

OUCH!

نشرة الوعي الأمني الإخبارية الشهرية للجميع

أفضل ثلاث عمليات احتيال على وسائل التواصل الاجتماعي

نظرة عامة

في حين أنّ وسائل التواصل الاجتماعي هي طريقة رائعة للتواصل والمشاركة والمتعة مع الآخرين، إلا أنها أيضاً طريقة منخفضة التكلفة لمجرمي الإنترنت لخداع ملايين الأشخاص والاستفادة منهم. لا تقع ضحية لعمليات الاحتيال الثلاثة الأكثر شيوعاً على وسائل التواصل الاجتماعي.

عمليات الاحتيال الاستثمارية

هل سبق لك أن رأيت منشوراً حول فرصة استثمارية تعود عليك بعائد ضخم في فترة زمنية سريعة للغاية مع مخاطر قليلة أو معدومة؟ في الحقيقة أن هذه الضمانات هي حيل استثمارية. بكل سهولة يسرق المحتالون أموالك بعد ايداعها لديهم. غالباً ما تتضمن عمليات الاحتيال هذه إعلانات أو قصص نجاح من عملاء سابقين للترويج للاستثمارات، ولكن هذه مجرد شهادات مزيفة لزيادة ثقتك. غالباً ما تكون عمليات الاحتيال الاستثمارية هذه حول الاستثمار في العملات المشفرة أو العقارات، وغالباً ما يتم الدفع بالعملات المشفرة أو من خلال طرق دفع أخرى غير معتمدة ومتعارف عليها. إذا كان الاستثمار يبدو جيداً جداً بحيث لا يمكن تصديقه، فمن المرجح أن يكون خدعة. تذكر أنه لا يوجد شيء اسمه استثمارات مضمونة وعالية العائد. استثمر أموالك فقط في موارد موثوقة ومعروفة، وليس لدى الغرباء الذين تقابلهم عبر الإنترنت الذين يعرضون مخططاً سريعاً للثراء.

عمليات الاحتيال الرومانسية

عندما يُطوّر المجرمون علاقة عبر الإنترنت مع شخص معين يبدو عليه أنه وحيد أو ضعيف يمكن خداعه للحصول على المال، يعرف هذا باسم عملية احتيال الرومانسية حيث يستخدم المجرم أي تكتيكات ممكنة لبناء الثقة، بما في ذلك تبادل الصور المزيفة أو إرسال الهدايا، ثم يشارك قصة مأساوية حول الحاجة إلى المال لدفع النفقات مثل فواتير المستشفى أو تكاليف السفر لزيارة الضحية شخصياً. لتجنب اللقاء مع الشخص بشكل حقيقي، قد يقول هؤلاء المجرمون إنهم يعملون في صناعة تمنعهم من القيام بذلك، مثل البناء أو الطب الدولي أو الجيش. غالباً ما يطلبون المال كتحويل مصرفي أو بطاقات هدايا للحصول على النقد بسرعة والبقاء مجهولي الهوية. هذه الأنواع من عمليات الاحتيال ليست شائعة فقط على وسائل التواصل الاجتماعي وإنما أيضاً على تطبيقات المواعدة عبر الإنترنت. كن حذراً مع الأشخاص الذين تقابلهم عبر الإنترنت، وخذ الأمور ببطء، ولا ترسل الأموال أبداً إلى شخص تواصلت معه فقط عبر الإنترنت.

بالإضافة إلى ذلك، إذا كنت تعتقد أن شخصاً تعرفه قد يكون عرضة لمثل هذا الهجوم أو في علاقة عبر الإنترنت ترفع هذه الأعلام، فقدم له المساعدة. في بعض الأحيان قد يكون من الصعب جداً على شخص منخرط في اتصال عاطفي أن يرى مدى خطورة الموقف.

عمليات الاحتيال في التسوق عبر الانترنت

تحدث عمليات الاحتيال للتسوق عبر الإنترنت عند شراء أشياء عبر الإنترنت بأسعار لاتصدق ومنخفضة للغاية ولكنك لا تستلم هذه المنتجات أبداً. ستروّج الإعلانات المغرية على وسائل التواصل الاجتماعي لأسعار لا تصدق وتحتوي على روابط تنقلك إلى مواقع تبدو مشروعة وتبيع علامات تجارية معروفة، لكن هذه المواقع غالباً ما تكون مزيفة. كن حذراً من مواقع الويب التي لا تحتوي على معلومات اتصال أو تحوي معلومات اتصال مزيفة أو تستخدم عناوين بريد إلكتروني شخصية. اكتب اسم المتجر عبر الإنترنت أو عنوان الويب الخاص به في محرك بحث لترى ما قاله الآخرون عنه. ابحث عن مصطلحات مثل "احتيال" و "خداع" و "لن يحدث ذلك مرة أخرى" و "مزيف". كن حذراً جداً من العروض الترويجية أو الصفقات عبر الإنترنت التي تبدو جيدة جداً بحيث لا يمكن تصديقها. من الآمن لك شراء هذه العناصر مع تكلفة أكثر بقليل . ولكن من مواقع موثوقة استخدمتها من قبل أنت أو أحد اصدقائك.

والخبر السار هو : أنت أفضل دفاع عن نفسك. أنت المسيطر. فقط كن في حالة تأهب لمثل هذه الحيل وستتمكن من تحقيق أقصى استفادة من وسائل التواصل الاجتماعي بأمن وأمان.



المحرّر الضيف

كريس البيج (@chriselgee) مكتشف ثغرات أمنية لدى @CounterHackSec، ويعمل في الجيش الوطني ومدرس معتمد لدي SANS إنه يستمتع بالتعرف على التفاصيل الفنية الجريئة، وبناءها في فهم تنظيمي أكبر، ومشاركتها مع الطلاب والعملاء.

الموارد

<https://www.bbb.org/ScamTracker> : Better Business Bureau Scam Tracker
<https://www.sans.org/newsletters/ouch/social-engineering-attacks> : الهندسة الاجتماعية
<https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21> : تسوق اونلاين بأمان
<https://www.sans.org/newsletters/ouch/vishing> : هجمات المكالمات الهاتفية الاحتيالي

ترجمها للعربية: محمد سرور، فؤاد أبو عويمر، جهاد أبو منذر، اسلام الكردي

IOUCH نُشر! OUCH من قبل فريق الوعي الأمني في SANS وتُوزع بموجب الرخصة [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) . لك الحرية في المشاركة أو توزيع هذه النشرة الإخبارية شرط عدم تعديلها أو بيعها. الفريق التحريري: والت سكرينغنس، فل هوفمان، ألان واغونر، ليزلي ريدأوت، برينسيس يونغ.