إضاءات

نشرة توعوية يصدرها معهد الدراسات المصرفية

دولة الكويت - نوفمبر 2020

سرقة المعلومات الخاصة بالهوية المالية
FINANCIAL IDENTITY THEFT

السلسلة 13 | العدد 2

المقدمة

عندما يُذكر مصطلح «سرقة الهوية»، يتبادر للذهن مباشرة أنشطة الاحتيال البسيطة كسرقة بطاقات الائتمان، أو انتحال شخصية شخص آخر لطلب قرض، أو ما شابه. في الواقع، يتعدى الأمر كونه بهذه البساطة، حيث ينطوي مفهوم سرقة الهوية على عدد أكبر من الجرائم التي يمكن ارتكابها، حال انتحال هوية شخص آخر باستخدام بيانات التعريف الأساسية الخاصة به، وذلك على مستوى المعاملات الحكومية، الطبية، الجنائية وكذلك انتحال الهوية عبر الإنترنت. هذا، بالإضافة إلى بعض الأشكال الفريدة والمُركّبة لسرقة الهوية المالية على وجه التحديد.

محاور العدد:

- مفهوم سرقة معلومات الهوية المالية وما يتضمنه
- علامات إنذار يجب الالتفات إليها
- كيف يؤثر اختراق البيانات Data Breach على أمن معلومات الهوية
- البطاقات الشخصية وما تفصح به من معلومات
- خطر مشاركة المعلومات على مواقع التواصل الاجتماعي
- كيفية تجنب سرقة معلومات الهوية المالية
- دولة الكويت: بعض الجرائم وعقوبتها في قانون جرائم تقنية المعلومات

مفهوم سرقة معلومات الهوية المالية وما يتضمنه

تحدث سرقة الهوية المالية عندما يتمكن شخص ما من الدخول إلى البيانات المالية لشخص آخر، واستخدامها والتلاعب بها بما يخدم مصلحته ويحقق له المكاسب، في حين التظاهر بأنه صاحب البيانات الحقيقي. وقد يكون السارق شخصاً غريباً استطاع اختراق بيانات شخص آخر لا تربطه به معرفة سابقة، أو يكون شخصاً من داخل دائرة معارف الشخص المسروقة هويته، كزملاء العمل، الأصدقاء أو الأقارب ممن يستطيعون الحصول على مستنداته واستخدامها دون علمه.

ومن أهم المعلومات التي يحتاجها سارق الهوية كل من التالي:

- **الرقم المدني:** حيث يتعين على جميع الأشخاص الحفاظ على سريته وعدم إدخاله على الإنترنت على مواقع قد تتعرض للاختراق، وكذلك الحفاظ على البطاقة المدنية في مكان آمن طوال الوقت، دون تركها في متناول الآخرين. هذا، ويجب التنويه إلى أن الرقم المدني تتم طباعته أحياناً على مستندات أخرى كالفواتير مثلاً، والتي ينبغي تمزيقها جيداً والتخلص منها فور الانتهاء من الحاجة إليها.

- **بيانات التعريف الشخصية:** وهي معلومات أخرى يسهّل الحصول عليها عملية سرقة الهوية المالية على سبيل المثال: عنوان السكن، تاريخ الميلاد، اسم الأم – وهي معلومات تكون بالطبع معروفة للأقارب والأصدقاء.

هذا، وتتضمن مجالات سرقة الهوية المالية أنشطة أكثر تعقيداً قد يكون لها تبعات خطيرة، وجنائية أحياناً. على سبيل المثال، أن يقوم سارق الهوية باستخدامها في التقديم على طلب لقرض كبير، تاركاً صاحب الهوية الأصلي غارقاً في الديون وفي جرائم احتيال، بالإضافة إلى زيادة دخل لم يتم الإفصاح عنها للضرائب، مما يترتب عليه تهمة التهرب الضريبي.

