

خدمة حقيقية كدت أن أقم فيها شخصياً

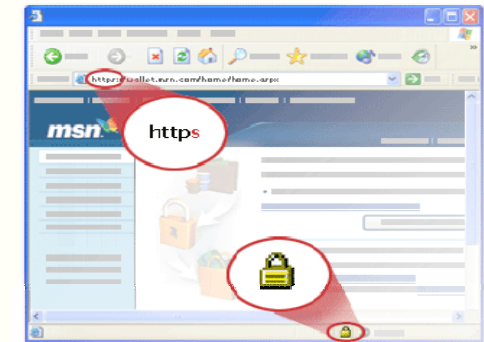
في أحد الأيام جئني رسالة بريد إلكتروني من عنوان أحد أساتذتي. هذه الرسالة تقول أنه أثناء زيارة عمل له في نيجيريا تعرض لحادث سطو في الشارع وتمت سرقة جميع متعلقاته من أموال وجواز سفر وأي أوراق تدل على هويته. ويطلب على استحياء أن أرسل له مبلغ ثلاثة آلاف دولار على حساب مدير الفندق الذي يقيم فيه. وكدت أن أرسل المطلوب لولا علمي بأن هذا أستاذي هذا له ابنا يعمل وكيلًا للنياحة، فقلت أستشير له لعله يساعد بالاتصال بوزارة الخارجية.

لقد كانت المفاجأة مذهلة: أستاذي هذا موجود بالمملكة العربية السعودية، للأسف قد تم الاستيلاء على حساب بريده الإلكتروني. وقد قام المحتالون بارسال نفس الرسالة لكل الذين تم التعامل معهم من ذلك البريد الإلكتروني. وقد تم عمل اللازم والاتصال بالاستاذ الفاضل والذي طلب من شركة خادم البريد الإلكتروني باغلاق الحساب الخاص به. وقد تم الاتصال التليفوني بكل من لهم علاقة بذلك البريد لطمأنتهم أولاً ثم تحذيرهم من ذلك العمل الأثم.

كيف أستطيع معرفة ما إذا كان موقع الويب مزيفاً؟

كما هو الحال مع رسائل البريد الإلكتروني الوهمية، فإن مواقع الويب التي تنتحل الهوية المزيفة تشتمل على رسومات الشعار وارتباطات الويب المقنعة. وبذلك يصعب معرفة ما إذا كانت وهمية. إن أفضل استراتيجية هي البحث عن الأشياء التي يجب أن تتوفر في مواقع ويب القانونية.

١- **أمان SSL** تستخدم مواقع ويب القانونية (Secure Sockets Layer (SSL طبقة المآخذ الأمانة (SSL) مقياس مقترح تم تطويره من قبل Netscape Communications لتأسيس قناة اتصالات آمنة لمنع كشف المعلومات الحساسة، مثل أرقام بطاقات الائتمان.



٢- **شهادة رقمية لموقع الويب**: ومن الفوائد الإضافية لـ SSL المصادقة على بيئة شبكة الاتصال أو تعدد المستخدمين، وهي عملية التحقق من صحة معلومات تسجيل دخول المستخدم. تقارن كلمة المرور واسم المستخدم مع القائمة المصرح بها، وإذا وجد تطابق، فيمنح حق الوصول باستخدام المستوى المسموح به. وهي عملية تعريف موقع الويب لك.

