Spanish

LOS DIEZ MEJORES CONSEJOS DE PRIVACIDAD

1. Los piratas informáticos utilizan correos electrónicos de phishing para acceder a su información segura. Tenga cuidado con todas las comunicaciones que reciba y, si cree que el correo electrónico es sospechoso, no haga clic en ningún enlace ni abra ningún archivo adjunto.

2. Mejore su seguridad en línea configurando la autorización de dos factores (two-factor authorisation). Agregar un paso Agregar un paso más de autenticación de su identidad dificulta que un atacante acceda a sus datos.

3. No siempre habilite la geolocalización. Es común que los sitios web le pidan que comparta su ubicación. Al hacerlo, crean un perfil en torno a su ubicación e intereses. En su lugar, seleccione manualmente su ubicación para proteger mejor sus datos.

4. Instale bloqueadores de anuncios: los anuncios pueden estar rastreándole en segundo plano. Utilice bloqueadores de anuncios para desactivar seguimientos y análisis de segundas y terceras partes.

5. Desconfíe de las redes de Wi-Fi públicas, ya que suelen ser menos seguras que las normales y dan acceso a más datos de los necesarios al dar conexión a Internet.

6. Tiene derecho a preguntar por qué se recopila información sobre usted. Esto incluye, por ejemplo, agencias gubernamentales estatales y otras organizaciones. Sus políticas de privacidad podrían contener esta información.

7. Mantenga sus documentos y archivos seguros si contienen información confidencial o personal. Considere la posibilidad de utilizar el cifrado (encryption) para bloquear discos duros portátiles y USB para evitar el acceso no autorizado si se extravían.

8. Mantenga la confidencialidad y seguridad de contraseñas, PIN y otros códigos de acceso. El uso de un administrador de contraseñas (password manager) es una buena manera de mantener seguras sus contraseñas e inicios de sesión, ya que se almacenan en bases de datos cifradas.

9. Habilite la configuración de privacidad y revísela regularmente cuando utilice redes sociales en línea y sitios de redes (por ejemplo, Facebook, Twitter). Considere la posibilidad de hacer que sus perfiles de redes sociales sean privados.

10. Deseche de forma segura el correo que contenga datos personales (por ejemplo, triturándolos). Nunca ponga documentos confidenciales que tengan sus datos personales en la papelera de reciclaje.