7 نصائح تساعدك على حماية خصوصيتك الرقمية أثناء إجازة العيد

الثلاثاء 4 يونيو 2019 05:06 م

ساعات قليلة؛ وتبدأ إجازة عيد الفطر المبارك التي يستغلها العديد منا في السفر، أو قضاء وقت ممتع مع العائلة خارج البيت، وبالطبع نحن لا نتحرك هذه الأيام دون هاتفنا الذكي، الذي أصبح مرتبطًا بكل تفاصيل حياتنا ابتداءً من جميع حساباتنا على منصات التواصل الاجتماعي، والتطبيقات المهمة ذات الصلة بالحساب البنكي، وبطاقات الإئتمان، وحتى الألعاب المُصممة لاستخدام بعض مكونات الهاتف مثل: الكاميرا، والميكروفون وغيرها، أو استخدام بعض إمكانيات نظام التشغيل.

وبالنظر إلى هذا الواقع؛ وللحصول على الخصوصية الكاملة، ستحتاج إلى تثبيت مجموعة من الأدوات التي قد تتسبب في إبطاء سرعة الإنترنت مثل: متصفحات الويب المخصصة، وتطبيقات تأمين البريد الإلكتروني، وتطبيقات الدردشة المشفرة، والشبكات الخاصة الافتراضية VPN، وأنظمة التشغيل التي تركز على الأمن، أو بدلًا من كل ذلك ستحتاج إلى البقاء بعيدًا عن الإنترنت تمامًا.

لكن لا تفقد الأمل؛ فبالرغم من أن الخصوصية الكاملة أمر غير قابل للتحقيق عمليًا، إلا أنه يمكنك حماية نفسك بطريقتين: إما عن طريق إغلاق أجهزتك وحساباتك، حتى لا يمكن الوصول لبياناتك، أو اتباع سلوكيات وقائية أثناء استخدام الإنترنت.

يمكنك اتباع بعض السلوكيات الوقائية من خلال إجراء بعض التغييرات البسيطة على أجهزتك، وحساباتك، والتي ستتيح لك الحفاظ على أمن بياناتك ضد محاولات الأطراف الخارجية غير المرغوب فيها للوصول إلى بياناتك، وكذلك حماية خصوصيتك من أولئك الذين لا تريد مشاركة معلوماتك معهم.

فيما يلي 7 نصائح تساعدك على حماية خصوصيتك الرقمية أثناء إجازة العيد:

1- تأمين حساباتك:
شهدت الفترة الأخيرة الكثير من خروقات البيانات، وتسريب كلمات مرور عملاء شركات كبرى، مثل: شركة Equifax العاملة في مجال خدمات الائتمان الاستهلاكي، وياهو، وفيسبوك، ولينكدإن، وHome Depot، وسلسلة فنادق ماريوت، وغيرها. لذلك إذا كان لديك حسابات عبر الإنترنت، فمن المحتمل أن يكون القراصنة قد وصلوا لبيانات واحد منها على الأقل.

لمعرفة أي من حساباتك قد اُخترق بالفعل، يمكنك اتباع الخطوات التالية:

توجه إلى هذا الرابط https://haveibeenpwned.com/.
اكتب عنوان بريدك الإلكتروني المستخدم في الحساب الذي تريد فحصه، ومن خلال خدمة Have I Been Pwned؛ يمكنك إجراء الفحص من خلال قاعدة بيانات تعمل كمكتبة لاختراقات البيانات التي حدثت، وستخبرك الخدمة إذا كان عنوان بريدك الإلكتروني، أو معلوماتك الشخصية قد سُربت ضمن إحدى الاختراقات السابقة المعروفة بشكل عام.
بمجرد تحديد الحساب الذي اُخترق عن طريق البريد الإلكتروني الذي أدخلته، يجب عليك تغيير كلمة المرور الخاصة بهذا الحساب، وأي حسابات أخرى استخدمت فيها كلمة المرور نفسها.

مع كثرة الخدمات، والمواقع، والتطبيقات زادت كلمات المرور الخاصة بنا، وهذا هو السبب الذي يجعل غالبية المستخدمين يتخلون عن تخصيص كلمة مرور مختلفة لكل حساب، لذلك يمكنك استخدام أدوات إدارة كلمات المرور، التي تساعدك في إنشاء كلمات مرور، وحفظها، وإدخالها تلقائيًا لكل موقع أو تطبيق تستخدمه، يمكنك الاستعانة بأحد تطبيقات إدارة كلمات المرور، مثل: 1Password، وLastPass، أو أي تطبيق مماثل، حيث يمكن لهذه التطبيقات إنشاء كلمات مرور قوية، واقتراح تغيير كلمات المرور الضعيفة، ومزامنة كلمات المرور بين الكمبيوتر والهاتف.

