أخطاء شائعة أثناء استخدام البريد الالكتروني

في هذه النشرة نستكمل استعراض مجموعة الأخطاء الشائعة التي يرتكبها مستخدمو البريد الالكتروني...

1- عدم اجراء النسخ الاحتياطي لمحتويات البريد الالكتروني

يتم استخدام البريد الالكتروني بشكل واسع في المراسلات والخطابات ما بين المؤسسات وموظفيها، كما يعتبر في كثير من الحالات بمثابة خطابات رسمية للمعاملات المالية والقرارات المصيرية، و نظراً للأهمية الكبيرة لهذه الخطابات والمراسلات، فإنه من المنطقي اعتبار محتوي البريد الالكتروني محتوى هام و القيام باجراء النسخ الاحتياطي لله حتى يتم الاحتفاظ بكافة المراسلات البريدية والعودة إليها وقت الحاجة، خاصةً عندما يكون الحجم المتاح للتخزين في البريد الالكتروني محدوداً، يوجد عدة وسائل لاجراء النسخ الاحتياطي و منها:

1) ارسال نسخة من البريد إلى بريد خاص من خلال حقل BCC
2) اجراء عملية أرشفة للبريد من خلال برامج إجارة البريد مثل برنامج Microsoft Outlook
3) القيام بالاحتفاظ بنسخ من البريد الالكتروني على القرص الصلب من خلال استخدام Save As من المتصفح

2- أخذ البريد العشوائي والمخادع بصورة جدية

يستخدم مرسلو البريد العشوائي العديد من الحيل التي تهدف لخداع المستخدمين وحثهم على ارسال بياناتهم أو الكشف عن كلمات المرور الخاصة بهم أو الاحتيال بهدف السرقة

وهو الأمر الغالب، و لكن بشكل عام يوجد مجموعة من الحيل المعروفة و منها ايهام المستخدم بالفوز بجائزة مالية ضخمة أو أن البيانات المالية في البنك بحاجة إلى تأكيد أو وجود تعديلات في نظام البريد الالكتروني والتي تتطلب ارسال كلمة المرور لجهة الارسال.

3- ارسال البيانات المالية أو الشخصية عبر البريد الالكتروني

تقوم كافة البنوك والمؤسسات العاملة بالأنظمة الالكترونية لتراسل البيانات بتوفير بيئة اتصال آمن ضمن مواقع الويب الخاصة بهم، و هذا الاتصال الآمن يهدف إلى حماية بيانات المستخدمين والحفاظ على سريتها و احباط أي محاولات للتلصص على هذه البيانات بأي وسيلة كانت، و أما سبب الاعتماد على هذه الصفحات الآمنة لتقل البيانات بدلاً من البريد الالكتروني فهو كونها أقل عرضة للهجمات والاحتيال من البريد، فالبيانات المرسلة عبر البريد الالكتروني يمكن الوصول إليها بطرق عديدة، منها:

1) محاولة اكتشاف كلمات المرور للمستخدمين
2) استخدام برامج المراقبة والتنصت على خطوط الانترنت
3) مزود البريد الالكتروني نفسه قد يقوم بالكشف عن محتوي البريد في حالات معينة

ولهذا السبب لا ينصح باستخدام البريد الالكتروني لارسال البيانات الهامة مطلقاً

4- إلغاء الاشتراك من قوائم بريدية لم تشترك فيها أصلاً

من الوسائل الشائعة التي يستخدمها مرسلو البريد العشوائي ارسال الآلاف من الرسائل المزيفة على عناوين عشوائية و تنسيقها هذه الرسائل على صورة رسائل اخبارية من مؤسسات خاصة، و أيضاً ادراج رابط لإلغاء الاشتراك من القائمة البريدية، و هذا الرابط

في حالات كثيرة يعتبر فخ للحصول على أكبر عدد من عناوين البريد الحقيقية والتي غالباً ما سيتم اغراقها بالكثير من رسائل البريد العشوائي المختلفة، ولهذا فعند استقبال أي بريد من هذا النوع وعدم تذكر الاشتراك في القائمة البريدية، فالأفضل تحديد عناوين البريد على أنها SPAMأو JUNK ليتم بعد ذلك حذفها بشكل آلي من مزود البريد نفسه.

5- الثقة في رسائل البريد المرسلة من "الأصدقاء"

أغلب مستخدمي الانترنت يتعاملون بحذر عند استقبال رسائل البريد من عناوين مجهولة، و لكن قلة من يتعامل بنفس الأسلوب مع الرسائل التي يتم استقبالها من العناوين المعروفة، فمستخدم البريد الالكتروني قد يعتبر أن رسالة بريد معينة آمنة فقط لأنه تمكن من التعرف على هوية المرسل، و لكن في كثير من الحالات قد يحتوي بريد الأصدقاء على نفس المخاطر التي يمكن مواجهتها عند استقبال أي نوع آخر من البريد المجهول المصدر. و أما سبب ذلك فهو أن بعض البرامج الخفية (Trojans) تقوم باستخدام أجهزة "الأصدقاء" وارسال رسائل عشوائية من خلال حساباتهم الشخصية والتي غالباً ما يقوم المستخدمون بعمل حفظ تلقائل لكلمات المرور.

6- تجاهل فحص كافة المرفقات من احتوائها على فيروسات الحاسوب

أكثر من 90٪ من الفيروسات التي تصيب أجهزة المستخدمين مصدرها الأساسي البريد الالكتروني و لهذا فمن الضروري جداً إعداد برامج مكافحة الفيروسات لتقوم بالفحص الآلي لكافة رسائل البريد الالكتروني والملفات المرفقة ليتم تقليل مخاطر وصول الفيرسات إلى أجهزة المستخدمين، الكثير من مزودي خدمات البريد الالكتروني مثل Gmail, Windows Live, Yahooيستخدمون برامج داخلية لتصفية رسائل البريد الالكتروني المرسلة والمستقبلة وفحصها من الفيروسات قبل الارسال، ولهذا فعند عدم

القدرة على توفير برامج للحماية من الفيروسات فمن الأفضل تصفح البريد مباشرةً من خلال الصفحات التي يقدمها مزودي البريد الالكتروني عبر الويب للاستفادة من برامج الفحص الداخلية، وأما عند اختيار تصفح البريد عبر برامج خارجية مثل Outlook فيجب تثبيت واستخدام برامج الحماية من الفيروسات

7- استخدام كلمات مرور سهلة للبريد الالكتروني

وهي من أكثر الأخطاء شيوعاً وانتشاراً، فمثل هذه الكلمات السهلة تشمل كلمات عامة مثل (اسم المدينة، اسم الدولة، اسم شخصية مشهورة، ...) أو كلمات شخصية مثل)الاسم، تاريخ الميلاد، الرقم الوطني، ...) أو أسوأ مثل استخدام ارقام متتالية أو حروف مكررة. عادةً ما يلجأ المخترقون الى استخدام برامج تقوم بفحص كافة كلمات المرور المتوقعة سواءً بتوظيف ائمة مسبقة بالكلمات المشهورة أو اجراء فحص لكافة الاحتمالات، وأما الوسيلة التي يمكن من خلالها الحماية من هذا النوع من الهجمات فهي استخدام كلمات مرور قوية، و بشكل عام فإن التالي يعتبر خصائص لكلمات المرور القوية:

1) طويلة (8 خانات على الأقل)
2) معقدة (تشمل على حروف + أرقام + رموز خاصة)
3) غير ذات علاقة باسم المستخدم الشخصي
4) ليست من الكلمات الشائعة الاستخدام