

شورر تكنولوجيا



الإنترنت عالم مفتوح من حولنا من السهل جداً فيه الوصول لأي شخص والحديث معه وربما الاطلاع على بياناته وأسراره، لكن لا يفعل ذلك إلا لصوص الإنترنت والمتطفلون، وأسرارنا وبياناتنا الموجودة على أجهزة الحاسب الآلي والهاتف المتحرك الذي أصبح متصلاً بالإنترنت طوال الوقت أصبحت أيضاً معرضة للسرقة والاطلاع عليها من قبل بعض الفنيين في مراكز الصيانة حيث يتلصص بعضهم على أسرار العملاء عند ترك الأجهزة في تلك المراكز التي لا يكون أغلبها معتمداً وبالتالي يفعلون ما يشاؤون في أجهزتنا من دون أن نعرف . والسؤال: كيف نتقي شر هذا العالم المفتوح ونحمي أنفسنا منه، خاصة أن عدم الحماية من الممكن أن يعرضنا لمشكلات وكوارث كبيرة تؤدي إلى هدم بيوت بأكملها؟

ضعاف النفوس يستغلون الإهمال

"أسرارنا في" الصيانة

من دون أن ندري تتعرض أسرارنا وبياناتنا على أجهزة الكمبيوتر أو الهاتف المتحرك للعبث، سواء كان ذلك من خلال تركها في مراكز الصيانة أو بيعها، ففي حال بيعها يتمكن البعض من استعادة المحذوفات بطرق عدة تمكنه من كشف كل الصور والبيانات الخاصة بنا وبالتالي من الممكن أن نتعرض لأضرار ومشكلات نحن في غنى عنها تأتي أيضاً من بعض المتطفلين في مراكز الصيانة .

كيف نتفادى العبث بأسرارنا هذه سواء عند اللجوء لمراكز الصيانة أو بيع الأجهزة لأشخاص لا نعرفهم، وهل تحويلها لنفايات أفضل من بيعها حتى لا نتعرض للأذى .

يقول إبراهيم عبدالسلام، صاحب مركز لصيانة أجهزة الكمبيوتر بالشارقة: هناك الكثير من الأجهزة التي تأتي إلينا للتعامل معها وصيانتها من فئات عمرية مختلفة، خاصة من الفتيات والنساء والشباب، وبالتأكيد سيكون فيها الكثير من الصور والبيانات الخاصة بهم ونراعي ذلك دائماً في عملنا الحرص على سريتها دائماً .

ويضيف: نعتبر أسرار وبيانات العملاء على أجهزة الكمبيوتر بمثابة أمانة لا ينبغي أن نطلع عليها ويجب المحافظة عليها . في حين أن هناك كثيراً من المتلصصين يرغبون في الاطلاع عليها في كثير من مراكز الصيانة

ويرى عبد السلام أن الأفضل أن يحتفظ أصحاب أجهزة الكمبيوتر الشخصي بكل ما يهمهم من معلومات على أقراص خارجية حتى لا تكون أسرارهم عرضة للسرقة أو الاطلاع عليها من قبل الآخرين سواء في مراكز الصيانة أو في حالة فقدانهم لأجهزتهم لأي سبب كان .

ويؤكد أن كثيراً من المستخدمين لأجهزة الكمبيوتر والهاتف المتحرك أصبحوا على دراية بهذا الأمر بعد الكشف عن جرائم كثيرة بخصوص هذا الشأن أغلبها بغرض التلصص على معلومات وصور شخصية للعملاء وهو أمر غير مقبول .

يتفق مع الرأي السابق بشير عبد الملك، متخصص في صيانة أجهزة الحاسب الآلي بالشارقة، ويقول: عملي يتمثل في صيانة الكمبيوتر وبالتالي تأتي إلينا كثير من الأجهزة عليها صور للعملاء، لكن نحرص دائماً على عدم فتحها بأي طريقة . كانت حتى لا نخون الأمانة

ويضيف: لا أنكر أن هناك من يسعى للتعرف إلى ما بداخل الأجهزة ومن الممكن أيضاً أن يحصل على نسخ منها كنوع من التطفل أو الاستخدام السيئ لها ولكن هذا نادر ويوقع فاعله تحت طائلة القانون والمساءلة .

