كيف تحمي نفسك على الإنترنت؟

علي الرضا سبيتي

لقد أصبح الإنترنت أو الاتصالُ الشبكيُّ الجزءَ الأكبرَ من حياتنا اليومية، ويأخذ حيّزاً كبيراً من وقتنا وتواصلنا مع الآخرين، وحتى من معاملاتنا وعمليات الشّراء والبيع وغيرها. بل حتّى الدّراسة، وكسب المعلومات، والتّسلية، صارت الشبكة العنكبوتية هي أداتَها.

لكنّ الحذرَ واجبٌ! خاصّةً بعدما علق في خيوط هذا الشبكة الرقمية على الأقل 1 من أصل 10 أشخاص نعرفهم. إذ تتنوّع المخاطر ما بين انتهاك الخصوصية الشخصية، أو سرقة المعلومات الخاصّة، وغيرها.

حسنًا، قد يكون من المستحيل أن تحمي نفسك بنسبة 100% من أيِّ انتهاكٍ على الإنترنت، فحتّى بعض الشركات التي تعتبر آمنةً يدور حولها شكوكٌ وملاحقاتٌ قانونيةٌ بسبب انتهاك الخصوصية، أو بيع معلوماتٍ خاصةٍ بالمستخدِمين. فمثلاً فايسبوك الذي دخل إلى كلِّ تفاصيلنا اليوميّة، اعترف بأن المعلومات الشخصية لأكثر من 87 مليون مستخدمٍ قد سُرّبت لأغراضٍ دعائيةٍ وسياسيّةٍ. هذا الأمر يرتّب علينا سلسة خطواتٍ يجب أن نتّبعها من أجل الحصول على أكبر قدرٍ من الحماية الممكنة على هذه الشبكة.

ولكن بدايةً لنتعرف على المخاطر التي قد نواجهها عند استخدام الإنترنت:

التصيد (Phishing): وهي عمليةٌ احتياليةٌ بحيث يعرض عليك موقعٌ مموَّهٌ على أنه أحد المواقع الموثوقة، للحصول على معلوماتٍ شخصيةٍ أو كلماتِ مرورٍ، أو معلوماتٍ مصرفيةٍ... إلخ. هذه العملية تحصل عادة عبر البريد الإلكتروني أو الرسائل المباشرة التي تحتوي على روابط للصفحة المموّهة، وتكون قد صممت لتُشابه الصفحة الحقيقيّة بشكلٍ مطابِقٍ.

البرمجيات الخبيثة (Malware):
هي عبارةٌ عن برمجياتٍ صغيرةٍ تكون أيضاً مموَّهةً على شكلِ برنامجَ ما أو مدمَجةً ضمن أحد البرامج ليصعُب كشفُها. ويعمل هذا البرنامج على رصد تحركاتك على الإنترنت وتسجيل كلمات السرّ والمعلومات التي يريدها المبرمج. وعادة يوزّع هذا البرنامج عبر البريد الإلكتروني أو عند تنزيل الملفات أو البرامج من مواقعَ غير موثوقةٍ.

المطاردة الإلكترونية (Stalking):
وهي ملاحقة الشخص من قبل فردٍ أو جهةٍ للحصول على معلوماتٍ تساعد في مضايقته أو أذيته، كمعرفة أفراد أسرته أو أوقات خروجه من المنزل، أو اهتماماته.

الاختراق (hacking): هي عملية لسرقة الحسابات على أحد المواقع التي قام فيها المستخدم بتسجيل الدخول، أو سرقة البيانات المخزّنة على أحد الأجهزة.

الهندسة الاجتماعية: وهي أسلوبٌ للتحايل والحصول على المعلومات من الشخص مباشرةً عبر طرح أسئلةٍ قد لا تبدو ذاتَ أهميةٍ، ولكنها تساعد المستهدِف في استخدامها ضد الشخص المستهدَف، كالعمر وعنوان السكن والعمل..

