خِدَاعك عبر وسائل التواصل الاجتماعي

نظرة عامة

لا شك بأن الكثير منا تلقى هجمات تصيُد عبر البريد الإلكتروني، سواء في العمل أو في المنزل. رسائل البريد الإلكتروني هذه عادة ما تبدو أصلية أو شرعية، كما هو الحال من البنك الذي تتعامل معه أو رئيسك في العمل أو متجرك المفضل على الإنترنت. ومع ذلك، فهي في الحقيقة هجوم في محاولة لدفعك أو خداعك لاتخاذ إجراء لا يجب عليك اتخاذه، مثل فتح مرفق البريد الإلكتروني المصاب أو مشاركة كلمة المرور أو تحويل الأموال. التحدي هو أنه كلما أصبحنا أكثر ذكاءً في اكتشاف هذه الهجمات عبر البريد الإلكتروني وإيقافها، كلما حاول مجرموا الإنترنت ابتكار طرق أخرى للاتصال بالأشخاص وخداعهم.

يمكن أن تحدث محاولات الخداع عبر أي نوع من تطبيقات التواصل تقريبًا، من WhatsApp , Skype و Slack إلى Twitter أو Facebook أو Snapchat أو Instagram أو حتى تطبيقات الألعاب. فقد يكون التواصل عبر هذه المنصات أو القنوات أكثر رسمية أو جدارة بالثقة، وهذا هو بالضبط السبب وراء استخدام المهاجمين لها لخداع الآخرين. بالإضافة إلى ذلك، مع هذه التقنيات الحديثة اليوم، أصبح من السهل على أي مهاجم في أي مكان في العالم التظاهر بأنه أي شيء أو أي شخص يريده. لذا بات من المهم أن تتذكر أن أي محاولة للاتصال تأتيك مصادفة، قد لا تكون كما تبدو، كما وأن المتصلين بك ليسوا دائمًا كما يبدون عليه.

تنبيهات أساسية

فيما يلي سنسرد القرائن الأكثر شيوعًا والتي ربما تنطبق على رسالة تلقيتها للتو أو منشوراً ما قرأته ومن المحتمل أن يكون هجوماً.

النقاط الرئيسية

الإلحاح: رسالة ذات ميل بالإلحاح تتطلب «إجراءً فوريًا» قبل حدوث شيء سيء، مثل التهديد بإغلاق حساب أو إرسالك إلى السجن. يهدف المهاجم هنا ايقاعك بالتسرع لارتكاب خطأ.

الضغط: الضغط عليك لتجاوز أو تجاهل السياسات أو الإجراءات في العمل.

الفضول: شعور قوي بالفضول أو بشيء جميل أو جيد جدًا من الصعب تصديقه. لاء لم تفز باليانصيب.

الخطورة: ويكون على شكل طلب للحصول أو الافصاح عن معلومات شديدة الحساسية، مثل رقم بطاقة الائتمان أو كلمة المرور الخاصة بك، أو أي معلومات لا يمكنك مشاركتها بسهولة.

الرسائل الرسمية: بحيث يدَّعي مرسل الرسالة أنها تأتي من مؤسسة رسمية، ولكنك ستلاحظ احتواءها على أساليب وقواعد نحوية أو هجائية ضعيفة. لن تستخدم معظم المؤسسات الحكومية وسائل التواصل الاجتماعي لإجراء اتصالات رسمية مباشرة معك. إذا لم تكن متأكدًا مما إذا كانت الرسالة شرعية، فاتصل بالمؤسسة مرة أخرى ولكن استخدم رقم هاتف موثوق به، مثل رقم من موقعه على الويب.

انتحال الهوية: بحيث تتلقى رسالة من صديق أو زميل في العمل، لكن الصوت أو طريقة الصياغة لا تشبهه. إذا كنت مرتابًا، فاتصل بالمرسل على الهاتف للتحقق من أنه أرسل تلك الرسالة. فمن السهل على المهاجم الإلكتروني إنشاء رسائل يبدو منها أنها من شخص تعرفه. في بعض الحالات، يمكنهم الاستيلاء على حساب أحد أصدقائك، ثم يتظاهر بأنه صديقك ويتواصل معك. كن على دراية خاصة بالرسائل النصية، وتويتر وغيرها من تنسيقات الرسائل القصيرة، فالأمر عادة ما يكون أصعب بكثير من ناحية التعرف على شخصية المرسل من خلالها.

أنت دوماً أفضل دفاع ضد تلك الحيل والخدع والهجمات. إذا بدت لك الرسالة غريبة أو مشبوهة، فما عليك سوى تجاهلها أو حذفها أو إذا كانت من شخص تعرفه شخصيًا، فاتصل بالشخص الموجود على الهاتف لتأكيد ما إذا كان قد أرسلها بالفعل.

الضيف المحرر

الدكتورة جيسيكا باركر (@drjessicabarker) هي شخصية قيادية في الجانب الإنساني لأمن المعلومات. وهي المدير التنفيذي المشارك لشركة Cygenta ، حيث تتابع شغفها للتأثير بشكل إيجابي على الوعي بأمن المعلومات والسلوكيات وثقافة الحماية في جميع أنحاء العالم. وهي رئيسة ClubCISO ومتحدثة رئيسية معروفة.

مصادر إضافية

Social Engineering: https://www.sans.org/u/Uz6
Phone Call Scams: https://www.sans.org/u/Uzb
Stop That Phish: https://www.sans.org/u/Uzg
Personalized Scams: https://www.sans.org/u/Uzl