OUCH! تموز (يوليو)، 2022
SANS SECURITY AWARENESS
نشرة الوعي الأمني الإخبارية الشهرية للجميع

هجمات التصيد تزداد تعقيدًا

أصبحت هجمات التصيد الاحتيالي الطريقة الأكثر شيوعًا التي يستخدمها المهاجمون عبر الإنترنت لاستهداف الأشخاص في العمل والمنزل. لطالما كانت هجمات التصيد عبارة عن رسائل بريد إلكتروني يرسلها مهاجمون عبر الانترنت لخداعك للقيام بشيء لا يجب عليك فعله، مثل فتح مرفق بريد إلكتروني مصاب أو النقر فوق ارتباط ضار أو مشاركة كلمة مرورك. بينما تستمر هجمات التصيد التقليدية اليوم، يقوم العديد من المهاجمين الإلكترونيين بإنشاء رسائل بريد إلكتروني متقدمة للتصيد الاحتيالي تكون أكثر تخصيصًا ويصعب اكتشافها. كما أنهم يستخدمون تقنيات مثل الرسائل النصية أو وسائل التواصل الاجتماعي أو حتى المكالمات الهاتفية للتفاعل معك وخداعك. إليك أحدث حيلهم وكيف يمكنك اكتشافها.

يقوم المهاجمون الإلكترونيون بإجراء أبحاثهم

اعتادت رسائل التصيد الاحتيالي الإلكترونية أن يكون من السهل اكتشافها لأنها كانت رسائل عامة تم إرسالها إلى ملايين الأشخاص العشوائيين. لم يكن لدى المهاجمين عبر الإنترنت أي فكرة عمن سيقع ضحية ؛ لقد عرفوا فقط أنه كلما زاد عدد رسائل البريد الإلكتروني التي أرسلوها، زاد عدد الأشخاص الذين يمكنهم خداعهم. يمكننا في كثير من الأحيان اكتشاف هذه الهجمات الأبسط من خلال البحث عن رسائل بريد إلكتروني غريبة تتضمن "عزيزي العميل" في البداية ، أو أخطاء إملائية ، أو رسائل كانت جيدة جدًا لدرجة يصعب تصديقها، مثل الأمراء النيجيريين الذين يعرضون عليك ملايين الدولارات.

المهاجمون الإلكترونيون اليوم أكثر تعقيدًا بكثير. إنهم الآن يبحثون عن ضحاياهم المقصودين لإنشاء هجوم أكثر تخصيصًا. بدلاً من إرسال بريد إلكتروني للتصيد الاحتيالي إلى خمسة ملايين شخص، أو الظهور على أنها رسائل بريد إلكتروني عامة مرسلة من قبل الشركات، قد يرسلونها إلى خمسة أشخاص فقط ويصممون الهجوم بحيث يبدو أنه مُرسَل من شخص نعرفه. يقوم المهاجمون عبر الإنترنت بهذا من خلال:

- البحث في ملفات تعريف LinkedIn الخاصة بنا، أو ما ننشره على وسائل التواصل الاجتماعي، أو باستخدام المعلومات المتاحة للجمهور أو الموجودة على Dark Web.
- صياغة الرسائل التي يبدو أنها واردة من الإدارة أو زملاء العمل أو البائعين الذين تعرفهم وتعمل معهم.
- تعلم ما هي هواياتك وإرسال رسالة لك تتظاهر بأنك شخص يشاركك مصلحة مشتركة.
- تحديد أنك حضرت مؤتمرًا مؤخرًا أو عدت للتو من رحلة ثم صياغة بريد إلكتروني يشير إلى رحلاتك.

يستخدم المهاجمون السيبرانيون بنشاط طرقًا أخرى لإرسال نفس الرسائل، مثل إرسال الرسائل النصية إليك أو حتى الاتصال بك مباشرةً عبر الهاتف.

كيفية الكشف عن هجمات التصيد الأكثر تقدمًا

نظرًا لأن المهاجمين عبر الإنترنت يأخذون وقتهم ويبحثون عن ضحاياهم المقصودين، فقد يكون من الصعب اكتشاف هذه الهجمات. والخبر السار هو أنه لا يزال بإمكانك اكتشافهم إذا كنت تعرف ما تبحث عنه. اطرح على نفسك الأسئلة التالية قبل اتخاذ إجراء بشأن رسالة مشبوهة:

1. هل تخلق الرسالة إحساسًا متزايدًا بالإلحاح؟ هل تتعرض لضغوط لتجاوز السياسات الأمنية لمؤسستك؟ يحاول المهاجمون دفعك لارتكاب خطأ. كلما زاد الشعور بالإلحاح، زاد احتمال وقوع هجوم.

2. هل البريد الإلكتروني أو الرسالة منطقية؟ هل سيُرسل الرئيس التنفيذي لشركتك رسالة نصية على وجه السرعة تطلب فيها المساعدة؟ هل يحتاج مشرفك حقًا إلى التسرع وشراء بطاقات الهدايا؟ لماذا قد يطلب مصرفك أو شركة بطاقة الائتمان التي تتعامل معها معلومات شخصية يجب أن تكون بحوزتهم من قبل؟ إذا بدت الرسالة غريبة أو في غير محلها، فقد تكون هجومًا.
3. هل تتلقى بريدًا إلكترونيًا متعلقًا بالعمل من زميل عمل موثوق به أو ربما مشرفك، لكن البريد الإلكتروني يستخدم عنوان بريد إلكتروني شخصي مثل @gmail.com؟
4. هل تلقيت بريدًا إلكترونيًا أو رسالة من شخص تعرفه، لكن الصياغة أو نبرة الصوت أو التوقيع في الرسالة خاطئة وغير عادية؟

إذا بدت الرسالة غريبة أو مشبوهة، فقد تكون هجومًا. إذا كنت تريد تأكيد ما إذا كانت رسالة بريد إلكتروني أو رسالة شرعية، فإن أحد الخيارات هو الاتصال بالفرد أو المؤسسة التي ترسل لك رسالة برقم هاتف موثوق به.

أنت أفضل دفاع إلى حد بعيد. استخدام الحس السليم.

المحرّر الضيف

فيل هوفمان هو مستشار شبه متقاعد في مجال تكنولوجيا المعلومات يتمتع بخبرة 40 عامًا، مع التركيز على البنية التحتية والأمن. إنه مساهم ومحرر على المدى الطويل لـ OUCH! وهو متحمس للتكنولوجيا وركوب الدراجات والتصوير الفوتوغرافي.

الموارد

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
المعلومات الاستخبارية مفتوحة المصدر: https://www.sans.org/security-awareness-training/resources/search-yourself-online

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