ولتفادي الوقوع في هذه المخاطر ثمّةَ خطواتٌ عند تصفُّحِك الإنترنت على الحاسوب أو الهاتف، أو لدى تعاملك مع أيِّ جهازٍ موصولٍ بالإنترنت:

عدم الإتصال بشبكات الإنترنت المجانية كما في المطاعم والفنادق، لأنها بأغلبها شبكاتٌ مفتوحةٌ وغيرُ آمنةٍ، وتجعل من جهازك لقمةً سهلةً لأيِّ مخترقٍ متّصلٍ معك على الشبكة نفسها. وعند استعمال هذا النوع من الشبكات يُفضَّل الاستعانة بخدمة VPN، وهو برنامجٌ يساعدك على الاتصال بالإنترنت عبر شبكةٍ آمنة، ويغيّر مكان اتصالك بآخرَ وهميٍّ ومشفَّر ممّا يجعل من الصّعب على المخترق الوصول إلى جهازك، أو يمكن استخدام برنامج Tor للتصفح الذي يقوم بالعملية نفسها ولكن هذا الأخير قد يكون أبطأ نوعاً ما.

ضرورة وجود برنامج جيّد للحماية من الفيروسات، والتأكّد من تحديثه دائماً لضمان الحماية من أيِّ نوعٍ من الفايروسات أو البرمجيّات الخبيثة الجديدة.

التأكد دائماً من تحديث نظام التشغيل على الحاسوب والهاتف بالإضافة إلى البرامج المستخدمة التي تتضمن دائماً تحديثاتٍ تتعلّق بالحماية والخصوصية.

عدم فتح رسائلَ أو بريدٍ إلكترونيٍّ من مصدَرٍ مجهولٍ، لأنها قد تحتوي على روابطَ لمواقعَ مشبوهةٍ أو تتضمّن برمجيّاتٍ خبيثةً،

تبدأ بالعمل بمجرّد فتح البريد الإلكترونيّ إذا كان عبارةً عن كود HTML، بدون أن يعرف بها نظام التشغيل.

عدم فتح أيِّ روابَط غيرِ واضحةٍ أو مجهولةِ المصدر، وعند الدخول إلى أيِّ موقعٍ، التأكّد من وجود شعار القفل في مقدمة الرابط، أو أن يبدأ بـHTTPS عوضاً عن HTTP فقط، هذا يشير إلى أنّك متّصلٌ مع موقعٍ آمنٍ.

عدم التسجيل على أيِّ موقعٍ غيرِ موثوق، أو يتضمّن التسجيلُ فيه أسئلةً أكثرَ من المعتاد، فقد يكون موقعًا يعملُ على جمع البيانات الخاصّة بالمستخدمين فقط.

عدم القيام بعمليّات بيعٍ أو شراءٍ على مواقعَ غيرِ معروفةٍ أو غيرِ موثوقةٍ. ولا تقم بعمليات الشراء عبر الإنترنت عبر حسابك البنكيّ الأساسيّ. بل قم بإنشاء حسابٍ خاصٍّ لهذه العمليّات تودِع فيه المبلغ المطلوب عند كلِّ عمليّةٍ فقط. وفي حال حدوث أيِّ مشكلةٍ ستقتصر على هذا الحساب الصغير وسيبقى حسابُك الرئيسيُّ بأمان.

عدم تنزيل البرامج المجانيّة أو التحميل من مواقع مشاركة الملفات. ذلك أنّها المواقعُ الأكثرُ قدرةً على القرصنة، وعلى استهدافك بالبرمجيات الخبيثة عند التحميل منها. والأسلم هو استثمار بعض المال على البرنامج الأصليّ إذا كنت شديد الحاجة إليه، كي لا تخاطر بخصوصيّتك ومعلوماتك الشخصيّة.

هذا في ما يخصّ التصفّح الإلكترونيّ بشكلٍ عامٍّ، ولكن عندما نكون أكثرَ تحديدًا، عندئذٍ نصل إلى البرامج والمواقع التي نستخدمها بشكل يوميٍّ. هنا، ثمّة إجراءاتٌ إضافيّةٌ. ففي مواقع التواصل الاجتماعيّ، ليس عليك القلق فقط من الفيروسات والبرمجيّات أو المخترقين، هنا الخطر يكون حتى من المستخدمين العاديين، وقد تكون المشكلة في محاولة اختراق حسابك، أو متابعة أخبارك وملاحقتك ومراقبتك بأيِّ غرضٍ كان، وقد تكون مجرد شخصٍ عاديٍّ لا يرغب أن يشارك أمور حياته مع أيٍّ كان.

