الاحتيال الإلكتروني: "من فضلك احذر من الضغط على الرابط التالي!"

اتخذت ثورة "الذكاء الاصطناعي" مكانًا مهمًا في القيام ببعض الأعمال الدرامية كان آخرها مسلسل "المرآه السوداء"، الذي اتخذ من الذكاء الاصطناعي عنصرًا مهمًا تدور حوله أغلب الأحداث من اجتماعية إلى سياسة تمس رموز بعينهم إلى اقتصادية تمس اقتصاد بلاد بأكملها، متنبأً بأن ثورة الذكاء الاصطناعي لن تغيّر طريقتنا في التعامل مع الخدمات من حولنا فحسب، بل ستغيّرنا نحن شخصيًا.

كانت هناك حلقة من المسلسل مخصصة لما يُسمي بالقرصنة أو الاختراق الإلكتروني، ترى فيها بطل الحلقة يقول بخوف "لقد صوّروني في غرفتي من خلال جهاز الكمبيوتر الخاص بي" وانتهى الحال به أنه قاتل وسارق لبنك بأمر من جهة مجهولة لا يعرف كيف استطاعت الوصول إلى بياناته الشخصية، واحتفظت بكلمات السر الخاصة به، حتى استطاعت اختراق حاسوبه و تستطيع مراقبته من خلال الكاميرا، ولكن هل كل اختراق إلكتروني "قرصنة" أو "احتيال" إلكتروني ينتهي بنا إلى السرقة والقتل؟

بحسب تقرير عام 2016 لتتبع جرائم الاحتيال الإلكتروني عالميًا، يتم الإبلاغ عما يقرب من 100.000 حالة تعرض لجريمة احتيال إلكتروني كل شهر

كانت تلك نتيجة مبالغ فيها لما يمكن أن يصنع بنا الذكاء الاصطناعي خلال بضعة سنوات من الآن، ولكن هذا لا يعني أن العالم لا يُعاني من مشاكل الاحتيال الإلكتروني، إذ تكون جريمة الاحتيال الإلكتروني أكثر جرائم السرقة انتشارًا، فبحسب تقرير عام 2016 لتتبع جرائم الاحتيال الإلكتروني عالميًا، يتم الإبلاغ عما يقرب من 100.000 حالة تعرض لجريمة احتيال إلكتروني كل شهر، والمفاجأة هي وقوع الآلاف من الضحايا في الفخ، بسماحهم لمنتحلي الشخصية ومرتكبي هذا النوع من الجرائم بالاستحواذ على معلومات شخصية تمكنهم من انتحال شخصيتهم أو سرقة أموالهم.

