

Tips para cuidar tus datos personales en Internet

En una consulta realizada a 10 mil usuarios alrededor del mundo, arrojó cifras alarmantes. Se comprobó que la mitad de los usuarios que utilizan una aplicación financiera desconoce si el fabricante de la aplicación vende su información personal a terceros.

Menos de 1/3 de los encuestados había leído las condiciones de uso antes de descargarse la app (31 %) o las políticas de privacidad (29 %). Lo que muestra la actitud de los consumidores a la hora de protegerse a sí mismos o sus finanzas. Y el grado de vulnerabilidad al que están expuestos por las ciberamenazas como resultado.

Consejos para cuidar los datos

1.- Leer las políticas de privacidad y términos de uso de las plataformas. Con esto se entenderá cuál es el destino de los datos y qué control se tendrá sobre ellos una vez cedidos a la organización en cuestión.

2.- Tener cuidado de no caer en ciberestafas. No seguir enlaces que contengan información sospechosa. Una mirada crítica a lo que se ve en Internet puede ayudar a proteger la información.

3.- Pensar dos veces antes de compartir información en Internet. Entre menos datos personales se compartan en Internet, menos expuesta va a estar la información personal.

4.- Ser responsables con lo que se comparte en redes sociales. Estar atentos a lo que se comparte en línea y con quién es una manera de frenar el alcance que tienen estas campañas.

5.- Chequear que el enlace que se visita pertenezca a la organización oficial. Verificar si la conexión es cifrada mediante HTTPS, lo que puede usualmente observarse como un candado verde donde se encuentra la URL. Y que el certificado sea firmado por una entidad confiable.

6.- Utilizar contraseñas seguras. Procurar no repetirlas entre diferentes plataformas y activar el doble factor de autenticación siempre que se pueda.

7.- Escribir la URL del sitio al que se intenta ingresar

directamente en la barra de direcciones. No hacerlo mediante los resultados de buscadores como Google, ya que los primeros resultados no siempre son los genuinos debido a una actividad conocida como black hat SEO.

8.- Utilizar redes conocidas y privadas para navegar por Internet. Es mejor utilizar redes propias y privadas para navegar, y realizar actualizaciones frecuentes al firmware del router hogareño. Si no es posible conectarse mediante una red segura, procurar utilizar una VPN para cifrar el contenido del tráfico.

9.- Proteger el equipo desde el cual procesamos y enviamos la información. Hay que hacerlo con una buena solución de seguridad y actualizaciones frecuentes del sistema operativo y aplicaciones.

Con información de [2001](#)