وبالنسبة لتحويل الأجهزة الإلكترونية في حال عدم التمكن من إصلاح بعض عيوبها لنفايات وتركها مهملة بالمنزل حتى لا يستغلها البعض، يوضح أن هذه الطريقة ليست بالأفضل حتى لا نخسر قيمة الجهاز عند بيعه بمبلغ معقول نستكملة لشراء جهاز أفضل، إضافة إلى أن المتلصص لن يشغل باله بجهاز لا يمكن أن يستعمل ثانية، بل سيستخدم أجزاء منه . كقطع غيار .

ويوضح عبد الملك أن هناك بعض المحال غير المرخصة لصيانة الهواتف وبالتالي تصبح أكثر خطراً على البيانات لأن من فيها يعمل في الخفاء من دون معرفة الجهات المسؤولة وبالتالي فبعضهم قد ينسخ الأسماء والصور والمعلومات

. بمجرد اتصال الهاتف بجهاز الصيانة من دون علم العميل

ويقول كمال عزيز، متخصص في صيانة الحاسب الآلي بأحد مراكز الصيانة بشركة أكسيوم: من الممكن أن يحدث سوء استخدام من قبل فني الصيانة للمعلومات المهمة ولذا يجب أخذ نسخة احتياطية كاملة من الهاتف الذكي أو الكمبيوتر على قرص صلب خارجي وإعادة تهيئة الهاتف أو جهاز الكمبيوتر، ومسح محتوياته بالكامل، ومن ثم تقديمه للفني، أو طلب الصيانة في وجود العميل وهذا بالتأكيد أفضل وسيلة للحماية

ويضيف: مراكز الصيانة الكبرى والمتخصصة في الشركات المعتمدة يجب أن يثق بها العملاء لأن من يعملون بها هم أهل ثقة ويعملون تحت إشراف جهات متخصصة هي بالأساس شركات لها سمعتها في الأسواق وبالتالي ليس من السهل أن يقوم الفنيون فيها بالتلصص على بيانات وصور العملاء

ويقول وليد عبد الستار مدرس حاسب آلي بمنطقة عجمان التعليمية ومتخصص في الصيانة: الأمر شائك جداً في الوقت الحالي بسبب انتشار مراكز الصيانة من دون معرفة الأفضل والأكثر أمناً بينها . ويوضح أن هناك طرقاً عدة يمكن من خلالها حماية أسرارنا على الحاسب الآلي أو الهاتف ومن أهمها عدم وضع صور شخصية عليها بل حفظها في وسائل تخزين خارجية أو وضع الصور المهمة داخل برامج لا يمكن أن تفتح إلا عن طريق رقم سري وبالتالي . يصعب على أي شخص فتح هذه الملفات

سيف الطنجي، طالب بكلية القانون بجامعة الشارقة، يقول: من رابع المستحيلات أن أترك جهازي الشخصي أو الهاتف المتحرك في مراكز الصيانة من دون أن أفق بجوار المسؤول عن الصيانة لمراقبة ما يقوم به فقد تعرضت من قبل لمسح صور كثيرة على جهازي معظمها لأهلي ولا أدري هل اطلع عليها أم لا

ويضيف: في الوقت الحالي لا أحفظ أي بيانات خاصة بي أو بالمقربين في الكمبيوتر، بل على قطعة خارجية لأنها الأضمن كي لا أقع تحت الخوف من العبث بها في حال تصليح الجهاز أو بيعه أو حتى رؤية أصدقائي في الجامعة له

وعن بيعه للأجهزة الإلكترونية الخاصة به بعد فترة من الاستعمال، يقول: لست من هواة ذلك، فعندما تظهر أنواع أحدث من الأجهزة سواء الحواسيب أو الهواتف، أترك القديم لأحد أقاربي الصغار بعد إعادة ضبط المصنع له وأقوم بشراء الجهاز الجديد لكن مسألة البيع غير واردة عندي في هذا المجال

ويقول سراج الرشيد، موظف مبيعات بشركة لامترا العقارية بدبي: في حال وجود عطل بجهاز الكمبيوتر الخاص بي أذهب إلى متخصص من زملائي في الشركة بشكل ودي لتصليح الجهاز بدل الذهاب لمراكز الصيانة حتى لو كان الأمر كبيراً فالأهون عندي شراء جهاز جديد بدلاً من ترك أسراري متاحة للجميع