2- احرص على تحديث أنظمة التشغيل، والبرامج على أجهزتك:
تتلقى أنظمة تشغيل الهواتف وأجهزة الكمبيوتر، ومتصفحات الويب، والتطبيقات الشائعة، وحتى الأجهزة المنزلية الذكية تحديثات دورية مع ميزات جديدة، وتحسينات أمنية. حيث تحرص الشركات المنتجة لأنظمة التشغيل والبرامج، على تعزيز أمنها، ومعالجة الثغرات التي ظهرت في الإصدارات القديمة، وعادة ما تكون تحديثات الأمان هذه أهم بكثير من برامج مكافحة الفيروسات؛ لإحباط هجوم القراصنة.

لذلك يمكنك حماية خصوصيتك من خلال استخدام أحدث إصدار من نظام التشغيل والبرامج على جميع أجهزتك دائمًا، وتفعيل ميزة التحديث التلقائي في جميع أنظمة التشغيل من خلال الإعدادات.

وهذا ينطبق أيضًا على التطبيقات التي على هاتفك، أو جهازك اللوحي، وانتبه بشكل خاص لتحديث التطبيقات التي تستخدمها بانتظام لإجراء التعاملات المالية، أو الشخصية.

3- حماية تصفح الويب الخاص بك:
تتبع الشركات والمواقع كل ما تفعله عبر الإنترنت، حيث تقوم الإعلانات، وأزرار الإعجاب في منصات التواصل الاجتماعي، ومواقع الويب بجمع معلومات حول موقعك الجغرافي، وعادات التصفح، وغير ذلك الكثير، وتكشف البيانات التي جُمعت عنك أكثر مما تتوقع.

قد تظن نفسك ذكيًا بما يكفي لعدم كشفك مطلقًا عن مشاكلك الطبية، أو مشاركة جميع اهتماماتك على فيسبوك مثلًا، ولكن يجب أن تعرف أن مواقع الويب التي تزورها توفر معظم البيانات التي يحتاجها المعلنون لتحديد هويتك، وهذا جزء من الكيفية التي تظل بها الإعلانات المستهدفة واحدة من أكثر ابتكارات الإنترنت إثارة للقلق.

لذلك يمكنك استخدام إضافات متصفحات الويب الخاصة لحماية خصوصيتك مثل: uBlock Origin التي تقوم بحظر الإعلانات، والبيانات التي تجمعها المواقع. وتمنع إضافة uBlock أيضًا تشغيل البرمجيات الضارة في متصفحك، وتمنحك طريقة سهلة لإيقاف حظر الإعلانات، عندما تريد دعم المواقع التي تعرف أنها آمنة.

يجب عليك أيضًا تثبيت إضافة HTTPS Everywhere؛ حيث تقوم تلقائيًا بتوجيهك إلى الإصدار الآمن من الموقع، عندما يدعم الموقع ذلك، مما يجعل من الصعب على المهاجمين الاطلاع على ما تتصفحه، خاصةً إذا كنت تستخدم شبكة Wi-Fi عامة، في مقهى أو مطار أو فندق.

4- لا تقم بتثبيت تطبيقات أو إضافات من مصدر مجهول:
يعتبر كل تطبيق غريب تقوم بتثبيته على هاتفك، وكل إضافة مجهولة للمتصفح، بمثابة ثغرة أمنية محتملة، كما أن هناك عددًا لا يحصى من التطبيقات التي تقوم بتتبع موقعك في كل مكان تذهب إليه، وتجمع بياناتك دون طلب الموافقة، حتى في تطبيقات الأطفال.

لذلك توقف عن تنزيل التطبيقات وإضافات المتصفح من مواقع غير موثوق بها، والتزم بتنزيلها من مواقع الشركات المطورة لها، أو من متاجر التطبيقات الرسمية.

غالبًا أنت لا تحتاج إلى نصف التطبيقات المُثبتة على هاتفك، والتخلص من هذه التطبيقات سيجعل هاتفك يعمل بشكل أسرع، كما يجب عليك مراجعة أذونات الخصوصية للتطبيقات التي تستخدمها.

5- استخدم برنامجًا محدثًا لمكافحة الفيروسات:
قد لا تبدو الفيروسات شائعة حاليًا كما كانت قبل عقد من الزمان، لكنها لا تزال موجودة، ويمكن أن تتسبب البرامج الضارة على جهاز الكمبيوتر الخاص بك في حدوث جميع أنواع الانتهاكات بدءًا من النوافذ المنبثقة المزعجة، والتنقيب السري عن عملات البيتكوين، إلى المسح الضوئي للحصول على معلومات شخصية.

