



CIBERCONSEJOS DE SEGURIDAD

EGOSURFING: El saludable hábito de buscarse en internet

Puede sonar egocéntrico. Pero buscar qué información existe de nosotros en internet es necesario, ya que nos permite descubrir si se ha revelado datos confidenciales sin nuestro consentimiento, o si existen cuentas que nos suplanten, y realizar las gestiones para que dejen de estar disponibles en línea.



QUÉ ES EL EGOSURFING

Se conoce como egosurfing el buscar qué hay de nosotros en las redes sociales y otros sitios de la web.

Esto es útil para saber si existe información confidencial que ha sido difundida sin nuestro consentimiento, o si sufrimos algún caso de suplantación.

BÚSQUEDA EN GOOGLE

El primer paso es buscarnos en Google.

- 1.- Debemos buscar nuestro nombre y apellido, RUT, dirección, teléfono, email, cuentas de redes sociales y otros datos que puedan identificarnos en internet.
- 2.- Conviene buscar nuestro nombre entre comillas. Por ejemplo, "Juan Pérez" trae resultados más precisos.
- 3.- En Google Imágenes se puede hacer una "búsqueda inversa", en la que subimos fotos de nosotros y podemos ver si las mismas han aparecido en internet.

USAR GOOGLE ALERTS

Al ingresar a <https://www.google.com/alerts>, podemos crear "alertas" que nos avisan de nuevas publicaciones con distintos términos de interés, en este caso, distintos ejemplos de datos personales.

- Los conceptos deben ir entre comillas, así Google nos avisa solo cuando aparecen juntos. Si nuestro nombre es común, conviene también buscar nuestro nombre con ambos apellidos.
- Se puede elegir la periodicidad de las alertas y a qué email queremos que nos lleguen.

Revisa tus R.R.S.S.

- 1.- Buscar nuestro nombre o cuenta en las principales redes sociales, además de variantes similares a nuestros nombres digitales, para ver si alguien ha creado cuentas para hacerse pasar por nosotros.
- 2.- También podemos fijarnos en la impresión que dan nuestras publicaciones en internet, y si queremos cambiar esa imagen o decidimos revelar menos información sobre nosotros mismos.
- 3.- Podemos aprovechar de asegurarnos de que nuestra configuración en redes sociales comparta la menor cantidad de información posible.

Si encontramos cuentas que nos suplanten o revelen nuestros datos:

- Denuncia ante la debida plataforma. Mostramos como hacerlo en Facebook, Instagram y Twitter en nuestra ciberguía contra el acoso digital:
<https://www.csirt.gob.cl/media/2021/03/Cibergui%CC%81a-Denuncia-el-Abuso-Digital.pdf>
- Si crees sufrir de un delito o que tu integridad corre peligro, contactar a:

Cibercrimen PDI

(+562) 27080658

(+562) 27080659