ويضيف: تعرضت من قبل لموقف جعلني أقرر عدم الذهاب لهذه المراكز حيث اكتشفت مصادفة أثناء ذهابي للسؤال عن الجهاز أن الفني الذي يقوم بتصليحه ينسخ الصور الموجودة عليه على اسطوانات خاصة به فقامت بإبلاغ الشرطة على الفور وحضرت واتخذت الاجراءات اللازمة

من جانبه يقول المتخصص الاجتماعي إبراهيم عبيد إن الشخص الذي يتلصص على بيانات وأسرار الآخرين بأية طريقة غير سوي يسعى دوماً لمعرفة أسرار غيره، سواء كان ذلك متاحاً أمامه أو غير متاح

ويوضح أن المجتمع يرفض مثل هذه الصفات، وأن ما يقوم به البعض في مراكز الصيانة الخاصة بالأجهزة الإلكترونية عبث بأسرارنا ما يستوجب توضيح قوانين الحماية وتفعيلها بخاصة أن هناك بعض الأشخاص لا يعرفون ذلك ويتركون أسرارهم بصدق نوايا ولا يعلمون ماذا يحدث لها .

ويشير عبيد إلى أنه في الوقت الحالي الذي انتشر فيه الإنترنت ووسائل الاتصال المتنوعة بات من السهل الوصول إلى بيانات المستخدمين حتى ولو لم يذهبوا إلى مراكز صيانة لذا يجب على الجميع عدم ترك أسرار أو صور يمكن أن تسبب له مشكلات فيما بعد في حال تعرضها للسرقة .

ويقول الداعية الإسلامي فضيلة الشيخ نشوان العابد إن الإسلام يرفض اطلاع المتخصصين في الصيانة أو غيرهم على أسرار الآخرين لأنها أمانة وكلت إليهم وبالتالي يجب أن يحافظوا عليها ولا يكشفوها لأنفسهم أو لغيرهم . ويضيف: اطلاع المتخصصين في تصليح الأجهزة الإلكترونية على ما تحويه من أسرار شخصية للعملاء ذنب يعاقب عليه مرتكبوه .

ومن الأفضل عدم الاحتفاظ بأي بيانات شخصية، بخاصة الصور والمواد الفيلمية، على أجهزتنا الإلكترونية في حال بيعها أو إرسالها لمراكز الصيانة لأن ضعف النفوس يستغلون ذلك لمصلحتهم ويسببون الضرر لغيرهم .

يغلب عليها التشهير والسب والقذف

الابتزاز الإلكتروني قضية عالمية

باتت قضايا الابتزاز الإلكتروني تمثل تحدياً كبيراً يتعلق بخصوصياتنا نظراً لما يمكن أن نتعرض له من سرقة لأسرارنا من قبل متطفلين ومن ثم تهديدنا فيما بعد وطلب دفع مقابل مادي حتى تعود الصور أو البيانات إلينا أو التشهير بنا وهو . ما يجعلنا حريصين جداً في التعامل مع الإنترنت

وعلى المستوى العالمي، ازدادت هذه القضايا خاصة في الولايات المتحدة الأمريكية وأوروبا، رغم القوانين الصارمة التي تمنع ذلك أما في العالم العربي فباتت أروقة المحاكم مليئة بمثل هذه النوعية من القضايا، التي يقع فيها كثير من الضحايا وأكثر أنواع قضايا الابتزاز هي سرقة صور وبيانات الآخرين والمساومة عليها مقابل مبالغ كبيرة



مع زيادة عدد مستخدمي مواقع التواصل في العالم العربي، انتشرت مثل هذه القضايا التي يكون معظم المتهمين فيها شباباً والضحايا هم من الفتيات ممن يضعن صوراً لهن على أجهزتهن أو حساباتهن الشخصية على مواقع التواصل . ويقعن ضحية لهؤلاء من منعدمي الضمير

وفي الإمارات توجد كثير من قضايا الابتزاز أغلبها يتمثل في طلب أموال مقابل عدم نشر صور خاصة بالضحية تم التقاطها برضا منها أو عنوة حيث يلجأ المتهم لطلب أموال مقابل عدم نشرها وفي حال إبلاغ الجهات المختصة تقوم . بتتبع الجاني والضحية حتى تتمكن من تجميع خيوط القضية ومن ثم تقديم المتهم أو الجاني للمحاكمة

ومؤخراً اتهمت نيابة دبي موظفاً بنشر صور لسيدة ومطالبتها بمبلغ مليون دولار مقابل وقف هذا النشر، وكان ذلك بسبب وجود خلافات مادية بين زوجها والجاني فقام المتهم بتصويرها من دون علمها في أكثر من مكان وهددها بنشر الصور حتى يرضخ زوجها الذي قام بإبلاغ الشرطة .