لذلك إذا كنت معرضًا لخطر النقر على الروابط المحفوفة بالمخاطر، أو كنت تشارك جهاز الكمبيوتر مع عدة أشخاص في الأسرة، فمن المفيد ضبط إعداد برنامج مكافحة الفيروسات، وخاصة على الأجهزة العاملة بنظام التشغيل ويندوز Windows، حتى تتمكن من حماية خصوصيتك بشكل أكبر.

وإذا كان جهازك يعمل بنظام ويندوز 10، فعليك استخدام برنامج مايكروسوفت المدمج Windows Defender؛ حيث يوفر الكثير من الأمان لمعظم الأشخاص، وهو خيار مكافحة الفيروسات الرئيسي في إصدار ويندوز 10.

6- تنشيط تتبع الهاتف ومسح البيانات عند فقده:
أنت بحاجة إلى التأكد من أنه لا يمكن لأحد الدخول إلى هاتفك إذا فقدته، أو سرقه أحد، من المعروف أن الهواتف الذكية تُشفر افتراضيًا، وذلك أمر رائع، ولكن لا يزال عليك اتخاذ بعض الخطوات لضمان إغلاق هاتفك بشكل صحيح في حالة اختفائه.

أولًا: يجب عليك إنشاء رمز مرور قوي على شاشة القفل Lock screen، والابتعاد عن وضع كلمة مرور سهلة التخمين، وإذا كان هاتفك يدعم التأمين بواسطة البصمة فاستخدمها، واجعل كلمة السر البديلة قوية أيضًا.

ثانيًا: احرص على تفعيل وإعداد ميزة التتبع عن بُعد في هاتفك Find My Device؛ وهي خدمة تقدمها هواتف أندرويد، آي أو إس وتتيح لك تتبع موقع هاتفك في حالة فقده، أو قفله عن بُعد، أو مسح البيانات عن بُعد أيضًا.

7- تفعيل ميزة التشفير على حاسوبك المحمول:

إذا فقدت حاسوبك المحمول، أو قام أحدهم بسرقته، يمكن للسارق الوصول إلى بياناتك بسهولة، وحتى إذا كان هناك كلمة مرور، ما يزال بإمكان السارق نسخ الملفات من الجهاز إذا كان لديه بعض الخبرة في التعامل مع هذه الأجهزة

يجب عليك تشفير القرص الصلب على جهازك، حيث تحمي كلمة المرور، ومفتاح الأمان بياناتك؛ وبدون كلمة المرور أو المفتاح يسهل وصول أي شخص إلى بياناتك، لذلك استخدم إحدى برمجيات التشفير الخاصة بهذا الأمر، واتبع الإرشادات حول كيفية إعداد التشفير على كل من نظام التشغيل ويندوز، وماك Mac.

عند الحديث عن سرقة حاسوبك المحمول، فأنت معرّض في أي وقت لفقد كل البيانات المخزنة عليه، لذلك فإن الأمر يستحق بذل بعض الجهد لأخذ نسخة احتياطية من البيانات وحفظها في مكان آمن، وهنا يمكنك استخدام خدمة النسخ الاحتياطي عبر الإنترنت Backblaze، التي تقوم بتشفير جميع بياناتها بطريقة لا يمكن حتى للعاملين فيها الوصول إليها، وهنا تضمن حماية خصوصيتك، وتامين بياناتك في الوقت نفسه

في نهاية المطاف؛ ترتبط الخصوصية، والأمان ببعضهما جيدًا، لذلك تحتاج إلى التعود على حماية الاثنين قد يستغرق الأمر في البداية الكثير الوقت، ولكن بمجرد اتباع الخطوات المذكورة أعلاه فكل ما سيتبقى هو تعزيز حكمك على الأشياء الأكثر أهمية، واتباع سلوكيات وقائية جيدة عبر الإنترنت، والتي تتمثل فيما يلي:

احذر من الروابط في رسائل البريد الإلكتروني، وعلى وسائل التواصل الاجتماعي
اجعل حساباتك خاصة، ولا تشارك أي شيء لا تريد جعله عامًا
حافظ على خصوصية عنوان البريد الإلكتروني الرئيسي، ورقم الهاتف، ولا تستخدمهما إلا في الأمور المهمة
استخدم عنوان بريد إلكتروني فرعي للمواقع غير المهمة مثل: التسوق، والأنشطة الأخرى عبر الإنترنت
تجنب استخدام اسمك ورقمك الحقيقي عندما تضطر إلى الاشتراك في خدمة لا تهتم بها