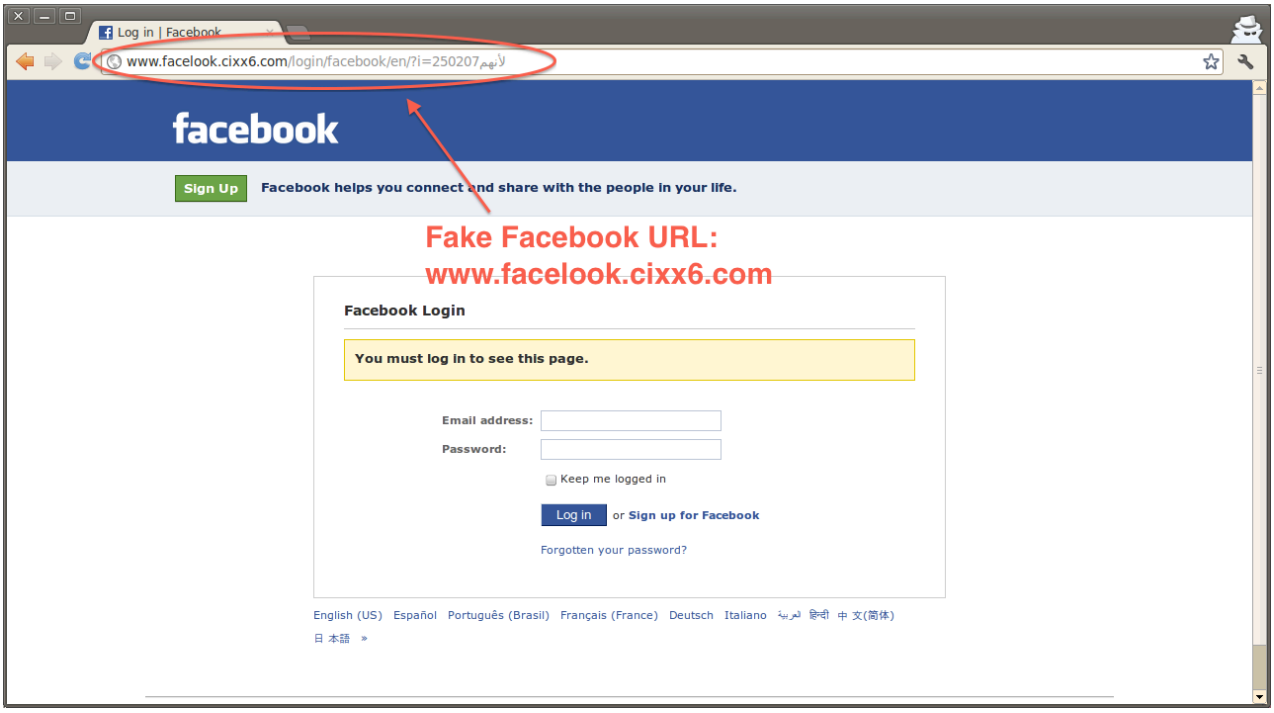
ما هو الاحتيال الإلكتروني؟

في البداية يجب أن نعرف ما هو الاحتيال الإلكتروني من الأساس، وما الفرق بينه وبين الاختراق الإلكتروني "القرصنة"، تبدو الأخيرة الأكثر سماعًا بين الشباب وخصوصًا مستخدمي مواقع التواصل الاجتماعي، إلا أن القرصنة لا تعني فقط الحصول على كلمة سر حساب أحدهم على فيسبوك أو حسابه على جوجل، بل تعني القرصنة إيجاد الطريقة المبدعة لحل المشاكل باستغلال بعض الملكيات للوصول إلى نتائج غير متوقعة، يبدو التعريف بسيطًا للغاية ولا يُجرم "القرصنة" ويعتبرها مجرد حل مبدع لمشكلة ما، هذا يدفعنا لسؤال لماذا يقوم الناس بالقرصنة من الأساس؟

يكون القراصنة في العادة شديدي الذكاء، فيدفع الفضول أغلبهم للقيام بالقرصنة على نظام معين، أو شبكة معينة، لفك أسرار تركيبها ومحاولة تقليد الشفرات التي تكون كل رابطة فيها، إلا أن الفضول لا يُعد السبب الأوحد، تختلف أسباب القراصنة من شخص لآخر، قد يكون بعضها يتعلق بالأمن القومي، والآخر يتعلق بأسباب اجتماعية، أو يتجه البعض أحيانًا للسرقة، وهنا يظهر "الاحتيال الإلكتروني".

لقد تعرض أغلبنا للاحتيال الإلكتروني من قبل، فالأغلب يستخدم البريد الإلكتروني يوميًا، وهذا ما يستخدمه عادة منتحلي الشخصية للوصول إليك، فيرسلون لك رسالة على بريدك الإلكتروني من البنك المعتاد لك أن تتعامل معه أو من إحدى الشركات التي اعتدت أن تشتري منها المنتجات أونلاين، لتجد الرسالة مفادها طلب معلومات شخصية عنك للتأكد من هوية المستخدم، فتجد البنك يطلب منك رقم الحساب وكلمة السر وغيره من المعلومات الشخصية عنك، أو تجد الشركة تعيد طلب رقم بطاقة الإئتمان الخاصة بك، كما نجد أمثلة مشهورة من مواقع التواصل الاجتماعي بسؤالهم كثير من الأسئلة ينتج عنها فقط سماحك لمنتحلي الشخصية الحصول على أغلب معلوماتك في غضون ثوان.