هذه قضية في الإمارات ولكن على مستوى العالم توجد آلاف القضايا من هذا النوع، ففي الولايات المتحدة الأمريكية نشر أحد المواقع الإخبارية عن لجوء أمريكي لنشر صور خاصة بزوجته إن لم ترضخ لطلباته وتدفع له أموالاً

ولا تتعلق قضايا الابتزاز بنشر صور لآخرين ومطالبتهم بأموال مقابل وقف النشر أو عدم نشرها من الأساس، بل هناك قضايا السب والقذف وغيرها من القضايا في هذا الشأن التي باتت تورق المجتمعات وتؤثر بالسلب في الأجيال الجديدة خاصة من مستخدمي مواقع التواصل الاجتماعي .

ويقول محمد الرياف، المدير التنفيذي لشؤون تطوير التكنولوجيا في برنامج طوارئ الحاسب الآلي: خصوصياتنا في الوقت الحالي باتت على المحك وضعيفة مقارنة بالماضي ويرجع ذلك لأسباب عدة أهمها ارتفاع عدد مستخدمي التواصل الاجتماعي حيث يضع أغلب المشتركين صوراً شخصية لهم ولذويهم وبالتالي تكون عرضة للسرقة حتى من قبل الأصدقاء إذ من الممكن أن يتلصص البعض عليها أو ينقلوها لحسابات وهمية بغرض الابتزاز للطرف الآخر في حال وجود خلاف بينهم .

ويضيف: من الأفضل عدم وضع صور شخصية مهمة على مواقع التواصل الاجتماعي ومراعاة الأصدقاء المضامين ودرجة القرب منهم وكذلك وضع برامج حماية على أجهزة الحاسوب الشخصي حتى لا تكون عرضة للسرقة من قبل المتلصصين على شبكة الانترنت .

ويوضح أن مثل هذه القضايا أصبحت تلامس واقعنا في الوقت الحالي كثيراً بسبب انعدام الوازع الديني لدى كثير من الشباب الذين يستخدمون الإنترنت ومواقع التواصل في أشياء لا تفيدهم وبالتالي يكون ذلك خطراً على مستقبلهم سواء كان الدراسي أو الشخصي .

ويطالب الرياف بمعاينة من يبتزون الآخرين على الانترنت بأشد العقوبات حتى يكون ذلك رادعاً لغيرهم ممن يفكرون في القيام بمثل هذه الأمور وحتى لا تتكرر مرة أخرى وبالتالي يكون العقاب جزءاً من حل المشكلة التي من الممكن أن تؤدي إلى تدمير أسر بأكملها .

ويقول فريد فريدوني، نائب رئيس الأعمال التجارية في شركة #187;دو#171;: دائماً ما ننصح العملاء بضرورة حماية بياناتهم وأسرارهم على أجهزة الكمبيوتر حتى لا يكونوا عرضة لأي عملية اختراق أو سرقة قد تعرضهم فيما بعد إلى أضرار كبيرة يمكن أن تنغص عليهم حياتهم .

ويضيف: مهمتنا في الشركة مساعدة الجهات المختصة في الوصول إلى مرتكبي الجرائم من خلال تزويدهم بالمعلومات المطلوبة وهذا بالطبع لا يتم إلا من خلال إجراءات قانونية سليمة للحفاظ على بيانات وأسرار عملائنا وكل شركات الاتصال على مستوى العالم تقوم بذلك .

ويوضح أن الشرطة وجهات التحقيق لها أساليبها الخاصة في الوصول إلى الجناة الحقيقيين وتقديمهم للمحاكمة، فإن دور شركات الاتصال يقتصر على مساعدة هذه الجهات في حال طلبها أي معلومة .