أفضل ما يمكن عمله للحماية من الاحتيال عبر الإنترنت

- يجب عدم الرد على رسائل البريد الإلكتروني التي تطلب معلوماتك الشخصية؛ يجب النظر بعين الشك إلى أي رسالة بريد إلكتروني من شركة أو شخص تطلب معلوماتك الشخصية — أو تلك التي ترسل لك معلوماتك الشخصية وتطلب منك تحديثها وتأكيدتها. وبدلاً من ذلك، استخدم رقم الهاتف من إحدى الكشوف الخاصة بك للاتصال، لا تتصل برقم مدرج برسالة البريد الإلكتروني. وبالمثل لا تقدم أبداً أي معلومات شخصية لأي شخص يقوم باتصال غير مرغوب فيه.
- لا تقم بالنقر فوق الارتباطات المشبوهة: لا تقم بالنقر فوق ارتباط مضمن في رسالة مشبوهة. فقد يكون الارتباط غير جدير بالثقة. وبدلاً من ذلك، قم بزيارة مواقع الويب بكتابة محدد موقع المعلومات (URL) الخاص بها بداخل المستعرض الخاص بك أو باستخدام الارتباطات الموجودة في "المفضلة" الخاصة بك.
- استخدام كلمات المرور القوية وتغييرها كثيراً: إذا كان حسابك يسمح باستخدام كلمات المرور القوية، فهي تلك التي تجمع بين الأحرف الكبيرة والصغيرة والأرقام والرموز مما يجعل تخمينها أمراً عسيراً.
- لا ترسل معلومات شخصية في رسائل البريد الإلكتروني المنتظمة: وذلك لأن رسائل البريد الإلكتروني المنتظمة ليست مشفرة وهي تشبه إرسال بطاقة بريدية.
- مارس أعمالك مع الشركات التي تعرفها وتثق بها فقط: استخدم الشركات المعروفة ذات السمعة الحسنة والمشهورة بجودة الخدمة. يجب أن يشتمل موقع ويب الشركة دائماً على نهج الخصوصية الذي يصرح على وجه التحديد بأن الشركة لن تقوم بتمرير اسمك ومعلوماتك الشخصية للآخرين.
- تأكد من أن موقع الويب يستخدم التشفير: يجب أن يكون عنوان الويب مسبقاً بـ https:// بدلاً من http:// المعتادة في شريط عناوين المستعرض.
- حماية الكمبيوتر الشخصي الخاص بك: من الضروري استخدام جدار حماية وتحديث الكمبيوتر الخاص بك واستخدام برامج مكافحة الفيروسات.
- راقب معاملتك: راجع تأكيد الطلبات وكشوف بطاقة الائتمان والبنك بمجرد استلامها للتأكد من أنك مسؤول فقط عن المعاملات التي قمت بها.
- استخدم البطاقات الائتمانية للمعاملات عبر الإنترنت في معظم المواقع، تكون مسؤوليتك الشخصية محدودة بشكل كبير في حالة قيام شخص ما باختراق بطاقتك الائتمانية.

أهم طرق الاتصال بوزارة الداخلية المصرية

موقع معلومات وزارة الداخلية www.moegypt.gov.eg

البريد الإلكتروني لوزارة الداخلية center@iscmi.gov.eg

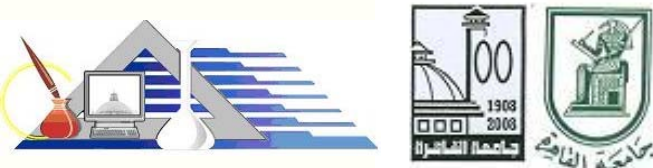
رقم تليفون مركز اتصالات الحكومة المصرية: ١٩٤٦٨

شرطة النجدة ١٢٢ مصلحة الأمن العام ١١٥

تليفونات مكافحة : الجرائم الإلكترونية : ٢٧٩٢١٤٩٠ جرائم الشبكات: ٢٧٩٢٨٤٨٤

جرائم الأموال العامة: ٢٧٩٢٩٩٨٨ جرائم المصنفات الفنية: ٢٧٩٤٣٢٩١

جرائم حقوق الملكية الفكرية: ٢٧٩٤٧٦٠٤



التعرّف على

خدم البريد الإلكتروني الوهمية

واصطياد الضحايا

إعداد

دكتور مهندس / هشام نبيه المهدي محمد

استاذ تكنولوجيا المعلومات المساعد

كلية الحاسبات والمعلومات - جامعة القاهرة

رائد الجمعية العلمية بالكلية

<http://www.h-elmahdy.net/>

ظهر محترفوا الاحتيال منذ بدء الخليقة، والآن بعد أن

أصبحنا في عصر الإنترنت فقد اتجه هؤلاء إلى الويب في محاولة

لاستغلال عملاء الإنترنت أصحاب النية الحسنة. أصبح الاحتيال

عبر الإنترنت ظاهرة وصارت تقنيات إنشاء رسائل البريد

الإلكتروني ومواقع الويب الخادعة أكثر تعقيداً. هذا العدد من

النشرة يلقي بعض الضوء على هذا الموضوع لعله يساعد في

الحماية من الاحتيال عبر الإنترنت.

