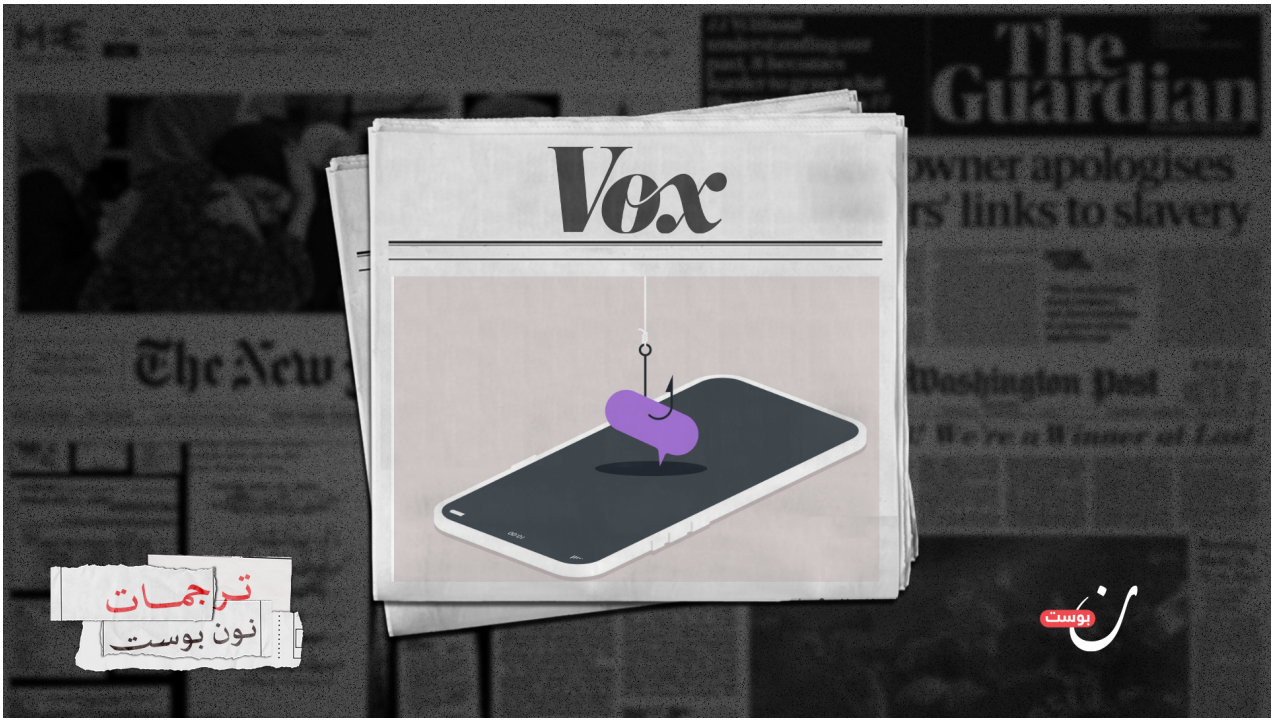
كيف تحمي نفسك من رسائل الاحتيال؟



ترجمة وتحرير: نون بوست

ما إن جلست لكتابة هذا النص، حتى وصلتني رسالة قصيرة تقول ببساطة: "مرحبًا". في وقتٍ آخر، ربما كنت سأشعر بالفضول تجاه هذه الرسالة الغامضة من رقم غير معروف، وربما تساءلت عن هوية مرسلها ورددت عليها، لكنني لم أعد حديث العهد على هذه اللعبة.

لقد تحوّلت الرسائل النصية الاحتيالية إلى صناعة بمليارات الدولارات. ومع تراجع المكالمات الآلية (الروبوتية) — بفضل قانون صدر عام 2009 وأجبر شركات الاتصالات على اتخاذ تدابير صارمة للحد منها — ارتفعت الشكاوى من الرسائل الاحتيالية بنسبة 500 بالمئة بين 2015 و2022. ورغم صعوبة تحديد العدد الدقيق للرسائل المزعجة التي تُرسل يوميًا، إلا أن المشكلة في تفاقم مستمر. ولم تعد المشكلة في كثرتها فحسب، بل باتت هذه الرسائل أكثر تطورًا ودهاءً من ذي قبل.