ويقول جمال العمدة، مهندس اتصالات بشركة #187;سوفت ناشونال#171; للبرمجة: هناك الكثير من البرامج التي يمكن أن نعتمد عليها حتى نحمي أنفسنا من سرقة أسرارنا على الكمبيوتر أو الهاتف المتحرك في الوقت الذي انتشرت فيه الهواتف الذكية التي تكون متصلة دائماً بالانترنت

ويشير إلى أن هذه البرامج متاحة على كثير من المواقع المتخصصة وأغلبها مجاني وبالتالي لا توجد عقبة في الحماية، لكن هناك طرقاً أخرى للابتزاز يمكن أن تحدث وهي أن يشهر شخص ما بنا على الانترنت أو ينشر معلومات وصوراً مفبركة عنا وهذه جريمة يجب إبلاغ الشرطة عنها على الفور حتى نتجنب تفاقم المشكلة

ويؤكد العمدة أن عالم الانترنت فضاء مفتوح للجميع من دون وجود رقابة ومسؤولية من البعض وهو ما يجعل وجود مثل هذه القضايا منتشراً بين كثير من المستخدمين خاصة ممن يستخدمون مواقع مرفوضة، وهو ما يعرضهم للمساءلة بجانب اختراق لأجهزتهم وبالتالي مشكلات أخرى هم في غنى عنها

ويقول محمد الشامسي، مهندس متخصص في البرمجيات: هناك أساليب أخرى كثيرة للابتزاز بعيدة عن قضايا التشهير والسب والقذف من بينها سرقة البريد الإلكتروني ومحاولة طلب أموال نظير استرجاعه أو سرقة البيانات الموجودة عليه ومخاطبة الأصدقاء بضرورة إرسال الأموال لأن صاحب البريد الإلكتروني في محنة

ويضيف: تعرضت لمثل هذه السرقة من قبل وابتز اللص اصداقائي وطلب منهم إرسال أموال لأنني في محنة وأريدها على الفور وأحد المقربين اكتشف الأمر واتصل بي واسترجعت البريد من خلال بعض الطرق التي نتعامل بها في عملنا

ويؤكد الداعية الإسلامي إبراهيم اليوسف أن الدين الإسلامي حرم مثل هذه الأمور التي تدخل في نطاق السرقة وبالتالي يطبق على مرتكبها الحد لأنه قام بالحصول على حقوق غيره من دون وجه حق

ويضيف: أغلب هذه القضايا يقوم بها شباب في سن المراهقة أو كبار فقدوا الوازع الديني ويسعون لخراب المجتمع وبالتالي يجب معاقبتهم أشد عقاب حتى يكونوا عبرة لغيرهم، ووسائل التواصل الحديثة هي التي سهلت ذلك

ويطالب الشباب والفتيات بعدم نشر صور أو معلومات خاصة بهم على شبكة الانترنت، خاصة مواقع التواصل الاجتماعي، لأنها أكبر مكان من الممكن فيه سرقة أسرارنا من دون أن نشعر ويعرضنا ذلك فيما بعد لكثير من المشكلات نحن في غنى عنها

قوانين الدولة تحمي

يرى المستشار القانوني يوسف الشريف أن الحصول على الدليل في معظم الجرائم الإلكترونية بات سهلاً في الوقت الحالي، خصوصاً في جرائم السب والقذف، لكن معظم جرائم القرصنة والسطو على البيانات يصعب الوصول إلى من قاموا بها لأنهم يستخدمون أساليب خداع عدة في سرقة الضحية سواء كانت مؤسسة كبرى أو أفراداً

ويشير إلى أن شركات الاتصالات في مختلف دول العالم تعمل على وضع كل أرقام الأجهزة الإلكترونية التي تعمل في نطاق تردها على خوادم خاصة من خلال قواعد بيانات كبيرة يمكن أن تكشف المراسلات بين الأجهزة ومن هنا يمكن أن يسترجعوا أيّاً من بيانات المستخدمين بأمر من الجهات المختصة لكن ذلك لا يحدث إلا في الجرائم التي تصل إلى

وعن العقوبات التي تطال من يبتزون الآخرين عن طريق الإنترنت يقول: تصل العقوبات في جريمة السب والقذف، وهي من جرائم الابتزاز، إلى السجن لعامين أو أكثر وكذلك غرامة مالية أما من يسرقون بيانات المستخدمين وصورهم، ويشهرون فعقوبتهم تصل إلى 5 سنوات

