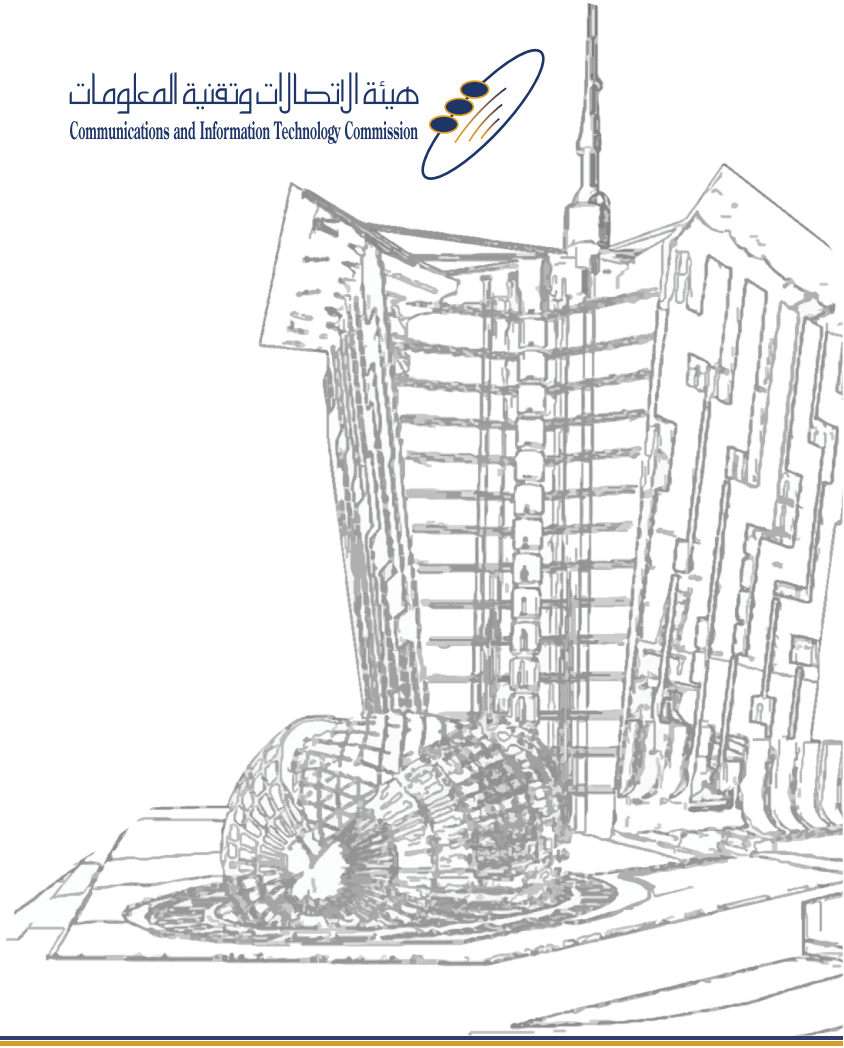
رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

التصيد الإلكتروني



www.citc.gov.sa
هيئة-الاتصالات-و-تقنية-المعلومات-السعودية

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 (Phishink Attack).

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

ما هو التصيد الإلكتروني

التصيّد 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

يمكن 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 مرسلة من جهة موثوقة.

ثانياً: عندما تتعرض لمثل هذه الرسائل, قم بزيارة الموقع الرئيسي للجهة المرسلة 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 التصفح (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 Attang Attack Victims Likely Targets for identity Theft. Gartner Research (2004).

آمر (مركز الاتصال الوطني) 199099 تحويلة 100

هاتف محلي 0114618000

البريد الإلكتروني info@citc.gov.sa

CITC.SA

CITCKSA

CITCKSA

CITC_SA

CITC_withU