الخليج

أخبار الدار, تحقيقات وحوارات

1 يوليو 2023 01:47 صباحا

اللص.. بريد إلكتروني مزيّف ينتحل شخصية شركة معروفة


http://
.com

تحقيق: راشد النعيمي

في ظل الرواج الكبير للتجارة الإلكترونية والطلب والشراء والتوصيل عبر الإنترنت، نشط نمط جديد من الاحتيال الذي يستغل لهفة تلقي المشتريات ووصولها إلى المستهلك، خاصة من لا يملك خلفية وخبرة في أساليب الاحتيال، وينصاع لأي بريد إلكتروني مزيّف ينتحل شخصية شركة توصيل معروفة، ويطلب بياناته المصرفية لدفع رسوم لا تتعدّى دراهم معدودة، قيمة خدمات تكون بوابة كبرى لنهب أمواله في ما بعد.

وبدأت شركات توصيل شهيرة في تحذير زبائنها من عمليات النصب التي تجري عبر انتحال شخصياتها، بعد أن كانت تستهدف «بريد الإمارات» في وقت سابق، وطالبتهم بضرورة الحذر والتأكد عبر مختلف القنوات والتطبيقات من سير شحناتهم أو الاتصال هاتفياً، عبر مراكز الاتصال المعتمدة، للتأكد من سير الشحنة. فيما دعت شركة شهيرة لمكافحة الفيروسات، إلى ضرورة وجود برامج المكافحة لكشف التصيّد الاحتيالي.

أشارت شركات توصيل إلى أن التصيّد، نوع من أنواع احتيال الهندسة الاجتماعية، حيث يحاول المهاجم ملاحقة ضحاياه ودفعهم إلى تقديم معلومات قيمة. ومن أبرز وسائل هجمات التصيّد، الرسائل الإلكترونية، حيث يصمّم المهاجم رسالة تبدو للمستقبل، كأنها من جهة موثوقة، وقد تكون الرسالة من بنك معين، أو على شكل تحذير من حادثة أمنية معينة، أو إرسال رابط يطالب المستخدم باستعادة كلمة المرور، أو دفع قيمة خدمات.

معلومات حساسة

شركة «أرامكس» أشارت في البداية إلى أن رسائل البريد الإلكتروني الاحتيالية والضارّة، أكثر طرائق الاحتيال شيوعاً عبر الإنترنت، وتهدف إلى خداع الجمهور بالتظاهر بأن مصدرها معروف كشركة «أرامكس» (على سبيل المثال: تسلّم رسالة إلكترونية تبدو في ظاهرها أنها مرسلة منها) من أجل حثكم على مشاركة معلومات شخصية ذات طبيعة حساسة، أو بيانات الحساب أو إرسال أموال، وقد تتضمن أيضاً طلباً بالتسجيل في مسابقة من أجل الفوز بجوائز.

وأضافت: «نلتزم في «أرامكس» بحماية المعلومات الحساسة لعملائنا، ونأخذ هذا الأمر على محمل الجد، ونواظب على مراقبة المعلومات والبيانات المتاحة لدينا من أجل تفادي ومنع أي سلوك احتيالي أو مشبوه، وفي حين أننا نبذل أقصى ما بوسعنا لحماية عملائنا وشركائنا، فإننا نحثهم أيضاً على دعم جهودنا هذه عبر القيام بواجبهم في رصد أي سلوك احتيالي محتمل من قبل أطراف خبيثة تستغل اسمها للتضليل».

ومن جانب آخر قالت شركة «فيدكس»، إنها لا تطلب عبر مكالمات أو بريد أو رسائل نصية أو رسائل بريد إلكتروني غير مرغوب فيها، معلومات الدفع أو معلومات شخصية مقابل بضائع بصدد النقل أو موجودة في حيازتها، وفي حال تلقي أي من هذه الاتصالات أو اتصالات مشابهة لها، فلا ترد أو تتعاون مع جهة الإرسال.

عمليات خداع

وقالت شركة مكافحة الفيروسات الشهيرة «كاسبر سكاي»: «إن عملية الخداع تبدأ بوصول إشعار بريد إلكتروني، يبدو أنه صادر عن خدمة توصيل شهيرة. وترسل الرسائل بلغات مختلفة، وتختلف أسماء خدمات البريد التي تنتحل باختلاف المناطق الجغرافية. ولا تكون عملية التقليد مثالية، فمن بين العلامات التي دلت على عملية الاحتيال، كانت كل عينات الرسائل الاحتيالية التي تمت مراجعتها مُرسَلة من عناوين بريد إلكتروني عشوائية ليس لها علاقة بأي من عناوين البريد الإلكتروني الرسمية للخدمات البريدية».

وأضافت أن رسائل البريد الإلكتروني الاحتيالية، تظهر بلغات متعددة وكأنها واردة من خدمات بريدية مختلفة معروفة، ويذكر الإشعار أن الطلب لم يسلّم بسبب عنوان خطأ، أو وجود رسوم إضافية نتيجة لنفقات غير متوقعة، أو سبب آخر معقول، ولكن بشكل غامض ثم يُطلَب من المستلم سداد مبلغ صغير (لا يتعدى 3 يوروهات) لضمان وصول الطلب. ويوفِّر المرسل رابطاً إلكترونياً لصفحة تبدو كموقع إلكتروني لخدمة بريد، ولكنها في الواقع صفحة «ويب» احتيالية.

