رسائل الإزعاج – Hoaxes & Spam

تعريف الـ Hoax

مصطلح الـ Hoax يُترجم حرفياً إلى "الكاذب" وهي تسمية دقيقة إلى حدٍ ما، حيث يطلق هذا المصطلح على البريد الالكتروني الذي ينشر أخباراً كاذبة ويطالب المستخدمين بنشرها، ويمكن أيضاً تعريفها بأنها نشر الاشاعات عبر البريد الالكتروني، وهي تختلف عن البريد المُخادع (Phishing) في كونها لا تطلب من المستخدمين زيارة مواقع خاصة وتزويدهم بمعلومات معينة، ولكنها في كثير من الأوقات يمكن أن تحمل أنواعاً جديدة من الفيروسات والتي تُنشر بحسن نية وبقصد المساعدة.

مخاطرها

تعتبر الرسائل الكاذبة (Hoaxes) مصدراً للازعاج، و بالاضافة إلى ذلك فإن كثيراً من هذه الرسائل تُسبب استهلاك موارد سيرفرات البريد الالكتروني حيث تبطئ الأداء العام للسيرفر بكونها ترسل إلى مجموعة كبيرة من الأفراد والذين غالباً ما يقومون بارسالها بدورهم، كما تقوم بعض هذه الرسائل بحث المستخدمين على حذف بعض الملفات الهامة في أجهزتهم كوسيلة لتحسين الأداء أو زيادة الأمان وهو ما قد يؤدي إلى تلف نظام التشغيل في حال التعاطي الايجابي مع مثل هذه الرسائل.

وزيادةً عما سبق، فإن احتواء كثير من الرسائل الكاذبة على تحذيرات من فيروسات (كاذبة) معينة يؤدي في النهاية إلى جعل المستخدم يتجاهل كافة التحذيرات عن الفيروسات الجديدة والتي قد يمكن أن تكون حقيقية في حالات قليلة جداً. وعلاوةً على ذلك فإن بعض هذه الرسائل تكون بهدف جمع أكبر عدد ممكن من عناوين البريد الالكتروني حتى يتم استخدامها لنشر المواد الاعلانية أو غيرها.

التعرف على الرسائل الكاذبة

يوجد بعض الاشارات العامة التي يمكن أن تكون مؤشراً على كذب هذه الرسائل ومنها:

- مطالبة المستخدم بتمرير البريد الالكتروني إلى كل من يعرفهم.

- وجود بعض الادعاءات في البريد ولكن بدون دليل داعم أو قد تكون مدعمة بأدلة مزيفة وغير حقيقية.
- استخدام لغة تقنية متخصصة في الرسالة بصورة توحي بالأهمية و تكون مبهمة في نفس الوقت.
- الاعتماد على مصداقية جهات خارجية لنشر أخبار باسمها، كأن يذكر أن الخبر ورد على شبكة CNN دون ارفاق رابط للخبر أو دليل عليه.
- الايحاء بالأهمية القصوى وضرورة الرد السريع.

تحتوي الرسائل الكاذبة (Hoaxes) بشكل عام على أمرين، الأول تهديد والثاني طلب، يهدف التهديد إلى جذب انتباه المستخدم ودفعة لاتمام القراءة وعادةً ما يكون التهديد متعلقاً بحماية الحاسوب من الاختراق أو من الفيروسات أو من منتجات لشركات معينة، وأما الطلب فقد يكون للمستخدم ليقوم بنشر هذا البريد وتعميمه وقد يكون عبارة عن مطالبة المستخدم بالقيام باجراءات معينة كحذف برنامج أو تثبيت برنامج أو حتى مقاطعة منتج معين، والتي تكون لأسباب تجارية أولاً وقد تكون في حالات معينة لأسباب حقيقية.

كيفية التعامل مع الرسائل الكاذبة

- لا تقم بتمرير أي رسالة إلا بعد التأكد من صحة المعلومات التي تحتويها، فإن كان الموضوع عن فتوى معينة يمكن مراجعة المواقع الاسلامية المختصة، وإن كان الموضوع عن حديث عن الرسول (صلى الله عليه وسلم) فيمكن مراجعة المواقع المختصة بالحديث، وإن كان الموضوع عن خبر معين يمكن مراجعة المواقع الاخبارية المتخصصة.
- عند احتواءها على تحذير من فيروسات أو أي مشاكل تقنية أخري، يمكن البحث باستخدام نص الرسالة نفسها أو يمكن مراجعة المواقع المتخصصة بذلك مثل:
  - McAfee:
    - http://vil.mcafee.com/hoax.asp
  - Symantec:
    - http://www.symantec.com/enterprise/security_response/threatexplorer/risks/hoaxes.jsp

البريد العشوائي (SPAM)

البريد العشوائي أو الـ Spam هو عبارة عن البريد الالكتروني الذي يحتوي على مواد إعلانية عن منتجات معينة أو عن يسوق لخدمات ما. هذا البريد هو من النوع الذي لا يرغب أي شخص باستقباله، وعادةً ما يقوم مرسلو هذا البريد أو الـSpammers بتجميع اعداد كبيرة من عناوين البريد الالكتروني عبر مجموعات الحوار أو عبر ارسال بريد كاذب Hoax كما سبق وأن ذُكر، أو حتى يقومون باستخدام برامج خاصة بتجميع البريد الالكتروني الذي يتم نشره على المواقع المختلفة وهذه البرامج تقوم بفحص الموقع المدخل وعندما تجد أي نص على الصيغة xx@xx.xxx تقوم مباشرةً باعتباره عنوان بريد الكتروني وتقوم بتسجيله في قاعدة بيانات خاصة بذلك.

وأما أساليب التعامل مع هذا النوع من البريد فمنها:

- عدم الاشتراك في أي مجموعة بريدية المجهولة أو العشوائية.
- الحذر من كتابة البريد الالكتروني في المواقع التي تطلب ادخال البريد اجبارياً لتصفح محتوى معين،
  - يمكن أولاً ادخال بريد عشوائي لمعرفة آلية تعامل الموقع مع البريد المدخل.
- عدم الرد بأي حال على أي رسالة من هذا النوع، لأن هذا الرد يثبت فعالية البريد وبالتالي يصبح هدفاً لمزيد من البريد العشوائي.
- استخدام بريد الكتروني يحتوي على خاصية فلترة البريد العشوائي
  - معظم مزودي خدمات البريد المجاني يوفرون هذه الخدمة.

دائرة أمن المعلومات