أود أن أقول إنني لم أنقر يومًا على رابط في رسالة مزعجة، لكن هذا غير صحيح. ربما كانت تتعلق بطرد غامض، أو بمخالفة مرور غير مدفوعة، أو بموضوع سياسي — لا فرق. فمع الكمّ الهائل من بياناتنا الشخصية المتاحة على الإنترنت، ومع دخول الذكاء الاصطناعي على الخط، أصبحت هذه الرسائل أكثر ذكاءً، واستهدافًا، وخطورة. المؤسف أن البرمجيات المصممة لصد الرسائل المزعجة لا تواكب بسرعة كافية البرمجيات التي تُستخدم في إنتاجها، وهو ما يثير القلق حيال علاقتنا المتغيرة بالتكنولوجيا.

هذه هي الأخبار السيئة، والأسوأ منها. أما الخبر الجيد، فهو أن البشر لا يزالون — حتى الآن — أذكى من الآلات. ومن خلال مزيج من الوعي الرقمي والأدوات البرمجية المناسبة، يمكنك تقليص تعرضك لمثل هذه الرسائل، أو على الأقل تقليل احتمال وقوعك ضحية للاحتيال.

المكالمات الآلية لم تكن بذلك السوء بعد كل شيء

تلقيت هذا الأسبوع رسالة احتيالية جديدة تزعم وجود مخالفة مرور غير مدفوعة، مرفقة برابط للدفع وخاتمة ودّية تقول: "فريق الطرق المدفوعة يتمنى لك يومًا سعيدًا!" ومن المفارقة أنني قد أكون مدينًا

فعلاً بمخالفة، لكنها بالتأكيد ليست من "فريق الطرق المدفوعة".

الرابط في الرسالة، الذي ينتهي بـ "نقطة وورلد"، كان أبرز مؤشر على الاحتيال. لم أنقر عليه، لكن لو كانت الرسالة أكثر تخصيصًا — باستخدام اسمي مثلًا أو بالإشارة إلى أن المخالفة وقعت في ولاية نيويورك حيث أقيم — لربما فعلت.

وهذا هو المسار الذي نتجه إليه. عمليات الاحتيال الشائعة، مثل الغرامات غير المدفوعة، عروض التوظيف، مصلحة الضرائب، أو الطرود غير المُسلّمة، تصبح أكثر خطورة بشكل كبير عندما تتضمن معلوماتك الشخصية مثل بريدك الإلكتروني أو عنوانك المنزلي.

ومع تزايد تسريبات البيانات خلال السنوات الأخيرة، باتت كمية هائلة من المعلومات الشخصية متاحة للمحتالين. وفي الوقت ذاته، سهّل الذكاء الاصطناعي التوليدي على المحتالين صياغة رسائل مقنعة خالية من الأخطاء اللغوية وبشكل جماعي. وأحيانًا، مجرد قراءتك للرسالة يمنح المحتالين فرصة للاستمرار.

تقول تيريزا موراي، وهي متخصصة في مراقبة شؤون المستهلك لدى صندوق التوعية التابع لمجموعة المصلحة العامة في الولايات المتحدة: "اعتمادًا على إعدادات إيصالات القراءة لديك، قد يتمكن المحتال من معرفة أنك قرأت الرسالة"، وتضيف: "ثم، لا قدّر الله، إذا نقرت على رابط أو اتصلت بالرقم الموجود في الرسالة، تبدأ اللعبة فعليًا".

هناك عدة طرق يمكن أن يستفيد بها المحتال. إذا نقرت على الرابط، فقد تُخدع لدفع المال أو تُضلل لتقديم المزيد من بياناتك الشخصية، والتي تُعد عملة بحد ذاتها في سوق الاحتيال. كثير من هذه الرسائل هي محاولات تصيّد، تقود روابطها إلى صفحات مصممة لسرقة بيانات الدخول. وفي أفضل الحالات، فإن مجرد النقر يثبت للمحتال أنك موجود ومستعد للتجاوب.

في سنة 2024، تجاوزت الخسائر الناتجة عن الاحتيال الهاتفي 25 مليار دولار، أي ما يعادل متوسط 450 دولارًا لكل ضحية. والمفارقة أن كبار السن أقل عرضة للوقوع في هذه الحيل، غالبًا لأنهم تعلّموا تجاهل المكالمات من أرقام غير معروفة.

فالغالبية العظمى ممن تجاوزوا سن الخامسة والستين في الولايات المتحدة يقولون إنهم لا يردّون على أرقام غير مألوفة، و57 بالمئة من هذه الفئة أدرجوا أسماؤهم في السجل الوطني لعدم الاتصال، وهي قاعدة بيانات تديرها هيئة التجارة الفيدرالية منذ سنة 2003، وفقًا لتقرير حديث من خدمة حظر المكالمات "ترو كولر".