ما الحيل التي يستخدمها منتحلي الشخصية؟



صفحة مزورة لموقع فيسبوك

يستخدم أغلب منتحلي الشخصية مؤسسات يتعامل معها الفرد مباشرة ويثق بها، كالبنوك و مواقع التواصل الاجتماعي المشهورة كفيسبوك و تويتر، إلا أنهم كل ما يفعلوه أنهم ينتحلون شخصية تلك المؤسسات، كما يستخدمون أساليب معينة يحاولون بها شل تفكير المستخدم للحصول على المعلومات بشكل سريع قبل أن يتأكد المرء من صحة الرسالة أم لا، مثل عبارات تجدها في بداية أغلب الرسائل التي تم انتحال شخصية مرسليها، مثل: "تم اختراق حسابك بشكل غير قانوني" أو "تم استخدام حسابك من قبل مجهولين خلال الساعات الماضية، من فضلك اضغط الرابط التالي".

تعد صفحات الإنترنت المزورة من إحدى الحيل أيضًا، يقوم فيها المزور بتصميم واجهات مشابهة للمواقع الشهيرة كفيسبوك وجوجل

إحدى أشهر حيل منتحلي الشخصية إلكترونيًا، هي مساعدة ضحايا الكوارث، حيث تستغل عصابات الاحتيال الكوارث الطبيعية التي تضرب البلاد فتقوم بإرسال رسائل عبر البريد الإلكتروني تدعو للتبرع عبر تحويلات بنكية، ويقوم المحتالون بإنشاء مواقع لمنظمات خيرية لا وجود لها على أرض الواقع تستخدم كواجهة لعمليات النصب.

تعد صفحات الإنترنت المزورة من إحدى الحيل أيضًا، يقوم فيها المزور بتصميم واجهات مشابهة للمواقع الشهيرة كفيسبوك وجوجل وغيرهما، وعند القيام بوضع كلمة السر ورمز الدخول يستطيع القراصنة التحكم بجهازك وسرقة محتوياته بما فيها الحسابات البنكية.

تكون النصيحة الأشهر هي ألا يضغط المستخدم على أي رابط إن كان مصدر الإيميل مشكوكًا فيه، وإن ضغط المستخدم الرابط، عليه أن يقوم بالتواصل مع حساباته البنكية أو أي شركات يملك فيها حسابًا ما لحمايتها من الاختراق وحمايتها من السرقة، كما يوجد الآن منظمات مختصة فقط بتلقي بلاغات انتحال الشخصية الإلكترونية (phishing-Anti)، أما على المستوى الشخصي، يجب على كل مستخدم يتعرض لتلك المواقف أن يفكر مرتين قبل الضغط على أي رابط غير موثوق به، أو أن يقوم بتأكيد بياناته على أحد المواقع بدون التأكد من عنوان الصفحة وأن الموقع موثوق به بالفعل.

إذا كانت الرسالة على بريدك الإلكتروني تثير شكك بأي شكل من الأشكال، فربما أن تتعرض لمحاولة احتيال إلكتروني، فربما استطاع المقرصن التعرف على نمط حياتك عن طريق انفتاحك الزائد على مواقع التواصل الاجتماعي وتقديم معلومات شخصية سهلة الحصول عليها، ليكون المقرصن حسابًا وهميًا لأحد أصدقائك ليحاول به أن يوقعك في فخ جريمته الإلكترونية، لذا يجب على مستخدم الإنترنت أن يكون شديد الحرص على ما يقدمه من معلومات لأي جهة كانت، حتي ولو كانت صفحته الشخصية.

رابط المقال: https://www.noonpost.com/17198/