جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

الإيميلات المزيفة

البريد الالكتروني او "الايميل" احدى وسائل التواصل الاجتماعي الأكثر شيوعا. نظرا لاهمتيها في شتى مجالات العمل والحياة الشخصية وغيرها, أدى ذلك الى توسع شريحة مستخدميها من جميع الاعمار والخلفيات. لكن ما يغفل عنه اكثرهم ان البريدالالكتروني هو أيضا احدى اشهر وسائل ارتكاب الجرائم الالكترونية. التي بدورها تسبب العديد من الاضرار للمستخدمين كسرقةالهوية والمعلومات الحساسة وما الى ذلك. كل هذا واكثر ينم عن ما يعرف "بالايميلات المزيفة".

ماهي الإيميلات المزيفة؟

ان "الايميلات المزيفة" هي ناتج عن ضعف امن معظم أنظمة البريد الالكتروني. وهي رسائل وهمية او مزيفة تهدف الى خداع المستخدم ليشارك معلومات حساسة كرقم الهوية الوطنية او معلومات البطاقة البنكية, او حتى اختراق جهاز المستخدم لسرقة ملفات والعديد من الأمور الضارة التي قد يؤدي تلفها الى العديد من الخسائر المادية والمعنوية, لذلك وجب اخذ الحيطة والحذر بزيادة الوعي لاكتشاف هذه الايميلات الخبيثة.

طرق اكتشاف الإيميلات الخبيثة:

١ التحقق من المرسلً في بعض الحالات يكون العنوان المرسل منه مشابه لما يبدوا موثوقا، ولكن هناك اختلاف بسيط في الإملاء.

٢ الأخطاء الإملائية والنحوية ليس من الوارد تكرار الأخطاء الإملائية واللغوية من شركات معروفة، فوجودها بكثرة يشير إلى خطرمحتمل.

٣ احتوائها على روابط أو مرفقات إذا كانت هذه الروابط تطلب معلومات شخصية من غيرُ مبرر واضح، فهي بالغالب تؤدي إلى سرقةالمعلومات الشخصية، وكذلك المرفقات الُ مطاِلبة بالمعلومات الشخصية.

٤ عنوان إيميل تهديدي هناك بعض الصيغ التي قد تدل على أن للُ مرِسل نوايا خبيثة، مثلاً: "ا حذر: سيتم إغلاق حسابك"، "الإجراءالعاجل المطلوب"".

جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

الإيميلات المزيفة

ماذا تفعل إذا تم اختراق البريد الإلكتروني الخاص بك؟

١ المسارعة في تغيير كلمة السر تغيير كلمة السر يمكنك من طرد المتسللين إلى حسابك

٢ المسارعة بإلغاء الربط بالحسابات الأخرى يكون ذلك عبر تغيير بريدك الإلكتروني المستخدم لحساباتك الأخرى

٣ أبلغ جميع جهات اتصالك بذلك تحميهم من خطر النقر على المرفقات من الرسائل الواردة منك دون علمك

٤ قم بإعادة تثبيت نظام التشغيل الخاص بجهازك يهدف ذلك إلى التخلص من البرمجيات الخبيثة المثبتة على جهازك.

٥ قم بإبلاغ قسم تكنولوجيا المعلومات في عملك يكون ذلك لأخذ الإجراءات اللازمة للتخلص من الخطر

طرق الوقاية من الايميلات المزيفة:

١ النسخ الاحتياطي للمستندات عند نسخ مستندانتك الهامة وحفظها في مكان امن, يمكنك ذلك من استردادها في أي وقت ممكن.

٢ التحديث الدوري لانظمة التشغيل. عند طلب جهازك لتحديث نسخة جديدة من نظام التشغيل, سارع بالحصول عليه. فأنه غالبا مايتضمن تطوير وتقوية لامان وسرية معلوماتك المحفوظة في الجهاز.

٣ تنزيل نظام حماية وامن. قد تباع هذه الأنظمة منفصلة والهدف منها هو حماية الاحهزة من أي اختراق يهدد تسريب معلوماتك.

عمل الطالبات:
الاء باحبيل، لينا العلي، لينا الدريهم

المصادر:

https://shortest.link/3gKH
https://www.optiv.com/insights/discover/blog/22-ways-protect-yourself-against-phishing- attac