كذلك، من الممكن سرقة الهوية المالية لطلب دفتر شيكات لحساب بنكي تم فتحه حديثاً، واستخدام اسم صاحبه الأصلي في تحرير عدد من الشيكات بدون رصيد، مما يعرضه للمساءلة القانونية، أو استخدام الهوية المالية المسروقة لشخص ما لضمان عملية بيع/ شراء معينة، ومن ثم يتفاجأ ذلك الشخص باستلام إشعارات لمنتجات/ خدمات تم شراؤها في بلد آخر تحت ضمانته، دون أن يعلم عنها شيئاً.

علامات إنذار يجب الالتفات إليها

- استلام كشوف حساب خاصة ببطاقات ائتمان غير معلومة
- وجود أخطاء (معلومات مغلوطة) على التقارير الائتمانية
- الحصول على رفض عند تقديم طلب على قرض/ زيادة لحد الائتمان
- الحصول على رفض عند تقديم طلب لخدمة معينة أو طلب استئجار
- الحصول على رفض عند تقديم طلب على وظيفة (بناءً على بحث لصحيفة الحالة الجنائية)
- استلام إشعارات تحصيل لحسابات أو قروض غير معلومة
- زيادة الفائدة المحصّلة على بطاقات الائتمان (نتيجة لزيادة غير معلومة في عمليات البطاقة)
- استلام فواتير لمنتجات وخدمات لم يتم شراؤها/ طلبها
- زيادة غير معلومة المصدر في معدّل تأمين السيارة (نظراً لوجود مخالفات أو حوادث غير معلومة)
- تأخر/ ضياع البريد الدوري المعتاد وصوله من المؤسسات المالية التي يتم التعامل معها (كالفواتير، كشوف الحساب أو البريد الإلكتروني)

كيف يؤثر اختراق البيانات Data Breach على أمن معلومات الهوية

يُعتبر الاختراق الذي حدث لإحدى شركات التجزئة الأمريكية، والذي تم من خلاله سرقة البيانات المالية الخاصة بالبطاقات الائتمانية لعشرات الملايين من العملاء أثناء موسم التسوق، وتحديداً خلال اليوم التالي لعيد الشكر والذي يُطلق عليه Black Friday، من أبرز حوادث الاختراق التي هزت العالم منذ بضع سنوات، حيث تحدثت وسائل الإعلام والقنوات الإخبارية حول العالم مطولاً عن مدى التمكن والمهارة التي تطلّبها إتمام هذا الاختراق.

أما الآن، وفي ظل التنامي المستمر لتكنولوجيا المعلومات، فقد أصبح ذلك الاختراق الضخم، والذي حدث عام 2013، يُعد أحد العمليات البسيطة والساذجة لسرقة الهوية المالية. فقد

حدث منذ ذلك الحين على مستوى الولايات المتحدة الأمريكية عدد من عمليات الاختراق الضخمة، والتي اتسع نطاقها ليشمل ملايين الضحايا.

على سبيل المثال: عملية اختراق البيانات التي شهدتها وكالة شؤون الأفراد التابعة للحكومة الأمريكية OPM (Office of Personnel Management) والتي تمت بمقتضاها سرقة أرقام الضمان الاجتماعي لعدد 22 مليون شخص، وكذلك اختراق بيانات الدخول إلى حسابات البريد الإلكتروني لحوالي مليون مستخدم التي شهدتها شركة ياهو Yahoo.

هذا، وقد تعرضت أكثر من (200) مؤسسة/ شركة أمريكية خلال عام 2017 وحده إلى اختراقات تستهدف الحصول على أرقام الضمان الاجتماعي وبيانات الرواتب الخاصة بعملائها، حيث يبدو أن مرتكبي جرائم سرقة الهوية المالية قد أدركوا أن المكاسب الأكبر تكمن في الحصول على البيانات الأوسع نطاقاً والأطول امتداداً مع مرور الوقت، حيث يطورون كل فترة من الأساليب التي تمكنهم من وضع أيديهم على تلك البيانات.