وينقر المستخدمون الذين تنطلي عليهم الخدعة على الرابط، ويذهبون مباشرة إلى صفحة السداد، ويدخلون بياناتهم الشخصية وبيانات البطاقة المصرفية كما طُلب منهم، ثم يدخلون رمز تأكيد يرسل في رسالة نصية.

ونصحت الشركة المستخدمين باتباع طرائق مختلفة لحماية أموالهم من المحتالين، عبر تتبّع الطرود بشكل أساسي، وإذا كان هناك عدد كبير من الطلبات لا يمكن تذكرها كلها، يمكن إنشاء ملف أو وضع قائمة للطلبات التي لم تصلك بعد، كما يجب تجنب النقر على الروابط في رسائل البريد الإلكتروني، وخاصة إذا لم تكن متأكداً تماماً أنها صحيحة، ولا تُدخِل بياناتك الشخصية أو المصرفية أبداً في صفحات تحيلك إليها روابط مماثلة.

وأضافت: «إذا ساورك الشك، فاتصل بخدمة التوصيل هاتفياً لتعرف ما يحدث. ويمكنك البحث عن رقم تتبّع الطرد في رسالة تأكيد الطلب أو الشحنة، والتحقق من حالة التوصيل على الموقع الإلكتروني الرسمي للخدمة، كما يمكنك تثبيت برنامج مكافحة فيروسات يتضمن حماية ضد التصيد الاحتيالي والغش».

تحذيرات وتنبيهات

وكانت مؤسسة «بريد الإمارات» قد دعت في وقت سابق المتعاملين إلى استخدام موقعها الإلكتروني الرسمي وتطبيق الهاتف المحمول عند إجراء عمليات الدفع الإلكتروني، عبر «الإنترنت»، لتسديد رسوم /emiratespost.ae/ الشحنات ومنتجات التجزئة، التزاماً منها بضمان أعلى مستويات موثوقية معاملات الدفع الآمن.

وتأتي هذه الخطوة في إطار الجهود الحثيثة والمستمرة التي تبذلها الشركة، لحماية المتعاملين من مخاطر الوصول إلى بوابات الدفع الرقمي غير القانونية التي تُمثل جزءاً من مخططات الاحتيال الإلكتروني.

وشددت على أهمية توخي الحذر عند إجراء المدفوعات، وبالأخص عبر رسائل البريد الإلكتروني والرسائل النصية القصيرة التي تدّعي أنها من «بريد الإمارات»، حيث توفّر روابط إلكترونية لنظام دفع تابع لجهة خارجية أو تحفيز المتعاملين على إنشاء حسابات وإجراء مدفوعات مقابل تسليم شحناتهم. وأكّدت الشركة أنها، ومن الآن فصاعداً، لن تُطلق أي رسالة نصية أو رسالة عبر البريد الإلكتروني لربط المتعاملين، ببوابة دفع إلكتروني خارج موقعها الإلكتروني الرسمي. وتذكّر المتعاملين بضرورة التحقق على الدوام من العنوان الإلكتروني للجهة المرسلة مع الامتناع عن الكشف عن أي بيانات خاصة أو معلومات.

طلبات زائفة

كما حذّرت شرطة أبوظبي في وقت سابق، من طرائق احتيال عبر طلبات التوصيل الزائفة، وإرسال بريد إلكتروني أو رسالة نصية إلى الضحية، ويُطلب منه إجراء دفع مقابل شحنة؛ حيث يضغط المتعامل على الرابط، ويدخل بيانات بطاقته البنكية، بعد ذلك تستخدم بيانات البطاقة في موقع للتجارة الإلكترونية، وتنشأ كلمة مرور لمرة واحدة، بعد ذلك لا يقرأ الضحية الرسالة بدقّة، ويعتقد أنه تسلّم كلمة المرور لمرة واحدة لعملية الدفع التي يجريها ويدخلها، ويحصل المحتال عليها ويستخدمها لإتمام معاملة الشراء الخاصة به.

وحددت 7 نصائح لتجنّب الوقوع ضحية للاحتيال، هي: عدم الضغط على الروابط الموجودة في رسائل البريد الإلكتروني أو الرسائل الصغيرة، دون التأكد من غرضها، والتأكد في حال كان هو أو أحد أفراد أسرته، يتوقعون وصول شحنة لهم، وقراءة الرسائل بعناية والتحقق من مصدرها، والتحقق من عناوين البريد الإلكتروني المشابهة أحياناً لعناوين في الموقع، وتجنّب تقديم البيانات البنكية عبر برنامج «واتس آب»، HTTPS البريد الإلكتروني الأصلية، ووجود والقراءة بعناية لرسائل كلمة المرور الواحدة التي يرسلها المصرف، وتجنب الضغط على العروض الترويجية عبر الإنترنت ومواقع التواصل، التي تبدو جيدة إلى حد يصعب تصديقه.

الصورة