



التصيد الإلكتروني



المركز الوطني الإرشادي لآمن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

مجمع الملك عبدالعزيز للاتصالات

هاتف ٢٦٣٩٢٣١ ١ ٩٦٦+

فاكس ٤٥٤٦٩٨٤ ١ ٩٦٦+

ص.ب ٧٥٦٠٦ الرياض ١١٥٨٨

المملكة العربية السعودية

www.cert.gov.sa

info@cert.gov.sa



المركز الوطني الإرشادي لآمن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission



Z CO.477 0033



المركز الوطني الإرشادي لآمن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

المركز الوطني الإرشادي لآمن المعلومات CERT-SA

لمحة:

المركز الوطني الإرشادي لآمن المعلومات بهيئة الاتصالات وتقنية المعلومات، هو مركز غير ربحي يهدف إلى رفع مستوى الوعي والمعرفة بأخطار أمن المعلومات، ويعمل بالتعاون مع أعضائه وشركائه على تنسيق جهود الوقاية والتصدي للأخطار والحوادث المتعلقة بالأمن الإلكتروني في المملكة العربية السعودية.

رؤيتنا:

أن تكون المرجعية الموثوق بها لآمن المعلومات في المملكة العربية السعودية.

مهمتنا:

- رفع مستوى الوعي بأمن المعلومات في المملكة العربية السعودية.
- تنسيق الجهود على المستوى الوطني لتفادي الاختراقات الأمنية، والعمل على احتواء أضرارها حال وقوعها.
- رفع مستوى الثقة في التعاملات الإلكترونية.
- التعاون والتنسيق مع المؤسسات والأطراف المؤثرة في تقديم خدمات الاتصالات وتقنية المعلومات في المملكة العربية السعودية في سبيل وقاية البنى التحتية والخدمات الإلكترونية من أخطار وتهديدات أمن المعلومات.
- تقديم المشورة والنصح للأفراد والمؤسسات فيما يتعلق بأمن المعلومات.

لمزيد من المعلومات الرجاء زيارة موقع المركز

www.cert.gov.sa

التصيد الإلكتروني

تتطور وسائل مخترقي الحاسوب (hackers) يوماً بعد يوم لخداع الآخرين من أجل الحصول على أرقامهم السرية أو أي معلومات حساسة، وإحدى أهم هذه الخدع هو ما انتشر في الآونة الأخيرة عبر المنتديات ورسائل البريد الإلكتروني، وهو ما يعرف بالتصيد الإلكتروني (Phishing Attack).

وتشير بعض الإحصائيات إلى أن بعض خدع التصيد في عام ٢٠٠٣م انطلت على نسبة ٥٪ من مستقبلي هذه الرسائل، وعددهم مليوناً مستخدم، وقد تم خداعهم ليقوموا بإفشاء معلوماتهم السرية لمواقع مصرفية مزيفة ومواقع بطاقات الائتمان، مما تسبب لهم بخسائر مادية مباشرة تقدر بنحو ١,٢ مليار دولار أمريكي^(١).

ما هو التصيد الإلكتروني

التصيد الإلكتروني (Phishing)، ويسمى أيضاً الاحتيال الإلكتروني والاستدراج الإلكتروني واللصوصية، ويعني قيام شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية يرتبط متلقي الرسالة بهذه الشركة، ويطلب الحصول منه على بعض المعلومات الشخصية مثل تفاصيل الحسابات المصرفية، وكلمات المرور، وتفاصيل بطاقة الائتمان، ويتم ذلك بعدة طرق أشهرها:

الطلب بالرد على الرسالة، أو وضع رابط في الرسالة لصفحة مزيفة، وعندها يقوم باستخدام المعلومات للدخول إلى الحسابات المصرفية عبر الإنترنت، أو الدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للسماح بالدخول إلى الموقع.

ومن الأمثلة الشائعة لهذا الخداع، أن تستقبل في بريدك الإلكتروني رسالة مزيفة باسم المصرف الذي تتعامل معه تحتوي على طلب المصرف منك الدخول لحسابك وتحديث بياناتك الشخصية، وعند الضغط على الرابط الموجود في الرسالة، يتم توجيهك إلى موقع إلكتروني مختلف، يكون مظهره مطابقاً لموقع ذلك المصرف. وعندما تقوم بإدخال اسم المستخدم والرقم السري كما طلب منك، فإن هذه البيانات ترسل لعنوان المخترق وليس إلى المصرف.

وكذلك من الأمثلة الشائعة الأخرى، المواقع المزيفة التي تدعي أنها تابعة لمؤسسات خيرية، وتطلب تبرعات لتمويل أنشطتها الإغاثية.

الأضرار المحتملة

إن حصول الجهة المحتالة على بياناتك الشخصية يمكّنها على الفور من انتحال هويتك، وسحب أو تحويل الأموال من رصيدك المصرفي.

طرق الوقاية

يمكنك أن تحمي نفسك من الوقوع فريسة لهذا النوع من الاحتيال باتباع الإرشادات والقواعد السهلة التالية:

أولاً: يلزم الحذر من الرسائل التي تطلب منك تحديث معلوماتك المالية أو الشخصية أو تأكيدها بشكل عاجل، إذ يجب عدم الرد عليها مباشرة، وكذلك يلزم الحذر من النقر على أي روابط إلكترونية بها، حتى لو ظهر لك أنها مرسله من جهة موثوقة.

ثانياً: عندما تتعرض لمثل هذه الرسائل، قم بزيارة الموقع الرئيسي للجهة المرسله من خلال كتابة العنوان الخاص بها المعروف لديك سابقاً في الصندوق المخصص للرابط في متصفح الإنترنت، أو عن طريق استخدام الارتباطات الموجودة في المفضلة، ولا تتردد في حال الاشتباه في الرسالة عن السؤال عن مصدرها وذلك بالاتصال هاتفياً أو من خلال البريد الرسمي لتلك الجهة، كالمصرف الذي تتعامل معه مثلاً.

ثالثاً: قبل أن ترسل معلومات مالية -كرقم بطاقة الائتمان- إلى موقع ما، تأكد أن الموقع يدعم بروتوكول التشفير (ssl)، وتستطيع معرفة ذلك من خلال ظهور قفل الأمان في نافذة المتصفح (في الشريط السفلي أو بجوار مربع العنوان).

رابعاً: تفقد بانتظام حساباتك المالية، وكشوف بطاقتك الائتمانية، وجميع تعاملاتك فيها، وفي حال اشتبهت بإحدى العمليات فعليك إبلاغ المصرف عنها فوراً.

المراجع:

(1) Litan, A. Phishing Attack Victims Likely Targets for Identity Theft. Gartner Research (2004).