كيف يكون الاحتيايل عبر الإنترنت أو اصطياد الضحايا؟

يشير أحد الأشكال المنتشرة للاحتييال عبر الإنترنت، والمعروفة باسم "اصطياد الضحايا"، إلى ممارسة "إرسال البريد غير الهام" للمستلمين باستخدام رسائل مزيفة تشبه الرسالة الصالحة من موقع ويب معروف أو شركة يتق بها المستلم، مثل شركة بطاقة الائتمان أو بنك أو مؤسسة خيرية. ويكون الغرض من الرسائل المزيفة هو خداع المستهلكين لتقديم معلومات شخصية أساسية. ولسوء الحظ يقع العديد من المستلمين (الذين لا يرتابون في الأمر) ضحية لمكائد اصطياد الضحايا هذه ويقدمون بغير قصد المعلومات الشخصية التالية :

- الرقم القومي. (NSN)
- رقم التعريف الشخصي. (PIN)
- رقم حساب البنك .
- رقم بطاقة الصراف الآلي/المدين أو بطاقة الائتمان.
- شفرة إثبات صحة بطاقة الائتمان. (CVC)
- رقم الهاتف والعنوان الخاص بك .

يستخدم المجرمون هذه المعلومات بعدة طرق لتحقيق مكاسب مادية. ومن الممارسات الشائعة جرائم انتحال الهويات، حيث يسرق المجرم معلوماتك الشخصية وينتحل شخصيتك ثم يمكنه عندئذٍ القيام بما يلي:

- طلب فتح اعتماد والحصول عليه باسمك .
- سحب حسابك بالكامل من البنك والحصول على أقصى حد تقدمه بطاقتك الائتمانية .
- تحويل المال من حساباتك الاستثمارية أو حد التسهيلات الائتمانية إلى حسابك الجاري، ثم استخدام نسخة من بطاقة المدين الخاصة بك لسحب المال من حسابك الجاري في جميع ماكينات الصراف الآلي حول العالم .

للحصول على معلومات حول كيفية تجنب الوقوع ضحية للاحتيال عبر الإنترنت، راجع قسم أفضل مايمكن عمله للحماية من الاحتيال عبر الإنترنت (صفحة ٦) في هذه النشرة.

أمثلة لمشاريع اصطياد الضحايا

تشمل بعض أمثلة اصطياد الضحايا:

- رسائل البريد الإلكتروني المزيفة مما يبدو وكأنه البنك الخاص بك أو شركة بطاقة الائتمان التي تحذرك من ضرورة التحقق من معلومات حسابك وإلا فسوف يتم تعليق الحساب .
- مجموعة من مواقع الاحتيال في المزادات ومستندات الضمان المزيفة. ويحدث ذلك عندما يتم عرض السلع للبيع في مزاد شرعي عبر الإنترنت لإغرائك بالدفع إلى موقع مستندات الضمان المزيفة .
- المؤسسات الخيرية المزيفة التي تطلب منك التبرع بالمال. لسوء الحظ، يستفيد الكثير من المحتالين من الأعمال الخيرية .

• صفقات المبيعات المزيفة عبر الإنترنت، حيث يعرض المجرم شراء شيء منك ويطلب دفع ثمن أعلى من الثمن الأصلي للسلعة المباعة. وفي مقابل ذلك، يطلب منك إرسال شيك له بفارق المبلغ. ولا يتم إرسال الدفع لك، ولكن يتم صرف الشيك ويحصل المجرم على الفارق. وبالإضافة إلى ذلك، يشتمل الشيك الذي قمت بإرساله على رقم حساب البنك وكود التوجيه للبنك والعنوان ورقم الهاتف .

هناك العديد من أنظمة "اصطياد الضحايا" (الحصول على البيانات الشخصية للمستخدمين دون معرفتهم). للحصول على أحدث تقرير حول أنظمة "اصطياد الضحايا" التي لم تكشف عنها الهيئات، قم بزيارة موقع ويب الخاص بجماعة العمل ضد "اصطياد الضحايا" .

كيف يمكنني معرفة إذا كانت رسالة البريد الإلكتروني خدعة أم لا؟ للأسف، يصعب من النظرة الأولى معرفة ما إذا كانت

الرسالة وهمية. وعلى سبيل المثال، يكون الكثير من رسائل البريد الإلكتروني المزيفة متصلة بشعارات شركات حقيقية. ولكن، فيما يلي الأشياء التي يمكنك مراقبتها:

- طلبات المعلومات الشخصية في رسالة بريد إلكتروني:** إن معظم الأعمال القانونية تتبع سياسة عدم السؤال عن المعلومات الشخصية عبر البريد الإلكتروني. يجب النظر بعين الشك إلى الرسالة التي تطلب منك معلومات شخصية حتى وإن بدت قانونية .
- أسلوب الاستعجال:** يكون أسلوب التعبير في رسائل البريد الإلكتروني لاصطياد الضحايا مهذباً في أغلب الأحوال وملائماً من حيث النغمة. ويحاول دائماً دفعك إلى الرد على الرسالة أو النقر فوق الارتباط المضمن. ولزيادة عدد الإجابات، يحاول المجرمون خلق الشعور بالأهمية مما يدفع الأشخاص إلى الرد الفوري بدون تفكير. وغالباً لا تكون رسائل البريد الإلكتروني المزيفة شخصية، بينما تكون عادة الرسائل الصالحة من البنك أو شركة التجارة الإلكترونية الخاصة بك شخصية.

