Arabic

أهم عشر نصائح للخصوصية

1. يستخدم قراصنة الإنترنت رسائل البريد الإلكتروني التصيّدية للوصول إلى معلوماتك الآمنة. احذر جميع الاتصالات التي تتلقاها، وإذا اعتقدت أن رسالة وصلتك بالبريد الإلكتروني مشبوهة، لا تنقر على أي روابط أو تفتح أي مرفقات.

2. حسّن مستوى أمنك على الإنترنت من خلال إعداد مصادقة ثنائية العوامل. فبإضافة خطوة أخرى للمصادقة على هويتك تجعل من الصعب على المهاجم الوصول إلى بياناتك.

3. لا تقم دائمًا بتمكين تحديد الموقع الجغرافي. من الشائع أن تطلب منك مواقع الإنترنت الإفصاح عن موقعك. لكنه بقيامك بذلك، تقوم تلك المواقع بإنشاء ملف تعريفي عن موقعك واهتماماتك. بدلاً من ذلك، حدّد موقعك يدويًا لحماية بياناتك بشكل أفضل.

4. قم بتثبيت أدوات حظر الإعلانات - فالإعلانات قد تتعقبك في الخلفية. استخدم أدوات حظر الإعلانات لتعطيل التتبع والتحليلات من أطراف ثانية وثالثة.

5. كن حذرًا عند استخدام شبكات Wi-Fi العامة، إذ إنها تكون غالبًا أقل أمنًا من الشبكات العادية وتتيح الوصول إلى أجزاء من بياناتك أكثر من اللازم عندما تعطيك وصلة إنترنت.

6. من حقك أن تسأل عن سبب جمع أي معلومات عنك. ويشمل ذلك، على سبيل المثال، وكالات حكومة الولاية والمؤسسات الأخرى. قد تحتوي سياسة الخصوصية الخاصة بها على هذه المعلومات.

7. حافظ على أمان وثائقك وملفاتك إذا كانت تحتوي على معلومات حساسة أو شخصية. فكّر في استخدام التشفير لقفل محركات الأقراص الثابتة المحمولة وأجهزة USB لمنع الوصول غير المصرّح به إذا فقدتها.

8. حافظ على سرية وأمان كلمات المرور وأرقام التعريف الشخصية ورموز الدخول الأخرى. يُعتبر استخدام برنامج لإدارة كلمات المرور طريقة جيدة للحفاظ على أمن كلمات المرور وتسجيلات الدخول الخاصة بك لأنه يتم تخزينها في قواعد بيانات مشفرة.

9. قم بتمكين إعدادات الخصوصية ومراجعتها بانتظام عند استخدام وسائل التواصل الاجتماعي ومنصات الشبكات (مثل Facebook وTwitter)، وفكّر في جعل ملفاتك الشخصية على وسائل التواصل الاجتماعي خصوصية.

10. تخلّص بشكل آمن من الرسائل التي تصلك بالبريد وتحتوي على تفاصيل شخصية (عن طريق تفتيتها مثلاً). لا تضع أبدًا وثائق حساسة تحتوي على بياناتك الشخصية في برميل إعادة التدوير.