تَصَيُّد الانترنت (Phishing)

تصيد الانترنت (Phishing) هو عبارة عن أحد أشكال الهندسة الاجتماعية، والهندسة الاجتماعية (Social_Engineering) هي وسائل يلجأ إليها البعض بهدف خداع و تضليل الضحية و تحفيزه للكشف عن معلومات هامة لا يقوم بكشفها في الظروف العادية، كأن يقوم بالاتصال على أحد موظفي الشركة مدعياً كونه مدير الشركة و يطلب تزويده بمعلومات معينة يحق للمدير الاطلاع عليها. و أما مصطلح الـ Phishing فقد تم استخدامه ليعبر عن عملية الخداع الالكتروني التي تتم بتزييف المواقع أو البريد الالكتروني ومحاكاة مواقع وعناوين البريد للشركات أو الأفراد بهدف دفع المستخدمين الغير مدركين لزيفها إلى تزويدهم ببياناتهم الخاصة والتي قد تكون بيانات مالية أو شخصية أو أي بيانات أخري سرية. ربما يرسل المهاجم بريداً الكترونياً باسم أحد البنوك ويطالبك بتزويد البنك(المزيف) ببيانات بطاقة الائتمان الخاصة بك أو قد يقوم بتزوير موقع يشبه صفحة البريد الالكتروني الخاص بشركتك و يدفعك إلى تسجيل الدخول لبريدك من صفحته المزورة، وفي جميع الحالات فإن المزوِّر سيحصل على بياناتك السرية و بارادتك الكاملة.

كيف تتجنب وقوعك ضحية لهجمات الـ Phishing؟

1- تجنب الثقة العمياء و لا تفترض دائماً حسن النية من الأفراد الذين تربطك بهم علاقة عبر الانترنت أو من المواقع الالكترونية المجهولة الهوية، و إذا استقبلت بريداً الكترونياً من أحد

الأفراد باسم شركة معينة فحاول التأكد من هوية المرسل و لو عبر الاتصال مباشرةً مع الشركة.

2- لا تقم بكتابة أي معلومات هامة، سواءً شخصية أو خاصة بالعمل لأي شخص إلا بعد التأكد تماماً من كونه يحمل صلاحيات الاطلاع على هذه المعلومات.

3- لا ترسل بياناتك المالية أو الشخصية الهامة عبر البريد الالكتروني أو المحادثات الفورية، و لا تقم بالرد على رسائل البريد الالكتروني المجهولة المصدر، (مجرد الرد على هذه الرسائل يؤكد الوجود الفعلي لبريدك و قد تكون بذلك عرضةً لرسائل مزعجة أكثر في المستقبل)، كما لا تقم بتتبع روابط المواقع التي قد تكون مدرجة في مثل هذه الرسائل.

4- توخ الحذر في استخدام مواقعك المفضلة، و قم بالنظر دوماً إلى عنوان الموقع URL فقد يكون الموقع مطابقاً تماماً لموقعك المفضل، مع وجود اختلاف في العنوان وهذا الاختلاف قد يكون فقط في النطاق النهائي للموقع مثل net. أو com. أو org. أو info. أو غيرها.

5- عندما تستقبل رسالة بريد الكتروني و تشك في كونها مزيفة، قم بالبحث عنها في الانترنت حيث يوجد العديد من المواقع التي تقوم بتجميع و أرشفة هذه الرسائل.

6- غالباً ما تكون مواقع الPhishing مليئة بالفيروسات و ملفات التجسس و البرامج المخفية Trojans ولهذا فإن استخدام برنامج حماية قوي يحد من تأثير هذه المواقع و لكن لا يمنعها بشكل كامل.

7- قم باستخدام برامج الحماية ضد التصيد (Anti-Phishing) مثل McAfee SiteAdvisor أو أداة Phishing Filter ضمن بيئة الـ Internet Explorer أو ما يتوفر من البرامج المختلفة.

دائرة أمن المعلومات