

أصبح الاتصال بالإنترنت أمرا غريزيا، ومع كل اتصال جديد تكشف جانبا من أسرارنا دون علم منا، فالرغبة في الخصوصية عبر مواقع التواصل، تشبه رغبة أحدهم في السير تحت المطر دون بلل. ويكشف فيلم “اختراق الخصوصية” الذي بثته الجزيرة الوثائقية ضمن سلسلة “نظرة على” كثيرا من أسرار اختراق الخصوصية عبر الإنترنت، حتى لأولئك الذين يظنون أنهم مطلعون على الجرائم الإلكترونية، فكم هو سهل التعرض للخداع عبر الإنترنت، خصوصا أننا نحن من نجعل أنفسنا ضحايا بإساءة استخدام الإنترنت. ويحاول الفيلم تقريبا أكثر من الواقع، وإفهامنا ما يجري حولنا، بالإضافة إلى بصمات أصابعك، ما هو الشيء الفريد والثابت الذي يرافقك منذ ولادتك وحتى مماتك؟ إنه ليس اسمك ولا تاريخ ميلادك، بل هوية التسجيل الوطنية التي تُعرفك كمواطن في دولة ما، وهي سلسلة حروف وأرقام لا يملكها أي شخص آخر، فكل حرف أو رقم له دلالة معينة؛ كسنة ميلادك ورقم تسجيلك في السجلات، إضافة إلى خوارزميات سرية تُحدد بعضا من هذه الأرقام. واليوم، لا تُستخدم هوية التسجيل الوطنية في الخدمات الحكومية والمعاملات التجارية فحسب، بل تفتح أبواب المكاتب الإدارية، وبيانات التأمين، في الأعوام الماضية، سُجلت حوادث لانتهاك الهوية الوطنية، ورغم قلة عددها، وأقنعتهم أنها صاحبة الهوية الحقيقية. وفي قصة ثالثة، استخدم رجل معلومات مجموعة من المشتركين في إحدى الفعاليات تتضمن أرقام هوياتهم الوطنية، من أجل شراء خطوط اتصال والحصول على هواتف محمولة. ونظرا لكل هذه الاحتمال والقصص فقد قررت دولة سنغافورة منع المنظمات أو الأماكن - كمُتاجر بيع التجزئة والوحدات السكنية - من جمع أو استخدام أو كشف أرقام الهويات الوطنية. وإضافة إلى المعلومات التي تكشفها الهويات الوطنية، فهناك معلومات أخرى يمكن أيضا كشفها عن طريق بطاقات العمل التي نتركها في المطاعم أو المؤتمرات وغيرها مقابل كوب مجاني من الشاي، “المصادر المفتوحة”. نافذة استخباراتية تدخل الآخرين في حياتنا وبمجرد أن قابل “جوشوا ليم”، ونوع حذائه، وكثير غير ذلك كالألعاب التي يُحبها، وأين قضى شهر العسل. وقد استقى “تشينغ لاي كي” كل هذه المعلومات من حسابات “جوشوا ليم” على مواقع التواصل الاجتماعي، في عملية لم تستغرق أكثر من 8 ساعات، أي جمع المعلومات المتاحة عن أي فرد عبر الشبكة المفتوحة. ومع إقرار “تشينغ لاي كي” أن استخدام “المصادر المفتوحة” بشكل فاعل يحتاج إلى مهارات وأدوات، فقد تعرّف مثلا على نوع حاسوب “جوشوا ليم” من صورة نشرها له بعد شرائه، صور الهاتف. ويعرف موقع هاتفك. ويضيف أن مزيدا من الوقت يُمكنه من معرفة مكان الإقامة بالضبط من خلال ما يظهر في الصور من مبانٍ ومعالم. وحتى إذا لم يكن الشخص من المشاهير، فقد يكون على صلة بأحدهم، ولهذا يستهدفه المهاجم للوصول إلى هذه المشهور. وقد نلتقطها في العمل أو الأماكن العامة، رغم أنها قد تظهر أوراقا منثورة أو حاسوبا مفتوحا أو بيانات خاصة وغير ذلك. فمواقع التواصل الاجتماعي. يستخدم 40% من سكان العالم وسائل التواصل الاجتماعي، ولكل شهرة ثمن. فمثلا هناك 120 مليوناً يتابعون حساب النجمة “كيم كارداشيان” على إنستغرام ويشاهدون تفاصيل حياتها، وكان ذلك السبب الذي أدخلها في وضع مُعقّد؛ فقد تعرضت في عام 2016 للسرقة تحت تهديد السلاح في باريس، بعد أن علم اللصوص أنها كانت في الفندق بمفردها، وبحوزتها مجوهرات بقيمة 10 ملايين دولار، وكل ذلك من خلال ملاحظتها على مواقع التواصل. ومنذ ذلك الحين وقع أكثر من 24 عملية سطو في لوس أنجلوس، عادة ما كان يُخطط لها عبر متابعة المشاهير بانتظام عبر مواقع التواصل. والمُوزع الموسيقي “جوكيم غوميز” مثال جيد على المستخدمين النشطين لوسائل التواصل، فهو ينشر كل ما يقوم به على إنستغرام، ويُشارك جوانب مختلفة من حياته مع 60 ألف متابع على مواقع فيسبوك وإنستغرام وتويتر. ونوع هاتفه ودراجته، وتصميم منزله، حتى لا يكون عرضة للسرقة. ولاحقا أصبح “جوكيم غوميز” لا يؤمن بالخصوصية على وسائل التواصل، ففي كل مرة تنشر فيها، سياسة الخصوصية. حين تُثبت تطبيقا على هاتفك أو حاسوبك وتفتحه للمرة الأولى، وبالطبع، فلدى كل منا عشرات التطبيقات على هواتفنا، وتشرح سياسة الخصوصية كيفية جمع واستخدام التطبيق لمعلوماتك، لكن الجزء الأصعب يتمثل فيما تعنيه. فما الذي أتخلى عنه حينما أوافق على هذه الشروط والأحكام؟ وهل الأمر سيئ حقا؟ يقول المحامي “ليونيل تان” - الذي يساعد الشركات على صياغة سياسة الخصوصية - إن بنود الخصوصية تنص ظاهريا على أنهم قد يُرسلون معلوماتك إلى شركات الإعلان أو الفاعليات لتحسين خدماتهم التي يُقدمونها إليك. إذا كانت مشاركة معلوماتك مع الجهات الأخرى ضرورية لتزويدك بالبيانات، فهم مُخولون لأن يقولوا إن الخدمات لن تكون متاحة لك إن لم تزودهم بموافقتك، شبكات الاتصال المجانية هناك تعليق يقول: “إذا لم تدفع، ويمكن ملاحظة مدى صحة هذا التعليق بالنسبة لبعض التطبيقات المجانية، وكذلك شبكات الاتصال المجانية التي نبحث عنها في المقاهي. الخبير في شركة “تشيك بوينت” - وهي شركة عالمية تُطوّر تقنيات لحماية المنظمات ضد هجمات الجرائم الإلكترونية - إن هناك تقنية تتيح لأي شخص اختيار أي اسم يريد لشبكة اتصال لاسلكية؛ ومن ثم فإن كنت في هذا المكان، وهنا يستطيع مُزوّد الخدمة الاطلاع على كل

ما تفعله عبر متصفح الإنترنت. وتحميل نسخة منها، وتعديلها عبر ما يُعرف بـ "هجوم الوسيط"؛ وحالما تتصل بها يتمكن المخترق من رؤية أي كلمة مرور تُدخلها وأي بريد إلكتروني تُرسله، وسيصل إلى صورك وملفاتك، وتُطمئنك بعض تطبيقات الرسائل والتخزين السحابي أن محتوى هاتفك مُؤمنٌ بخاصية التشفير التام بين الطرفين، وتعني أنك أنت والمستقبل فقط هما من تستطيعان رؤية المحتوى، ويعود "دان تان" للقول إنه في وسط هذا يوجد هجوم الوسيط، ثم يُعاد تشفيرها مجدداً، لذا تكون مُشفرة من وجهة نظرك، بما فيها جهات الاتصال، وغير ذلك. يسأل "جوشوا ليم" إن كان الأفضل إيقاف تشغيل الكاميرا والمسجل وخاصية تحديد المواقع، وبمساعدة هذه المعلومات المسروقة، سيتمكن أي شخص من انتحال شخصيتك، أو الحصول على معلومات تخص أصدقاءك. ويهدف المخترقون عادةً إلى جني المال مقابل بيع البيانات التي استولوا عليها من الأجهزة المخترقة، مما يحقق لهم في النهاية أرباحاً طائلة. إغراء الاتصال بشبكة لاسلكية مجانية لا يُقاوم، ومع ذلك فعليك أن تتجنب لاحقاً القيام بخدمات مصرفية، في عصر الإنترنت هذا، وعلينا مراقبة خطواتنا، إرث الأمير. ثمة أوقات نتعرض فيها للخداع لكي نُفصح عن معلومات مهمة. ويُشبه الاحتيال الإلكتروني صيد الأسماك، لكن الطُعم هنا هو رسالة في بريدك الإلكتروني، وما يُحاول محتالو الإنترنت صيده من حوض مليء بالمستخدمين، ومن الغباء جدا التعامل مع هذه الرسائل والرد عليها، فمعلوماتكم قيّمة جداً، وهي توصل عدداً أكبر من المجرمين إلى طرق لسرقتها دون علمكم، تُكلف ضحاياها ملايين الدولارات. فإذا كنتم تظنون أن هذه الخدع تنطلي فقط على كبار السن فأنتم مخطئون، وقد تصلك رسالة على هاتفك أو بريدك الإلكتروني فيها خبر مثير للاهتمام، وتضم رابطاً يُوصلك إلى موقع يُشبه تماماً موقعاً تملك اشتراكاً عليه، ولم يُكلف الأمر المحتال أكثر من نصف ساعة مثلاً لتصميم هذا الموقع المزيف، حماية النفس. يقول "دينغ يائو" -وهو طالب في جامعة سنغافورة للإدارة، ورئيس نادي "القبة البيضاء" الذي يضم مخترقين نزيهين يدعون إلى تعزيز الأمن السيبراني الإلكتروني- إنه يجب علينا التأكد قبل الضغط على أي رابط من أن العنوان الإلكتروني الظاهر موثوق، أو الاتصال بالشركة إذا كانت المعلومات المطلوبة حساسة، أو على شعار الموقع، فمعظمها لن يعمل إذا كان الموقع مُخصصاً للاحتيال. بل الأفراد أيضاً، فقد يستخدم البعض صورتك لانتحال شخصيتك على موقع فيسبوك مثلاً، ثم يستخدم الحساب المزيف باسمك وصورتك للإيقاع بضحاياه. ويُكافح موقع فيسبوك للتعامل مع الحسابات الوهمية والمكررة، فقد عطلوا أكثر من ملياري حساب وهمي عام 2018. ويرشدك كتاب "زيّفها. دليلك للدفاع رقمياً عن نفسك" للتعامل مع هذا الأمر، واستخدام هويات مزيفة لحساباتنا على المواقع والخدمات التي لا نرغب بمنحها هوياتنا الحقيقية، ويعني هذا اسماً وتاريخ ميلاد وبريداً إلكترونياً مزيفاً،