أما الشباب الأميركيون، فحظهم أسوأ. فوفقًا للتقرير ذاته، فإن الأشخاص الذين تتراوح أعمارهم بين 18 و44 سنة أكثر عرضة بثلاث مرات من كبار السن للوقوع في عمليات الاحتيال الهاتفية، بما في ذلك الرسائل النصية المزعجة، وربعهم تقريبًا أبلغ عن تعرضه للاحتيال أكثر من مرة. ومع ذلك، لم يسجّل سوى 30 بالمئة منهم أسماءهم في سجل عدم الاتصال.

ما يمكنك فعله وما لا يمكنك فعله لتفادي الرسائل الاحتيالية النصية

بما أن "سجل عدم الاتصال" صُمّم أساسًا لمنع المكالمات غير المرغوبة من المسوّقين عبر الهاتف، فإنه لا يُسهم كثيرًا في الحد من الرسائل النصية العشوائية. والأسوأ أن كثيرًا من هذه الرسائل يصدر من خارج البلاد، ومع غياب جهة رقابية دولية على الاتصالات، يمكن لمحتال يُدير مزرعة شرائح في جنوب شرق آسيا أن يُغرق هاتفك بإشعارات حول طرود غير مُسلّمة كما يشاء.

مزارع الشرائح، المعروفة أيضًا بمزارع الهواتف أو بنوك الشرائح، هي أنظمة تحتوي على عدد كبير من

شرائح الاتصال، وتُستخدم لإرسال كميات ضخمة من الرسائل النصية أو إجراء المكالمات دفعة واحدة، ولا تتطلب أكثر من بضع مئات من الدولارات لتشغيلها. وبالنسبة للمحتالين، فاقتناء أرقام هواتف يُعد شبه مجاني، وعلى عكس المكالمات الآلية التي تتم في الزمن الحقيقي، تُرسل الرسائل العشوائية دفعة واحدة في لحظة قصيرة. وإذا تم حظر رقم معيّن، ينتقل المحتال ببساطة إلى رقم آخر ويواصل الإرسال. والآن، أصبح بإمكانهم أيضًا استخدام تقنيات التوليد الآلي لصياغة رسائل أكثر إقناعًا وتخصيصًا.

في المقابل، تخضع شركات الاتصالات لمتطلبات تنظيمية أقل لحماية عملائها من الرسائل الاحتيالية. فقد منح قانون إنفاذ وردع إساءة استخدام المكالمات الآلية الهاتفية، الذي بدأ تطبيقه سنة 2021، لجنة الاتصالات الفيدرالية أدوات لمنع المكالمات الآلية، بما في ذلك إطار التحقق من هوية المتصل يُسمى "ستير/شاكن". لكن اللجنة لم تصدر أول قاعدة تستهدف الرسائل النصية المزعجة بشكل خاص إلا في عام 2024.

قد يبدو لك أن منع هذه الرسائل بسيط مثل استخدام فلاتر البريد غير المرغوب فيه، كما هو الحال في خدمات المراسلة الإلكترونية منذ عقود. لكن الرسائل النصية ليست متقدمة تقنيًا كبريد الإنترنت. فالتقنية الأساسية، وهي خدمة الرسائل القصيرة، تعود إلى ثمانينيات القرن الماضي، وتكادتفتقر إلى أي آليات أمان.

يقول آدم مايرز، رئيس قسم مكافحة التهديدات في إحدى شركات الأمن الرقمي، في رسالة إلكترونية: "خدمة الرسائل القصيرة تفتقر إلى بروتوكولات تحقق مدمجة، كتلك المستخدمة في البريد الإلكتروني. ورغم أن شركات الاتصال ومطوري البرمجيات يطبّقون آليات فلترة وحظر، فإن المهاجمين يطوّرون أساليبهم باستمرار".

يتمثل التحدي في فلترة الرسائل غير المرغوب فيها دون حجب الرسائل المشروعة. وهذا يتطلب التمييز بين الرسائل التي تصلك من أصدقائك، أو من البنك، أو من سائق التوصيل، أو من صديق جديد لم يُدرج بعد ضمن قائمة جهات الاتصال، وبين الرسائل الاحتيالية. كذلك، تُرسل العديد من الشركات والمؤسسات رسائل مشروعة بكميات كبيرة باستخدام أرقام قصيرة — تتكوّن من خمسة أو ستة أرقام — يجب تسجيلها لدى الجمعية الأميركية المختصة بشؤون الاتصالات اللاسلكية، التي تنظّم أيضًا آليات التفاعل مع هذه الرسائل.

