الاحتيال عن طريق استغلال الاعمال الخيرية والكوارث

يعرف مجرمو الإنترنت أن إحدى أفضل الطرق لدفع الناس إلى ارتكاب خطأ هي من خلال خلق شعور متزايد بالإلحاح. وإحدى أسهل الطرق لخلق شعور بالإلحاح هي الاستفادة من الأزمات. هذا هو السبب في أن مجرمي الإنترنت ينتهزون الفرص عندما يكون هناك حدث صادم له تأثير عالمي. ما يعتبره معظمنا مأساة، يعتبره مجرمو الإنترنت فرصة، مثل اندلاع حرب، أوكارثة طبيعية كبرى مثل انفجار بركاني، وبالطبع انتشار الأمراض المعدية مثل COVID 19. عندما يكون هناك قدر هائل من وسائل التواصل الاجتماعي والتغطية الإخبارية حول حدث معين، يعرف مجرمو الإنترنت أن الوقت قد حان للبدء بالاستهداف.

يستغلون هذه الفرصة لإنشاء رسائل بريد إلكتروني للتصيد الاحتيالي في الوقت المناسب أو عمليات احتيال حول الحادثة، ثم إرسال بريد إلكتروني للتصيد الاحتيالي أو إطلاق عملية الاحتيال إلى ملايين الأشخاص حول العالم. على سبيل المثال، خلال كارثة طبيعية، قد يتظاهرون بأنهم مؤسسة خيرية تطلب تبرعات لإنقاذ الأطفال المحتاجين. غالبًا ما يتصرف مجرمو الإنترنت في غضون ساعات من وقوع أزمة أو كارثة، لأن لديهم كل البنية التحتية التقنية مجهزة مسبقا. السؤال هنا: كيف يمكننا حماية أنفسنا في المرة القادمة التي تحدث فيها أزمة أو كارثة كبيرة ويسعى مجرمو الإنترنت إلى استغلالها؟

كيف نكتشف وندافع ضد هذه الهجمات

مفتاح تجنب عمليات الاحتيال هذه هو أن تشك في أي شخص يحاول أن يصل إليك. على سبيل المثال، لا تثق في رسالة بريد إلكتروني عاجلة تدعي أنها من مؤسسة خيرية بحاجة ماسة إلى التبرعات، حتى لو بدا أن البريد الإلكتروني من علامة تجارية تعرفها وتثق بها. لا تثق في مكالمة هاتفية تدعي أنها بنك طعام محلي تضغط عليك للتبرع. كلما زاد الشعور بالإلحاح، زاد احتمال وقوع هجوم. فيما يلي بعض المؤشرات الأكثر شيوعًا للخداع الخيرية:

- كن متشككًا جدًا في أي مؤسسة خيرية تتطلب التبرع عبر العملة المشفرة أو ويسترن يونيون أو تحويل الأموال أو بطاقات الهدايا.
- يمكن لمجرمي الإنترنت تغيير رقم هاتف معرف المتصل الخاص بهم لجعل مكالماتهم الهاتفية تبدو وكأنها من رمز منطقتك المحلي أو من اسم موثوق به. لا يمكن الاعتماد على خدمة تعريف المتصل Caller ID هذه الأيام.
- سيستخدم بعض مجرمي الإنترنت أسماء وشعارات تبدو وكأنها مؤسسة خيرية حقيقية. هذا هو أحد الأسباب التي تدفع لإجراء بعض الأبحاث قبل التبرع.
- غالبًا ما يقدم مجرمو الإنترنت الكثير من الادعاءات الغامضة والعاطفية حول ما سيفعلونه بأموالك ولكنهم لا يقدمون تفاصيل حول كيفية استخدام تبرعك.
- لا تفترض أن طلبات المساعدة على مواقع التمويل الجماعي مثل GoFundMe أو مواقع التواصل الاجتماعي مثل TikTok مشروعة، لا سيما في أعقاب أزمة أو مأساة.
- قد يحاول بعض مجرمي الإنترنت خداعك للتبرع لهم بشكرك على تبرع قدمته في الماضي بينما لم تتبرع لهم أبدًا في الواقع.
- لا تعط معلومات شخصية أو مالية ردًا على أي طلب غير مرغوب فيه.

كيف تصنع الفرق بأمان

للتبرع في أوقات الحاجة أو لمساعدة المتضررين من كارثة، تبرع فقط لمنظمات معروفة وموثوقة. أنت من ستبدأ الاتصالات وتقرر من الذي يمكنك الوصول إليه، مثل مواقع الويب التي يجب زيارتها أو المنظمات التي يجب الاتصال بها. عندما تفكر في التبرع لمؤسسة خيرية، ابحث عن اسمها بالإضافة إلى كلمات مثل "شكوى" أو "مراجعة" أو "تقييم" أو "خداع". لست متأكدًا من المؤسسات الخيرية التي تثق بها؟ ابدأ بالبحث في مواقع الويب الحكومية التي تثق بها، أو ربما الروابط التي توفرها مؤسسة إخبارية معروفة وموثوقة للغاية. التبرع في أوقات الحاجة هو طريقة رائعة لإحداث فرق، فقط تأكد من أنك تعطي لمنظمات شرعية.

المحرّر الضيف

الدكتورة جيسيكا باركر هي زعيمة حائزة على جوائز في الجانب الإنساني للأمن. هي المدير التنفيذي المشارك لـ Cygenta والمؤلفة الأكثر مبيعًا. جيسيكا عضو في المجلس الاستشاري لقمة SANS للتوعية الأمنية.

الموارد

FTC لمنع الاحتيال: https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
الهندسة الاجتماعية: https://www.sans.org/newsletters/ouch/social-engineering-attacks
أهم ثلاث عمليات احتيال: https://www.sans.org/newsletters/ouch/top-three-social-media-scams
هجمات المراسلة: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
التصيّد - هجمات المكالمات الهاتفية الاحتيالي: https://www.sans.org/newsletters/ouch/vishing
البحث عن التبرعات: https://www.charitynavigator.org

ترجمها للعربية: محمد سرور، فؤاد أبو عويمر، جهاد أبو نعمة، اسلام الكرد