ملاحظات:
الهندسة الاجتماعية على فيسبوك

التصيّد (phishing) هو استخدام موقع إلكتروني أو بريدٍ وهمي يبدو حقيقياً لخداعِ مستخدمي الإنترنت وتشجيعهم على التفاعلِ مع محتواه. كونكم صحفيون وناشطون إعلاميون، فإنكم تتعاملون مع معلومات حساسة. تشكل هجمات التصيد 91% من الهجمات الموجهة، كونها أسرع الطرق وأكثرها سهولة للوصول إلى معلوماتك وجهازك وشبكة اتصالاتك. من المهم تغييرُ عاداتك عندما يتعلق الأمر بوسائل التواصل الاجتماعي وتوخي الحذر عند التعامل مع الرسائل الواردة.

غالباً ما تستخدم هجمات كهذه لأخذ كلمات السر، أو البيانات المصرفية، أو السيطرة على الأجهزة، ويعد تثبيت برمجيات خبيثة على حاسب الضحية هدفاً مهماً، يمكن تحقيقه عبر:

- رابط يوصل الضحية إلى موقع يقوم بتثبيت البرمجية الخبيثة.
- ملف ملحق يقوم بتثبيت البرمجية الخبيثة عند فتحه.
- تحديثات مزيفة لبرامج الحاسب أو ملفات للتحميل تعرض الحاسب للخطر.
- يشكل كل من البريد الإلكتروني ووسائل التواصل الاجتماعي وسائط للهجمات من هذا النوع.

تجنب محاولات التصيد والتي قد تستخدم عدة سبل مثل:

- الجشع: كالحوافز المالية والوعود البراقة.
- العروض ذات الوقت المحدود أو تواريخ الانتهاء.
- الفضول: مثل "لا تفوتوا عليكم هذا" أو "المواد الممنوعة من العرض".
- الخوف: كالعواقب السلبية في حال عدم النقر.

توخ الحذر دوماً حول:

- إسلوب صياغة النص ومحتواه.
- تفاصيل حسابك – تجنب طلبات تسجيل الدخول لمواقع أخرى عبر رسالة بريد إلكتروني
- الروابط + الملحقات
- التطبيقات التي ترسل رسائل عشوائية
- الرسائل التي تصلك على بريدك بشكل عشوائي
- طلبات الصداقة من أشخاص غير معروفين.

آخر تحديث - كانون الثاني 2016