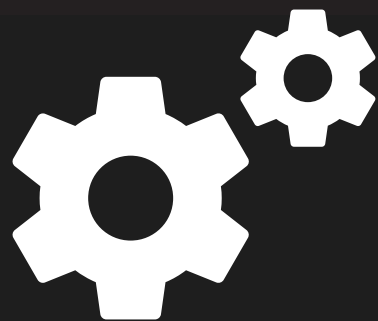




جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY



الإيميلات المزيفة

البريد الإلكتروني أو "الايمل" إحدى وسائل التواصل الاجتماعي الأكثر شيوعاً. نظراً لأهميتها في شتى مجالات العمل والحياة الشخصية وغيرها، أدى ذلك إلى توسع شريحة مستخدميها من جميع الأعمار والخلفيات. لكن ما يغفل عنه أكثرهم أن البريد الإلكتروني هو أيضاً إحدى أشهر وسائل ارتكاب الجرائم الإلكترونية. التي بدورها تسبب العديد من الأضرار للمستخدمين كسرقة الهوية والمعلومات الحساسة وما إلى ذلك. كل هذا وأكثر ينم عن ما يعرف "بالإيميلات المزيفة".

ماهي الإيميلات المزيفة؟

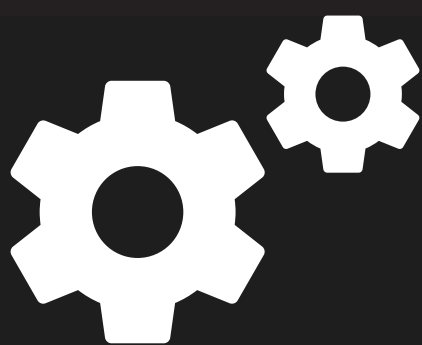
إن "الإيميلات المزيفة" هي ناتج عن ضعف أمن معظم أنظمة البريد الإلكتروني. وهي رسائل وهمية أو مزيفة تهدف إلى خداع المستخدم ليشارك معلومات حساسة كرقم الهوية الوطنية أو معلومات البطاقة البنكية، أو حتى اختراق جهاز المستخدم لسرقة ملفات والعديد من الأمور الضارة التي قد يؤدي تلفها إلى العديد من الخسائر المادية والمعنوية، لذلك يجب أخذ الحيطة والحذر بزيادة الوعي لاكتشاف هذه الإيميلات الخبيثة.

طرق اكتشاف الإيميلات الخبيثة:

- ١ التحقق من المرسل في بعض الحالات يكون العنوان المرسل منه مشابه لما يبدو موثقاً، ولكن هناك اختلاف بسيط في الإملاء.
- ٢ الأخطاء الإملائية والنحوية ليس من الوارد تكرار الأخطاء الإملائية واللغوية من شركات معروفة، فوجودها بكثرة يشير إلى خطر محتمل.
- ٣ احتوائها على روابط أو مرفقات إذا كانت هذه الروابط تطلب معلومات شخصية من غير مُبرر واضح، فهي بالغالب تؤدي إلى سرقة المعلومات الشخصية، وكذلك المرفقات الـ مطالبة بالمعلومات الشخصية.
- ٤ عنوان إيميل تهديدي هناك بعض الصيغ التي قد تدل على أن المرسل نوايا خبيثة، مثلاً: "أحذر: سيتم إغلاق حسابك"، "الإجراء العاجل 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 مستنداتك الهامة وحفظها في مكان امن, يمكنك ذلك من استردادها في أي وقت ممكن.
- ٢ التحديث الدوري لبرنامج التشغيل. عند طلب جهازك لتحديث نسخة جديدة من نظام التشغيل, سارع بالحصول عليه. فإنه غالبا ما يتضمن تطوير وتقوية لامن 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-attacks>