة المرور الخاصة بالحساب الحقيقي للضحية“.

ومن بين الطرق الأخرى، قد تتلقى رسالة بريد إلكتروني تفيد بأن حسابك قد تعرّض للاختراق، لذلك تحتاج إلى تغيير كلمة المرور لأسباب أمنية. وما إن تقوم بتغيير كلمة المرور الخاصة بك، حتى يستحوذ عليها المتسلل على كلمة المرور الخاصة بك. بمجرد حصول المتسللين على كلمة مرورك، يصبح نطاق الأشياء التي يمكنهم القيام بها أكبر بكثير.

الولوج إلى حساباتك الإلكترونية

بينت المجلة أن العديد من الأشخاص يميلون إلى استخدام كلمة المرور نفسها لولوج حساباتهم الإلكترونية، حيث يمكن للمتسلل النقر على خانة ”نسيت كلمة المرور“ لحسابك على موقع التواصل الاجتماعي للاستفادة منه في وقت لاحق. وبعد ذلك، يتجه المتسلل إلى البريد الإلكتروني وينقر على الرسالة الإلكترونية التي تعنى بتغيير كلمة السر، فيكون بذلك قادرا على الوصول إلى أي حساب تريده.

الاطلاع على بياناتك الشخصية

أفادت المجلة أن الأمور التي يقدر المتسللون على القيام بها متصلة بعضها ببعض، وتعتبر بمثابة ردود فعل متسلسلة. وبمجرد وصول أحد المتطفلين إلى حساباتك على الانترنت، لك أن تتخيل قدر المعلومات التي سيكون قادرا على جمعها. ويقول خبير العلوم الجنائية في شركة ”سكيور فورسنيكس“، ألان بوكستون إن المخترق سيستخدم عنوان بريدك الإلكتروني للاطلاع على حساب فيسبوك الخاص بك ومعرفة قائمة أصدقاؤك وبعض صورك.

إن لم يكن ذلك كافيا، تابع بوكستون بالقول إنه في حال وضع المتسلل عنوان بريدك الإلكتروني في موقع لينكد إن وبحث عنك، سيعرف مكان عملك ووظيفتك وزملاؤك والأماكن التي درست فيها من قبل. إن هذه المعلومات كافية ليبدأ المتسلل مطاردتك في العالم الحقيقي، ناهيك عن إمكانية الحصول على معلومات أخرى من إنستغرام وتويتر.

سرقة بياناتك المالية

ذكرت الكاتبة أن المشاكل الكبيرة ستبدأ في الحدوث فور حصول المتسللين على بيانات بطاقة اعتمادك أو بطاقتك البنكية، فمن المؤكد أنك قد أرسلت هذه البيانات عن طريق البريد الإلكتروني في مرحلة ما. وعموما، يقود ذلك إلى جعل حساباتك المصرفية عبر الإنترنت هدفا رئيسيا للمتسللين خاصة إذا كنت تستخدم عنوان بريدك الإلكتروني لتسجيل الدخول إليها.

تصبح الأموال في خطر فور اختراق بريدك الإلكتروني، حيث سيكون من السهل تعيين إعادة تعيين الحساب المصرفي والبدء في إصدار المعاملات. ويمكن للمتسللين فتح حسابات بنكية باسمك والحصول على قروض، فضلا عن إفساد تصنيف بطاقة الائتمان الخاصة بك.

ابتزازك

في حال لم تكن الأمور مخيفة بما فيه الكفاية، يمكن للمتسللين استخدام معلوماتك الشخصية لإلحاق الضرر بك وتدمير سمعتك وتهديدك، خاصة إذا ما وجد المستخدم شيئا يمكنه استخدامه ضدك لأنك لا ترغب في أن يتداول في العلن.

وفي هذا الصدد، قال الخبير الأمني في شركة ريدوار، دانييل سميث إن: ”المخترقين قادرين على التجسس عليك ومراجعة عظم رسائل البريد الإلكتروني الشخصية الخاصة بك، وهي معلومات يمكن

استغلالها لابتزازك بسهولة“.

انتحال هويتك

يعتبر انتحال هوية شخص ما أسوأ سيناريو على الإطلاق، لاسيما وأن المتسلل قد حصل لنفسه على جميع معلوماتك الخاصة ومعلومات التعريف بشخصيتك. ونظرا لإمكانية احتواء البريد الإلكتروني على رقم الضمان الاجتماعي الخاص بك ومعلومات بطاقة الائتمان، يمكن أن تكون سرقة الهوية في متناول اليد بالنسبة للمتسللين.

كيف يمكنك البقاء في مأمن من المتسللين

في هذا السياق، ينبغي عليك تجنب استخدام عنوان بريدك الإلكتروني لتسجيل الدخول إلى مواقع أخرى، وتأكد من أن كلمة مرورك قوية ويصعب تخمينها. علاوة على ذلك، ينبغي عليك ألا تغير كلمات المرور كل شهرين لمزيد الأمان. ويوصي غلاسبرغ أيضًا بتأمين حساب بريدك الإلكتروني من خلال مصادقة ثنائية العامل. ومن جهة أخرى، لا تشارك المعلومات أو تكتب كلمة مرور البريد الإلكتروني على شبكات الواي فاي العامة، وكن ذكيًا فيما يتعلق بالمعلومات التي تشاركها عبر البريد الإلكتروني.

ماذا تفعل إذا كنت تعتقد أنك تعرضت للاختراق؟

خلصت المجلة إلى القول إنه في حال سمعت عن رسائل البريد الإلكتروني العشوائية التي يتم إرسالها من عنوانك، فعليك تغيير كلمة المرور الخاصة بك على الفور، وإعلام جهات الاتصال الخاصة بك حتى يتجاهلوا ما قد يصلهم من بريدك. من الجيد أيضا تغيير إعدادات الخصوصية الخاصة بالبريد الإلكتروني إلى أقصى درجة أمان وفحص الكمبيوتر بحثًا عن البرامج الضارة والفيروسات.

المصدر: ريديرز دايجست