الجرائم والسرقات الإلكترونية

من الجرائم المنتشرة بكثرة عبر وسائل تقنية المعلومات والمواقع الإلكترونية السرقات الإلكترونية. ولها عدة صور تنتهي بأخذ مال أو معلومات أو صور خاصة أو أوراق رسمية أو أي عرض من ممتلكات المستخدم دون إذنه وقبوله. ورغم أن المسروق هنا يكون شيء معنوي عادة (أي غير محسوس)، إلا أنه لا يزال نوع من السرقة التي حرمها الله. وذلك لأن السارق يأخذ ما لغيره بدون حق ولا إذن، بطرق ملتوية وغير مقبولة.

وهذا فعل محرم وربما يدخل في باب السرقة التي هي من كبائر الذنوب وتستوجب الحد. قال تعالى: {وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءً بِمَا كَسَبَا نَكَالًا مِّنَ اللَّهِ وَاللَّهُ عَزِيزٌ حَكِيمٌ} [1]. وقد فرض الله حد السرقة ليكون رادع ومانع لآفة السرقة، بحيث إذا طُبِّق على بعض الافراد يردع البقية ممن توسوس له نفسه بهذه الجريمة في المستقبل فينتهي عنها. فينعم بعدها المجتمع بالأمن والسلامة من هذه الآفة.

ولذلك لم يتهاون الرسول ﷺ في تطبيق هذا الحد مهما كان. وعندما حاول أسامة بن زيد الشفاعة في المرأة المخزومية التي سرقت نهاه الرسول ﷺ عن ذلك؛ لعلمه بأن التهاون في إقامة الحد سيضعف أثره في ردع الناس ويرجع إنتشار السرقة من جديد.

وجاء هذا في حديث عروة رضي الله عنه، حيث قال: «أن امرأة سرقت في عهد رسول الله ﷺ في غزوة الفتح ففزع قومها إلى أسامة بن زيد يستشفعونه، قال عروة: فلما كلمه أسامة فيها تلون وجه رسول الله ﷺ فقال: أتكلمني في حد من حدود الله ؟! قال أسامة: استغفر لي يا رسول الله. فلما كان العشي قام رسول الله خطيبا، فأثنى على الله بما هو أهله، ثم قال: أما بعد، فإنما هلك الناس قبلكم؛ أنهم كانوا إذا سرق فيهم الشريف تركوه، وإذا سرق فيهم الضعيف أقاموا عليه الحد، والذي نفس محمد بيده لو أن فاطمة بنت محمد سرقت لقطعت يدها» [2].

أمثلة لطرق السرقات التي تحدث عبر تقنية المعلومات والمواقع الإلكترونية:

- كثيرا ما تصل رسائل الكترونية من قبل نصابين تبدو على شكل الرسائل البنكية الرسمية لتخدع المستلم فيظنها مرسلة من بنكه فيدخل معلومات حساسة، مثل كلمة السر ورقم بطاقة الدفع والرقم الوطني ونحوها من المعلومات التي يستطيع بها اللص الوصول لحسابات المستخدم وسحب المال منها. وأحيانا تكون الروابط لمواقع تبدو مثل أحد الشركات أو المتاجر الكبرى فيدخل المستخدم معلوماته لشراء سلعة وتتم سرقة المعلومات بهذه الطريقة.

- عبر دخول متلصص لحسابات المستخدمين، في مواقع الشركات والمتاجر الالكترونية الكبيرة مثل أمازون وغيرها وهناك يمكنهم شراء سلع على في حساب الضحية أو سرقة معلومات مهمة مثل بيانات الدفع والعنوان وغيرها. وذلك بعد حصوله بشكل ما على كلمة السر واسم المستخدم. وكثير ما يحدث هذا عند بيع الأجهزة الإلكترونية كالجوال والحاسوب. فبالرغم من مسحها، فإن بعض اللصوص المحترفين يستطيعون استعادة الملفات المحذوفة.

- عن طريق استلام مكالمة هاتفية مسجلة برسالة مخادعة تقنع مستقبل المكالمة بأن الإتصال من جهة حكومية ونحوها، وتطلب منه الضغط على زر معين ويتم بعدها سحب المعلومات المخزنة في الهاتف الجوال.

- عن طريق الهاكر لقواعد البيانات من الشركات التي تخزن معلومات عملائها.

- أحيانا تصل اتصالات هاتفية من مجهول بسرد الأكاذيب مثل أنه عامل من شركة مايكروسوفت ويريد الاتصال بالجهاز لإصلاح ويندوز أو نحوها من الحيل والأكاذيب، فيصدقه المستخدم ويقبل دعوته للاتصال بجهازه عبر الشبكة الافتراضية الخاصة (VPN). وعندها يستطيع المتلصص البحث في الجهاز عن المعلومات الحساسة والصور الخاصة والملفات الرسمية والحكومية مثل الهوية الشخصية ونحوها.

وهناك طرق أخرى كثيرة، ولعل هذه أكثرها انتشارا.

تمييز المواقع والشركات ذات الثقة من غيرها

هناك علامات تساعد المستخدم في تمييز الشركات ذات الثقة من الشركات غير الموثوق بها. وعلى الرغم من أنها ليست دقيقة، ولا يمكن الجزم القاطع بها في الحكم على الموقع أو الشركة، إلا إنها قد تساهم كثيرا في حماية المستخدم وتمكينه من معرفة بعض المواقع المشبوهة والابتعاد عنها. ولذا الأفضل التعامل مع الشركات الكبرى التي حظيت بثقة الناس مثل قوقل وأبل ونحوها، والبعد عن الشركات التي لا يشتمل موقعها عن أي نوع من أنظمة حماية المواقع وتبدو غير آمنة.