ويوضح أن القوانين الموجودة في الدولة تعد من القوانين الرادعة في هذا الشأن ويتم تطبيقها على المخالفين وبالتالي . تقل نسبة الجرائم من هذا النوع، مؤكداً أنه إذا ظهرت جرائم من وقت إلى آخر فهي قليلة مقارنة بدول أخرى

السحابة الإلكترونية و"الهارد الخارجي" مساحات وقاية

مع انتشار جرائم سرقة بيانات وصور المستخدمين على شبكة الإنترنت وكذلك عند تركها في مراكز الصيانة بات هذا الأمر شائعاً بالنسبة إلى كثيرين ممن لا يستطيعون الاستغناء عن معلومات خاصة بهم على أجهزتهم الإلكترونية . لذلك ظهرت بعض الطرائق والحيل لتكون طوق النجاة لهؤلاء، فقد أقدمت الشركات العالمية المتخصصة في مجال الكمبيوتر على ترك مساحات تخزينية على خوادمها الخاصة على شبكة الإنترنت بسعة تخزين عالية تبدأ من 5 غيغا . حتى يمكن للمستخدمين حفظ بياناتهم عليها في أي وقت واسترجاعها على أجهزتهم



وهذه الطريقة هي الأفضل لحماية بياناتنا من السرقة أو الاطلاع عليها في حال ترك أجهزة الكمبيوتر في مراكز الصيانة . أو حتى عندما يرغب البعض في الاطلاع على الجهاز في أي مكان بحيث يشاهد صوراً لا نرغب في رؤيته لها

ومع انتشار الإنترنت في كل مكان وسهولة الدخول إليه سواء عبر الكمبيوتر وبسرعات عالية، بات من السهل علينا حفظ الصور والبيانات على خوادم هذه الشركات، خاصة أنها مؤمنة بشكل كبير ومن الصعب والنادر جداً اختراقها أو سرقتها، وبالتالي هي أفضل وسيلة حتى الآن بجانب وضع معلوماتنا الشخصية على قرص صلب خارجي بعيداً عن جهاز الكمبيوتر الخاص بنا .

ولأنه من السهل جداً في هذا العالم المفتوح أن تسرق أسرارنا على أجهزة الكمبيوتر أو الهاتف المتحرك من دون أن ندري لأنها متصلة طوال اليوم بالإنترنت، علينا عدم وضع أي أشياء مهمة عليها إلا بعد التأكد من وضع حماية كافية لها .

وكما يقول محمد السيد، مهندس بشركة العربية للعود، إن حماية الأسرار الشخصية والبيانات الموجودة على أجهزتنا أمر يؤرق الجميع، خاصة مع انتشار لصوص الإنترنت في الوقت الذي تتصل فيه أجهزتنا الإلكترونية طوال اليوم بالشبكة .

ويضيف: يجب أن نضع في البداية برامج حماية قوية على الأجهزة وألا نتعامل مع المواقع المشبوهة التي تضع لنا فيروسات على الروابط التي ترسلها إلينا، لأنها فخ يقع فيه كثيرون بعد إيهامهم بأن هذا الرابط عليه وصلات لمواقع هدايا

. مجانية أو عروض وهمية، وبالتالي نكون عرضة لسرقة بياناتنا ونحن راضون تماماً



ويشير إلى أن برامج #187; السحابة الإلكترونية #171; هي الأفضل حتى الآن بجانب القرص الصلب الخارجي الذي يستخدم في حال رغبتنا في الاطلاع على صور أو أي مادة على الكمبيوتر، فمن الممكن أن نوقف الاتصال بالإنترنت نهائياً في حال مشاهدتها وبالتالي تعد إحدى وسائل الحماية

ويقول د . فادي علول، الأستاذ بكلية الهندسة بالجامعة الأمريكية بالشارقة، إن كثيراً من الدراسات والأبحاث أثبتت تعرض معظم الأجهزة الإلكترونية المتصلة بشبكة الإنترنت للاختراق من قبل المتلصقين أو القراصنة ومساومة أصحابها مقابل الحصول على أموال . ويضيف: من أكثر القضايا في هذا المجال سرقة البريد الإلكتروني، ولذا يجب علينا وضع كلمة سر قوية وتغييرها من وقت لآخر وعدم فتح البريد الإلكتروني من أكثر من مكان حتى لا نكون عرضة للمهاجمين من لصوص الإنترنت