من ناحية أخرى، يجب على المستهلكين أن يدركوا أهمية عمليات الاختراق المشار إليها – سواء كانت قد حدثت عمداً أو بطريق الخطأ – في التسبب في سرقة هوياتهم المالية. كما يجب معرفة الخطوات الواجب القيام بها فور العلم بأن بياناتهم قد تعرضت للاختراق، وذلك كما يلي:

في حال وصول تنويه من الشركة يفيد بأن بيانات العملاء قد تم اختراقها

- **قراءة الكتاب / البريد الإلكتروني المُرسل بعناية فائقة للتعرف على نوعية البيانات التي تم اختراقها:** بيانات مالية كأرقام حسابات بنكية/ بطاقات ائتمان، بيانات خاصة بالدخول على حسابات على الإنترنت كاسم المستخدم، كلمة السر، الأسئلة التي يتم طرحها للتأكد من الهوية security questions ...الخ. قد تكون الهوية قد تم اختراق معلوماتها بالكامل بما في ذلك الاسم، العنوان، تاريخ الميلاد، الرقم المدني، وهو الأمر الذي ستتحدد بناءً عليه الإجراءات الاحترازية الواجب اتخاذها فوراً، بدءاً من تغيير كلمة السر لحساب معين على الإنترنت وانتهاءً بمخاطبة البنك/ مؤسسات الائتمان التي يتبعها الشخص لطلب تجميد العمليات على حسابه الائتماني.

- **مراجعة تقارير العمليات الائتمانيةCredit reports:** يجب مراجعة هذه التقارير بشكل دوري، حيث أن هذه الخطوة الاحترازية من المهم القيام بها دوماً، بغض النظر عن حدوث اختراق للبيانات الشخصية، وذلك لتتبع أنشطة الحسابات الائتمانية واتخاذ الإجراءات اللازمة في حالة وجود عمليات/ أنشطة مشكوك في صحتها suspicious activity.

البطاقات الشخصية وما تفصح به من معلومات

يكاد يكون كل شخص بالغ تقريباً يحمل مجموعة من البطاقات والكروت الشخصية، والتي قد حصل عليها بصفته شخص لديه صفة ومعاملات ومسؤوليات بمجرد بلوغه السن القانونية مثل: البطاقة المدنية، رخصة القيادة، بطاقة ائتمان أو أكثر، بطاقة تأمين طبي، بالإضافة إلى عدد من بطاقات العضوية وكروت المزايا لمنتجات وخدمات معينة. وتمثل كل من تلك البطاقات العلاقة المتفردة بين حاملها وبين مؤسسة حكومية، مؤسسة خدمات طبية، مؤسسة مالية أو أية جهة أخرى.

وفي حين أن اختراق بيانات العملاء يشكل تهديداً على هوياتهم المالية، إلا أنه من المهم أيضاً ملاحظة ما تحمله جميع البطاقات من خطر الإفصاح عن المعلومات الشخصية لصاحبها/ حاملها، والذي من الممكن أن يؤدي إلى سرقة هويته المالية.

على سبيل المثال، فقد تعرضت شركة Newkirk Products الأمريكية، والتي تصنع جميع أنواع البطاقات الشخصية، لاختراق المخدّمات servers الرئيسية للشركة، والتي تحوي البيانات الخاصة بعملاء الشركة من شركات التأمين وخلافه. وقد أظهرت نتائج التحليل الجنائي أنه مع عدم تمكن الجناة من سرقة أرقام الضمان الاجتماعي الخاصة بالأشخاص التابعين لتلك الشركات، إلا أنهم استطاعوا الحصول على جميع المعلومات التي تتم طباعتها على بطاقات العضوية/ الاشتراك الخاصة بتلك الخدمات مثل الاسم، العنوان، رقم بوليصة التأمين، وكذلك رقم المجموعة التي يتبعها الشخص في التأمين الجماعي، مما يمكنهم من استخدام/ بيع الهويات التأمينية لهؤلاء المشتركين على الإنترنت.

خطر مشاركة المعلومات على مواقع التواصل الاجتماعي

تُعد مواقع التواصل الاجتماعي من أكبر المخاطر التي قد تُعرض الشخص لسرقة معلومات هويته المالية، حيث أن العديد من الناس يسرفون في مشاركة بياناتهم الشخصية وتفاصيل حياتهم اليومية مع الآخرين، على سبيل المثال: تاريخ الميلاد، مواعيد السفر والإجازات، وكذلك الأماكن التي يقضون فيها إجازاتهم عند نشر صور تتضمن تحديداً للموقع الجغرافي Geotagging.