أمثلة لأنظمة حماية المواقع

كما ذكرنا أن المواقع الموثوق بها عادة تحتوي على نوع من الحماية لتحمي مستخدميها وحفظ خصوصيتهم. وهناك عدة طرق للحماية، نذكر منها:

أن يحتوي الموقع على نظام أمن طبقة النقل (Secure Socket Layer) أو باختصار (SSL). وتعرف ببدء عنوان الموقع ب(https://) بدلاً عن (http://).

إستعمال شركات الأمن الإلكتروني التي تقدم خدمة تأمين شامل للمواقعن لاسيما للشركات والمتاجر الإلكترونية. ومن امثلتها (SquareTrade) و(Comodo SSL) و (SiteLock)

كذلك تأمين قواعد البيانات والمخدمات (Servers) المخزنة بها داخل الشركات. وهذا لا يظهر للمستخدم ولابد من البحث عما إذا كانت الشركة المستضيفة لهذه البيانات تستخدم نوع من الحماية مثل تشفير البيانات. وأحيانا تقوم الشركات بإستعمال سيرفرات من شركات أخرى مثل سيرفرات أمازون (AWS)، وقوقل كلاود (Google Cloud)، وميكروسوفت أزور (MS Azure)، وغيرها. وهذه الشركات الكبيرة عادة لها إمكانيات حماية قوية ويصعب اختراقها.

صفات المواقع والشركات الموثوق بها

ومن صفات الشركات ذات الثقة انها عادة:

- تكون خالية من الإعلانات.

- تكون لها منتجات ذات قيمة للبيع.

- يكون لها موقع احترافي (Professional Website)

- تكون عادة شركات كبري ومشهورة ولها أكثر من مكتب واحد ولها فروع في أكثر من موقع.

صفات المواقع والشركات المشبوهة

من العلامات التي عادة ما تثير الشبهة حول الموقع أو الشركة أنها توفر خدمات مجانية دون أي مقابل. فكثير من الشركات التي لا توفر غير المنتجات المجانية يكون هدفها هو التجسس وسرقة البيانات وإرسال الدعايات المزعجة.

- تصميم مواقعها عادة غير احترافي أو به روابط لا تعمل.

- مواقعها تكون عادة مليئة بالدعاية والصور ذات الألوان الصارخة.

- تظهر عادة في مواقعها نوافذ منبثقة (Popup Windows) تطلب الإجابة على سؤال بالضغط على زر. مثلاً تظهر رسائل عن ربح جائزة مثل رحلة سفر بعد الرد على بعض الأسئلة. ثم ما أن يبدأ المستخدم بالمشاركة بالإجابة على سؤال، حتى يتبعه سلسلة من الأسئلة التي تدعوه لشراء سلعة للحصول على الجائزة أو الاشتراك في خدمة ونحوها. وحتى إن فعل تأتي رسائل أخرى عن شراء سلع وخدمات أخرى. وهكذا تدخل المستخدم في متاهات، وتجعله يشترى أشياء لم يكن يحتاجها أو يريد شرائها. وبعد كل هذا عادة ما لا يحصل المستخدم على أي شيء ذو قيمة، بل يتم خداعه وتضييع وقته والحصول منه على معلومات تستخدم في التسويق.

- أنها تسرق معلومات المستخدم المخزنة في ملفات الارتباط (Cookies)، وبعد تصفح الموقع عادة ما تصل لمتصفحه كم من رسائل الدعاية عن طريق البريد الإلكتروني أو رسائل الجوال وغيره. ويتم ذلك عادة بزراعة برامج خبيثة للدعاية (Malware) في جهازه.

السرقات الالكترونية من منظور مقاصد القرآن الكريم

- السرقات الإلكترونية هي أخذ حق دون وجه، ويتضرر منها المسروق منه. ولذا فقد تدخل ضمن السرقات العادية والتي هي محرمة شرعاً بالكتاب والسنة والإجماع، وتتناقض مع مقصد التشريع أو الأحكام. السرقة عملية لا أخلاقية، وهذا يتناقض مع مقصد تهذيب الأخلاق.

- السرقة فيها ظلم وتزعزع أمن المجتمع واستقراره، وتتناقض مع مقصد سياسة الأمة وأمن الدولة. فتنشر الفساد والذعر وعدم الأمن وتتناقض بذلك أيضاً مع مقصد صلاح الأحوال الفردية والجماعية.

- السارق لا يرتدع للوعيد وهذا يتناقض مع مقصد المواعظ، والإنذار، والتبشير، والوعيد.

النصائح والضوابط المقترحة

- يجب الحذر من الرسائل المشبوهة وعدم التسرع بفتح الروابط فيها إلا بعد التأكد بأنها من الجهة المعنية كالبنك ونحوه.

- وعادة الرسائل المشبوهة تعرف بالنظر إلى الإيميل المرسلة منه، فإذا لم يكن ينتهي باسم الشركة المعنية، يجب ألا يفتح الرابط من غير البحث في أمرها. وكثير من الأحيان إذا نسخ المستخدم نص الرسالة وبحث عنه في محرك قوقل، يجد أن مستخدمي الانترنت تحدثوا عنها وأنها تحتوي على غش (Scam)، ويحذرون منها.

- يجب تجنب التعامل مع الشركات غير الموثوق بها بقدر الإمكان. ومع الوقت وإستخدام الانترنت لعدة أعوام يكتسب المستخدم الخبرة والحس الذي يجعله يحدد إذا ما كان الموقع أو الشركة آمن أو لا إلى حد كبير.

[1]سورة المائدة، آية ٣٨.

[2]أخرجه الألباني في صحيح النسائي (٤٩١٨) وصححه