وبالنسبة إلى البيانات المحفوظة على أجهزة الحاسب الآلي أو الهاتف المتحرك، فهناك وسائل كثيرة جداً لحمايتها ومن بينها وضع المواد كلها على قرص صلب خارجي أو من خلال حفظها على #187; السحابة الإلكترونية #171; التي توفرها الشركات العالمية مثل #187; أبل #171; و #187; مايكروسوفت #171; و #187; غوغل #171;، وكلها شركات كبرى في عالم الإنترنت ومعروف عنها قدرتها على حماية قواعد البيانات الخاصة بها، ولكن أفضل عدم اللجوء إلى مثل هذا الأمر إلا في حال عدم وجود قرص خارجي يمكن أن نحفظ عليه المواد الخاصة بنا على جهاز الحاسب الآلي

ويقول المدون داود محمد: إن وجود برامج حديثة تتعامل معها الشركات لخدمة المستخدمين كحفظ المعلومات على السحب الإلكترونية والتخزين على الإنترنت من أجل استرجاع البيانات في أي وقت أمر مطلوب لحماية أسرارنا ولكن بشروط، فرغم أهمية تلك الخدمة وسرعة استجابتها، فإنها اصطدمت ببعض التصرفات الخاطئة مثل ذهاب البعض إلى المحال التجارية التي تزعم تركيب برامج وتضع بريداً إلكترونياً كاسم مستخدم وكلمة مرور موحدة لجميع الزبائن، وكذلك يجب الحذر من ذلك حتى لا نقع في هذا الفخ

ويضيف: استخدام خدمة #187; السحابة الإلكترونية #171; في حالة كان البريد هو نفسه المخصص للبرامج يعني تزامن البيانات الموجودة في الأجهزة بين كل من يستخدم اسم المستخدم ذاته، لذلك من الأفضل التسجيل الخاص وتنزيل البرامج مرة أخرى باسم المستخدم الجديد، فهذا يضمن الخصوصية وطريقة إنشاء حساب جديد سهلة جداً . ويوجد لها العديد من الشروح على الإنترنت بالفيديو والصور

ويتفق معه عمرو شعيب، صاحب محال لصيانة أجهزة الكمبيوتر بالشارقة، قائلاً: حماية أسرار العملاء هي بالتأكيد هدفنا في حال تركهم لأجهزتهم للصيانة، لكن على شبكة الإنترنت لا نستطيع أن نحميها، بل نقدم لهم النصائح المطلوبة

ويضيف: لا نختلف على أننا أصبحنا في عالم مفتوح في كل شيء، خاصة الإنترنت، وبالتالي من السهل جداً أن يقتحم كثير من اللصوص أجهزتنا ويطلعون عليها، وهنا نحن نقف أمام تحد كبير، وهو كيفية حماية أسرارنا الموجودة على الأجهزة الإلكترونية

ويوضح أن طرائق الحماية كثيرة ومتعددة، لكن يجب أن نأخذ الحيطة والحذر دائماً، لأن القرصنة دائماً يسعون لتطويع أنفسهم وكشف ما تقوم به الشركات الكبرى التي دخلت في حرب كبيرة معهم في هذا الشأن وفي النهاية يكون المستخدمون هم الضحايا، لذا يجب التأكد دائماً من برامج الحماية وتغيير كلمات السر بشكل دوري.

ويقول راشد المنصوري، طالب في كلية التقنية بدبي ومتخصص في برمجة الحاسب الآلي، إنه بمجرد بداية الجهاز الاتصال بالإنترنت يصبح من السهل على أي من المتطفلين اختراقه ومعرفة بياناته، وذلك في حال الدخول على مواقع مشبوهة أو التواصل مع أشخاص غير معروفين وقبول صور أو ملفات منهم.

ويضيف: أسلوب الحماية يتمثل في أمرين، هما حفظ كل البيانات الشخصية على قرص صلب خارجي، وعند الرغبة في الاطلاع عليها يجب فصل الجهاز عن الإنترنت، والأمر الثاني تغيير كلمات السر من وقت لآخر ووضع كلمات معقدة جداً، وبالتالي تكون الحماية بسيطة جداً ولا تكلفنا الكثير.