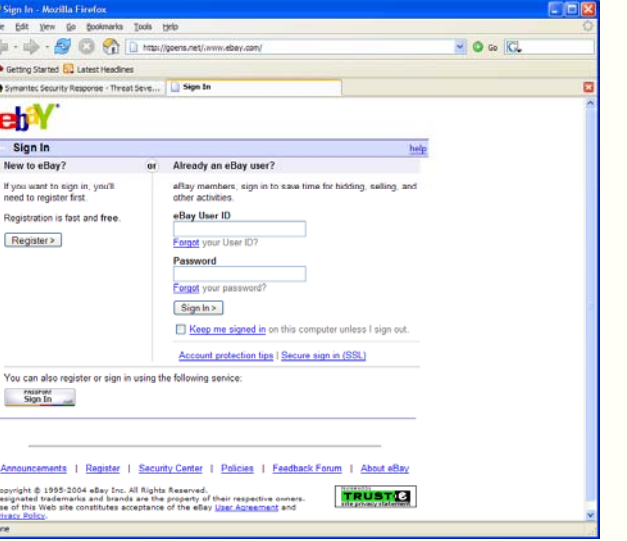
وفيما يلي مثالٌ من عمل حقيقي لاصطياد الضحايا:

عزيزي عميل البنك الهام، لقد بلغنا أنه يجب تحديث معلومات حسابك نظراً لوجود تقارير حول عملية احتيال وانتحال هوية لعضو غير نشط. وفي حالة الإخفاق في تحديث السجلات الخاصة بك فسوف يتم إلغاء حسابك. الرجاء اتباع الارتباط أدناه لتأكيد بياناتك .

- الارتباطات المزيفة:** في الرسائل بتنسيق HTML : تكون الارتباطات التي يتم حثك على النقر فوقها مشتملة على اسم شركة حقيقية بالكامل أو جزء من الاسم وتكون غالباً "مُتَّعَةً"أي أن الارتباط الذي تراه لا ينقلك إلى ذلك العنوان ولكن إلى مكان مختلف، يكون في الغالب موقع ويب تم انتحال هويته (طبعا للحصول على بيانات كروت ائتمانك).

المراجع: مجموعة من المقالات التي نشرها الدكتور هشام المهدي في دوريات ومؤتمرات http://office.microsoft.com/ar-sa/outlook/

الشكر واجب للأستاذ الدكتور/ محمد يوسف نائب رئيس الجامعة لدعمه للجمعية العلمية بالكلية ولكل الزملاء المراجعين ، ولمركز التعليم المفتوح بالجامعة لطباعته هذه النشرة



- طلبات المشاركة في صفقات عبر رسالة بريد إلكتروني:** مثل أن تأتيك رسالة من اسم من الأسماء المسلمة وتدعي أنها أرملة لمدير بنك في نيجيريا أو لوزير سابق في دولة أفريقية. وتقول أنها تملك ملايين الدولارات في حساب مشترك مع زوجها المرحوم ، وتطلب فقط موافقتك على مشاركتها وإرسال بيانات حسابك في البنك لتقوم بإرسال تلك الملايين لك لتتقاسمها سويا .. ولكن من يطيع تلك الخدع يخسر كل ما لديه في ذلك الحساب.



- المرفقات:** تطلبك العديد من مكائد اصطياد الضحايا بفتح المرفقات، والتي قد تصيب جهازك بفيروس. لا تفتح المرفقات في رسائل البريد الإلكتروني المشبوهة.

- الفوز بجوائز مئات الملايين من الدولارات أو اليورو:** تعتمد تلك المواقع على مدى طمع المتلقي ، فيطلب أولاً ملئ نموذجاً عادياً ليس به بيانات تخص حسابات البنوك ، ثم تتوالى الرسائل بأنك ضمن أول خمسة مرشحين للفوز ، وللاستمرار حتى النهاية في المسابقة يبدأ بطلب دفع مبالغ بسيطة في الأول ثم تتوالى الطلبات. ولايفيق المخدوع إلا بعد فوات الأوان.