إن مشاركة جميع التفاصيل والمعلومات على مواقع التواصل الاجتماعي ونشر الصور والإفصاح عن معلومات السكن والعمل وأفراد الأسرة تُعتبر جميعها بمثابة دعوة لمرتكبي الجرائم الإلكترونية لسرقة المعلومات الخاصة بالهوية. كذلك، يسارع أغلب الناس للموافقة على الشروط والأحكام Terms and Conditions الخاصة بتلك المواقع، دون دراية بما تحتويه من بنود، وبغض النظر عما يحتويه الجزء الخاص بإعدادات الخصوصية Privacy settings من محتوى.

وعليه، يُنصح بشدة أن تتم قراءة تلك الشروط والأحكام بعناية بالغة من قبَل جميع أفراد الأسرة قبل التسجيل في مثل تلك المواقع، حيث أن كل شكل من أشكال المشاركة فيها سواء كان مشاركة الصورphoto sharing، التدوين blogging، أو إعادة التغريد retweetيعتبر بمثابة بصمة إلكترونية يتركها المشارك وراءه، وتزيد من فرصة تعرض بياناته وهويته للسرقة.

كذلك، يجب عدم التسرع في قبول طلبات الإضافة friend requests على تلك المواقع من أشخاص لا توجد بهم سابق معرفة، حيث أن عدد الحسابات المزيفة التي يتم اكتشافها على مواقع كـLinkedIn Facebookg Twitterg في ازدياد يوماً بعد يوم.

كيفية تجنب سرقة معلومات الهوية المالية

هناك بعض الخطوات الإيجابية والإجراءات الاحترازية التي ينبغي على كل شخص عملها لتجنب التعرض لسرقة معلومات هويته المالية، ومنها:

- عدم مشاركة معلومات/ بيانات شخصية مع أي شخص يقوم بطلبها عن طريق الهاتف، البريد الإلكتروني أو الإنترنت.
- عدم إعطاء الرقم المدني لأي شخص/ جهة إلا بعد معرفة الغرض من طلبه، وفيما سيتم استخدامه.
- التخلص الدوري من أية مستندات/ بطاقات هوية تحتوي على أية معلومات شخصية، فور انتهاء صلاحيتها/ الحاجة إليها، ويفضّل أن يتم ذلك عن طريق جهاز التقطيع المخصص لهذا الغرض shredder.
- إغلاق أية حسابات لمواقع على الإنترنت لا يتم استخدامها، حيث لا يوجد داعي لبقاء المعلومات الشخصية متوفرة على المخدمات الخاصة بتلك المواقع servers، والتي قد تكون عُرضة للاختراق.

- الحرص على الإلمام بالدورة المستندية لأية فواتير أوإيصالات يتم استلامها دورياً، وكذلك مواعيد استلامها (شهرية، ربع سنوية...الخ)، وذلك للاتصال بالمؤسسة المعنية التي تصدرها والتنبيه إذا لم تصل أي منها في موعدها.
- المراقبة الدورية والدقيقة لأية تقارير أو كشوف خاصة بالحسابات البنكية، البطاقات الائتمانية، والإبلاغ عن أية عمليات مشكوك في صحتها للبنك/ المؤسسة المالية فوراً.
- الحرص على حماية الحسابات البنكية وغيرها من الحسابات على الإنترنت بكلمة مرور Password قوية لا تسهل معرفتها، لا تقل عن ثمانية أحرف، وتحتوي على مزيج من الحروف الأبجدية والأرقام.
- استخدام برامج الحماية الخاصة بأجهزة الحاسب الآلي Firewall Software، وعمل التحديث المستمر لبرامج مكافحة الفيروسات Anti-virus and spyware software، وذلك لحماية تلك الأجهزة من الاختراق قدر المستطاع.