نصيحة مهمة: لا تحذف الرسائل الموثوقة فورًا

غالبًا ما تتلقى العديد من الرسائل الآلية من مصادر موثوقة مثل الصيدلية، البنك، أو خدمات توصيل الطعام. ويشمل ذلك رموز التحقق المستخدمة في المصادقة الثنائية، وكذلك الرسائل من الأرقام القصيرة، بما في ذلك الرسائل المتعلقة بالحملات الانتخابية.

لذا من الأفضل عدم حذف هذه الرسائل فورًا، لأن الرسائل الجديدة من نفس المصدر ستُضاف عادةً ضمن نفس سلسلة المحادثات، مما يسهل عليك التحقق من صحتها ويخفف عنك القلق.

تقول تيريزا موراي من منظمة حماية المستهلك: "من الأفضل أن تضيف تسمية لهذه الرسائل وتحفظ أرقامها في قائمة جهات الاتصال". وتضيف: "إذا تلقيت رسالة تبدو كرمز تحقق من بنك معين لكنها لم تصلك من الرقم المحفوظ، فهذا قد يشكل علامة تحذير مهمة".

لكن، للأسف، لا يهتم المحتالون كثيرًا بالقوانين أو اللوائح، وشركات الاتصالات لا تبذل جهدًا كافيًا لمواجهة السيل المستمر من الرسائل العشوائية. فبناء أنظمة فلترة قادرة على مواكبة أساليب المحتالين يتطلب تكاليف إضافية، وبعض الشركات تدرج هذه الأدوات ضمن تكلفة الخدمة، بينما تفرض

شركات أخرى رسومًا إضافية مقابل أدوات أكثر فعالية. فإحدى الشركات الكبرى، "فيريزون" على سبيل المثال، تقدم فلاتر أساسية مجانًا، وفلاتر متقدمة مقابل 4 دولارات شهريًا.

قال أليكس كويليتشي، المدير التنفيذي لخدمة حظر المكالمات "يومايل": "هذا عمل حقيقي ويتطلب قدرًا كبيرًا من التحليل. أنا متعاطف، لكن شركات الاتصالات تواجه مشكلة صعبة للغاية". عندما يتعلق الأمر بتجنّب الرسائل الاحتيالية النصية، لديك بعض الخيارات. بالإضافة إلى ما توفره شركة الاتصالات التي تتعامل معها، هناك تطبيقات مثل "تروكولر" و"تكست كيلر" و"روبوكيلر" و"هيا".

لم يسبق لي أن دفعت مقابل أي من هذه الخدمات، لذا لا يمكنني الجزم بمدى فعاليتها. لكن ما يمكنني قوله هو أن عدم الرد على الهاتف ما يزال وسيلة فعالة لتفادي المكالمات الآلية — وإن كان ذلك وسيلة رائعة أيضًا لتفويت مكالمة من عيادة الطبيب. يمكن انتحال هوية الرقم الظاهر بسهولة، لذا لا تجب على المكالمة ما لم تكن تتوقعها. وإن كنت غير متأكد، تجاهل المكالمة واتصل بالرقم الرسمي لاحقًا.

يمكنك أيضًا الإبلاغ عن المحتالين إلى لجنة الاتصالات الفيدرالية من خلال إعادة توجيه الرسالة إلى الرقم 7726، والذي يُكتب كلمة "سبام"، أوتقديم شكوى عبر موقع الوكالة الإلكتروني. كما يمكنك الإبلاغ عن جميع أنواع الاحتيال إلى لجنة التجارة الفيدرالية أو إلى المدعي العام في ولايتك. أما الأمر الأهم، فهو ألا تتفاعل مع المحتالين. حتى لو بدأوا بكلمة "مرحبًا" وبدا عليهم الود، فإن الرد أو حتى قراءة الرسالة العشوائية يُظهر للطرف الآخر أنك شخص حقيقي، ما يجعلك هدفًا محتملاً. في الوقت الحالي، تذكّر أنك أكثر ذكاءً من الذكاء الاصطناعي — وتجاهله.

المصدر: فوكس

رابط المقال: https://www.noonpost.com/315581/