SANS SECURITY AWARENESS

OUCH!

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

لا تكن فريسة سهلة

مقدمة

تعد خدمات البريد الالكتروني والمراسلة متل (السكايب, تويتر والسناب شات) احدى الطرق الرئيسية التي نتواصل بها . نحن لا نستخدم هذه التقنيات كل يوم من اجل العمل فقط ولكن ايضا من اجل البقاء على اتصال مع الاصدقاء وافراد العائلة. نظرا لاعتماد الناس من كافة انحاء العالم على هذه التقنيات ..فقد اصبحت من اهم وسائل الهجوم التي يستخدمها المخترقون عبر الانترنت. في هذا العدد سوف نتعرف على التصيد وكيفية معرفة هذه الهجمات وايقافها سواء كنت بالعمل او المنزل.

ما هو التصيد

التصيد هو نوع من الهجمات الالكترونية التي تستخدم البريد الالكتروني والرسائل النصية من اجل خداعك وجعلك تتخذ اجراء لا يجب عليك اتخاذه .مثل النقر على رابط ضار ومشاركة كلمة مرورك او فتح مرفق بريد الكتروني مصاب. يعمل المهاجمون بجد من اجل جعل هذه الرسائل مقنعة وتحرك مشاعرك العاطفية لديك كالاستعجال والفضول . انهم يجعلون هذه الرسائل الالكترونية تبدو وكأنها من شخص او شيء ما تعرفه مثلا من صديق او شركة تتعامل معها كثيرا. وربما من الممكن اضافة شعار البنك الذي تتعامل معه او تزييف بريد الكتروني بحيث تبدو الرسالة أكثر شرعية. يرسل المهاجمون هذه الرسالة الى ملايين من الناس. فهم لا يعرفون من سيأخذ الطعم كل ما يعرفونه ان أحد ما سوف يقع ضحية لهم.

حماية نفسك

في جميع الحالات تقريبا يكون فتح رسائل البريد الالكتروني وقراءتها امرا جيدا. ولكن في حالة هجوم التصيد حيث يتم خداعك لعمل شيء ما. فهنا لحسن الحظ يوجد ادلة على ان هذه الرسالة تمثل هجوم والتالي سوف نوضح لك الحالات الاكثر شيوعا لحمايتك:

- احساس كبير بالإلحاح حيث يطالبك بعمل فوري قبل حدث شيء سيء مثل التهديد بإغلاق حسابك هنا يريد المهاجم ان يجبرك على ارتكاب خطأ.
- الضغط عليك لتجاوز وتجاهل سياستك واجراءاتك بالعمل.
- احساس قوي بالفضول مثل ابلاغك أنك فزت باليانصيب أو بجائزة مالية كبيرة جدا.

- تحية عامة متل «عزيزي العميل» حيث ان جميع الاصدقاء والشركات التي تتعامل معها تعرف اسمك.
- طلب معلومات شديدة الحساسية متل بطاقة الائتمان او كلمة المرور او اي معلومات اخرى يجب على المرسل الشرعي معرفتها.
- تشير الرسالة ان مصدرها منظمة رسمية ولكنها تحتوي على اخطاء نحوية وتهجئة ضعيفة. او تكون على هيئة بريد الكتروني شخصي @gmail.com
- تأتي الرسالة من بريد الكتروني رسمي متل « مديرك بالعمل » ولكنها تحتوي على عنوان «الرد إلى » ينتقل الى حساب بريد الكتروني شخصي لشخص ما.
- تتلقى رسالة من شخص تعرفه، لكن الاسلوب أو الصياغة لا يبدو مثله. إذا كنت مرتابا من الامر، فاتصل بالمرسل لتتحقق من أنه أرسلها. حيث انه من السهل أن يقوم المهاجم الإلكتروني بإنشاء رسالة تبدو أنها من صديق أو زميل عمل.

في نهاية المطاف فان الحس السليم يعتبر أفضل وسيلة للدفاع. حيث ان الرسالة الالكترونية إذا كانت غريبة او مشبوهة او جيدة لدرجة يصعب تصديقها. فهي على الغالب تكون هجوم تصيد.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة و المتخصصين في أمن المعلومات.

الضيف المحرر

تونيا ديدلي **Tonia Dudley** تعمل في مجال تطوير وتقديم برامج التوعية بأمن المعلومات منذ عام 2011. منها بناء أفضل برنامج للتوعية بمخاطر التصيد. يمكنك متابعتها على www.linkedin.com/in/toniadudley

مصادر إضافية

الهندسة الاجتماعية: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_aa.pdf

ساعد من حولك لحماية أنفسهم: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201710_aa.pdf

البريد الالكتروني: ما يفعل وما يترك: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201609_aa.pdf

حيلة الرئيس التنفيذي: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201607_aa.pdf

رخصة