لنبدأ بإجراءات الحماية بحساباتك:

لا تستعمل كلمةَ السر نفسها لكل حساباتك، أو كلماتٍ متشابهةً، لتكن كلمات السرّ مختلفةً من موقعٍ لآخرَ، ولا تجعلْها سهلة التخمين كتاريخ ميلادك أو اسم شخصٍ عزيزٍ أو أيِّ شيءٍ يتعلّق بك وقد يسهل تخمينه، ادمج بين الأحرف والأرقام والرموز.

لا ترسل كلمة المرور الخاصة بك إن كان عبر التعليقات أو الرسائل الخاصة على أيٍّ من مواقع التواصل الاجتماعي، وإذا اضطر الأمر تأكد من تغييرها مباشرة.

ادخل إلى الاعدادات الخاصة

بالخصوصية والأمان على هذه المواقع وقم بحمايتها وعدلها بما يضمن حمايتك بشكلٍ أكبر.

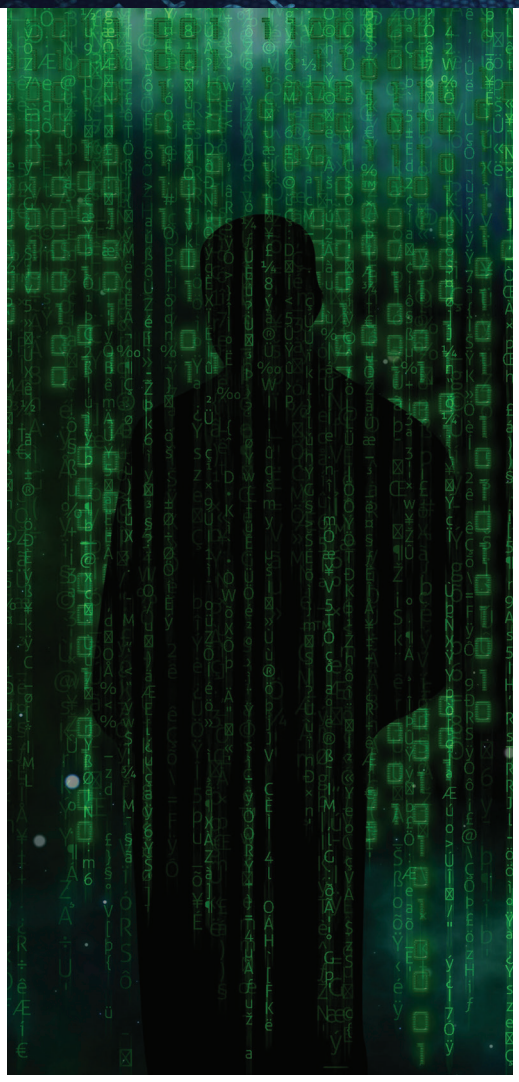
كتفعيل خاصيّةِ تأكيد تسجيل الدخول المكرر.

تأكد من تسجيل الخروج من أيِّ حسابٍ عند الانتهاء منه، خاصَّةً إذا لم تكن تستخدم هاتفك أو حاسبك الشخصيّ لضمان عدم حفظ كلمة السرّ، وعند تسجيل الدخول إذا طُلب منك حفظ الكلمة في المتصفح اضغط لا إن كنت تعتقد بأن أحد غيرك قد يستخدم المتصفحَ نفسه، وقم بمحو ذاكرة المتصفح بين الحين والآخر.

اجعل حسابَك سريّاً (private)، ولا تجعل معلوماتك الشخصية متاحةً لأيِّ كان، كرقم الهاتف وتاريخ الميلاد وغيرها، ممّا يسهّل اِستخدامَها في انتحال شخصيّتك في أماكن أخرى.

راجع جيّداً ما تقوم بنشره خاصّة إذا كان عامّاً ويمكن لأيِّ كان الوصول إليه، مثلاً لا يكون واضحاً وقت سفرك أو الأوقات التي تترك فيها منزلك فارغاً. لا تظهر أوقات خروجك ودخولك وتحركاتك وتفاصيل عائلتك الصغيرة خصوصاً إذا تضمّنت الأطفال.

هذا العالم واسعٌ جدّاً، وفيه الكثير من المخاطر التي تنتظرك هنا وهناك، لذلك انتبه جيّداً واحذر عند تصفّحك للشبكة العنكبوتيّة، فخصوصيّتك ومعلوماتك ليست للعرض وللمشاركة مع أيِّ كان.



علي الرضا سبيتي
متخصص في تكنولوجيا المعلومات