الهجمات وعمليات الاحتيال عبر الهاتف

نظرة عامة

حين تسمع عن المهاجمين الإلكترونيين، تظنّ أنّ هذا الشخص هو العقل المدبّر الخبيث الذي يجلس أمام كمبيوتر ويشنّ هجمات متطوّرة بواسطة الإنترنت. ومع أنّ كثيرًا من المهاجمين الإلكترونيين المعاصرين يستخدمون التقنيات، مثل البريد الإلكتروني أو تطبيقات المراسلة الفورية، إلّا أنّهم يستخدمون الهواتف أيضًا في خداع ضحاياهم. ولاستخدام الهاتف سببان مهمّان. أولًا، قلّة التقنيات الأمنية التي تراقب الاتصالات الهاتفية وترصد الهجمات بواسطتها وتصدّها بعكس البريد الإلكتروني. ثانيًا، يسهل على المجرمين التأثير مشاعريًا عبر اتّصال هاتفي، ويزيد هذا من فرصهم في خداع ضحاياهم. لنعرف معًا كيف نرصد ونصدّ هذه الهجمات.

كيف تجري الهجمة عبر اتّصال هاتفي؟

أولًا، عليك فهم ما يريده هؤلاء المهاجمون. فهم يريدون مالك أو معلوماتك أو فرصة الوصول إلى كمبيوترك (أو كلّ ما سبق). ويفعلون هذا بخداعك لفعل ما يريدونه. يتّصل هؤلاء المجرمون بالناس في أنحاء العالم، ويتصنّعون حالات طارئة. وهدفهم هو افقادك تركيزك بإخافتك حتى لا تفكّر بطريقة سليمة، ثمّ يدفعوك نحو ارتكاب خطأ ما. تشمل بعض الأمثلة الشائعة عن تلك المحاولات ما يلي:

يدّعي المتّصل أنّه من إدارة الضرائب الحكومية أو مكتب جمع الضرائب ويخبرك عن ضرائب لم تدفعها. ثمّ يشرح لك أنّك إذا لم تدفعها فورًا فستُسجن، ثمّ يضغط عليك حتى تدفع الضرائب بواسطة بطاقتك الائتمانية أثناء الاتّصال. هذه عملية احتيال، فأكثر إدارات الشؤون الضريبية، بما في ذلك دائرة الإيرادات الداخلية الأمريكية، لا تتواصل مع الأشخاص بواسطة اتّصال هاتفي أو رسالة إلكترونية. حيث تُرسَل كلّ الإخطارات الضريبية الرسمية بواسطة البريد العادي.

يدّعي المتّصل أنّه من فريق الدعم التقني في شركة مايكروسوفت ويُخبرك أنّ كمبيوترك مصاب بفيروس. وبعد إقناعك بهذا، يضغط عليك لشراء برنامجه الخاص أو توفير الاتّصال عن بعد بكمبيوترك. لكن الحقيقية هي أنّ شركة مايكروسفت لن تتّصل برقم هاتفك المنزلي.

تتلقّى رسالة بريد صوتي آلي تُخبرك بإقفال حسابك المصرفي، وأنّه عليك الاتّصال برقم خاص لإعادة فتحه. وحين تتّصل يردّ عليك نظام ردّ آلي يطلب منك معلومات هويتك ويسألك عدّة أسئلة شخصية عنك. لكن هذا الاتّصال ليس من طرف المصرف، بل هو لتسجيل معلوماتك لسرقة هويتك.

حماية نفسك

تُعدّ أنت أفضل دفاع ضدّ هجمات الاتصال الهاتفي. لذا، احفظ النصائح التالية.

كُن شديد الحذر في كلّ مرّة يتّصل بك شخص ويتصنّع حالة طارئة أو يضغط عليك لفعل أمر ما. وإذا كان الاتّصال معتادًا في البداية، ثمّ استهجنته في مرحلة لاحقة، يُمكنك رفض ما يُطلب منك.

إذا شعرت أنّ الاتّصال هو هجوم عليك، عليك إنهاء الاتّصال ببساطة. إذا أردت التيقّن من أنّ الاتّصال حقيقي، يُمكنك زيارة موقع المنظمة الإلكتروني (مثل موقع مصرفك)، ثمّ البحث عن رقم خدمة العملاء والاتّصال بهم مباشرة. وبهذه الطريقة تتيقّن من أنّك تتحدّث معهم.

لا تثق برقم المتّصل الذي تراه على جهازك، لأنّ المجرمين يستطيعون تزييفه حتى يبدو وكأنّه من منظمة حقيقية أو يبدأ برمز الاتّصال في منطقتك.

لا تُمكّن للمتّصل من التحكّم المؤقّت بكمبيوترك أو خداعك لتنزيل برنامج عرضه عليك. فهذه هي الطريقة التي يُصيب بها المجرمون كمبيوترك بفيروس.

إذا كان الاتّصال من شخص لا تعرفه شخصيًا، فلا تردّ عليه حتى يتحوّل إلى صندوق البريد الصوتي. وبهذه الطريقة يُمكنك الاستماع إلى الاتصالات من جهات غير معروفة في وقت لاحق. ويُمكنك في هواتف كثير تفعيل هذا تلقائيًا من خلال ميزة «عدم الازعاج».

إنّ عمليات الاحتيال والهجمات عبر الهاتف بازدياد مطرّد. وأنت أفضل دفاع لرصدها وصدّها.

المحرّر الضيف

توفّر جِن فوكس خدمات تقييم المخاطر وتدريبًا في مجالي الوعي الأمني والهندسة الاجتماعية بصفتها مستشارة أمنية أولى في شركة All Covered. يُمكن متابعة جِن عبر حسابها على تويتر @j_fox.

لموارد

معلومات المستهلك الخاصة بالهويات والخصوصية والأمن عبر الإنترنت: https://www.consumer.ftc.gov/topics/privacy-identity-online-security

الابلاغ عن عمليات احتيال عبر الهاتف (في الولايات المتّحدة الأمريكية): https://www.ftccomplaintassistant.gov/#crnt

الهندسة الاجتماعية: https://www.sans.org/u/Fi5