دولة الكويت: بعض الجرائم وعقوبتها في قانون جرائم تقنية المعلومات

ضمن جهود وزارة الداخلية لمحاربة الجرائم بجميع أنواعها وتطبيق القانون على الجميع، وفي خطوة تعد من الخطوات الهامة للقضاء على جرائم تقنية المعلومات، وبعدما لوحظ في الآونة الأخيرة من تجاوزات وجرائم يقوم بها البعض من خلال استخدام أجهزة الحاسب الآلي. أكدت وزارة الداخلية أنه سيتم العمل بقانون جرائم تقنية المعلومات بداية من يوم 2016/1/12، وذلك بعد ما تم نشره في الجريدة الرسمية بتاريخ 2015/7/7.

وفيما يلي بعض مواد القانون المشار إليه، على سبيل المثال وليس الحصر:

مادة (2)

الجريمة: الدخول غير المشروع إلى جهاز حاسب آلي أو نظام معلوماتي أو شبكة معلوماتية.
العقوبة: الحبس مدة لا تتجاوز ستة أشهر + غرامة (500 - 2000) دينار كويتي أو أحدهما.
الجريمة: إذا ترتب على الدخول إلغاء أو حذف أو تدمير أو تغير أو إعادة نشر بيانات أو معلومات.
العقوبة: الحبس مدة لا تتجاوز سنتين + الغرامة (2000 - 5000) دينار كويتي أو أحدهما.

إذا كانت البيانات أو المعلومات شخصية تكون العقوبة ثلاث سنوات حبس + غرامة (3000 - 10000) دينار كويتي او أحدهما.

مادة (3)

الجريمة: الدخول غير المشروع بقصد الحصول على بيانات أو معلومات حكومية سرية.
العقوبة: الحبس مدة لا تتجاوز (3) سنوات + الغرامة (3000 - 10000) دينار كويتي أو أحدهما.

إذا ترتب على الدخول إلغاء تلك البيانات او إتلافها أو تدميرها أو نشرها أو تعديلها تكون العقوبة الحبس مدة لا تتجاوز (10) سنوات + الغرامة (5000 - 20000) دينار كويتي أو أحدهما.

مادة (4)

الجريمة: إعاقة أو تعطيل الوصول إلى موقع، أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات عمداً
العقوبة: الحبس مدة لاتتجاوز سنتين + غرامة (2000 - 5000) دينار كويتي أو أحدهما.
الجريمة: الإدخال العمدي عن طريق الشبكة المعلوماتية أو باستخدام وسيلة من وسائل تقنية المعلومات ما من شأنه تعطيلها أو إيقافها عن العمل، أو دخول موقع لتغيير تصميمه او إلغائه أو تعديله أوإيقافه.
العقوبة: الحبس مدة لاتتجاوز سنتين + الغرامة (2000- 5000) دينار كويتي أو أحدهما.

مادة (5)

الجريمة: استخدام شبكة المعلومات أو وسيلة من وسائل تقنية المعلومات للوصول دون وجة حق إلى أرقام أو بيانات بطاقة ائتمانية أو مافي حكمه.
العقوبة: الحبس مدة لاتتجاوز سنة + غرامة (1000- 3000) دينار كويتي.

وتكون العقوبة الحبس لمدة لاتتجاوز (3) سنوات + غرامة (3000 -10000) دينار كويتي أو أحدهما إذا ترتب على ذلك الحصول على أموال الغير أو على ما تنتجة من خدمات.

هذا، ويمكن الاطلاع على القانون كاملاً من خلال الرابط التالي:

https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf

المصادر

الموقع الإلكتروني

Identity Theft Resource Center

https://www.idtheftcenter.org

الموقع الإلكتروني لوزارة الداخلية بدولة الكويت

https://www.moi.gov.kw

معهد الدراسات المصرفية

INSTITUTE OF BANKING STUDIES

ص.ب: 1080 الصفاة - 13011 الكويت

P.O.Box 1080 Safat 13011 Kuwait

تلفون: 22901100 965+ - فاكس: 22466430 965+

البريد الإلكتروني: cs@kibs.edu.kw - www.kibs.edu.kw

ibs_kuwait IBSKuwait