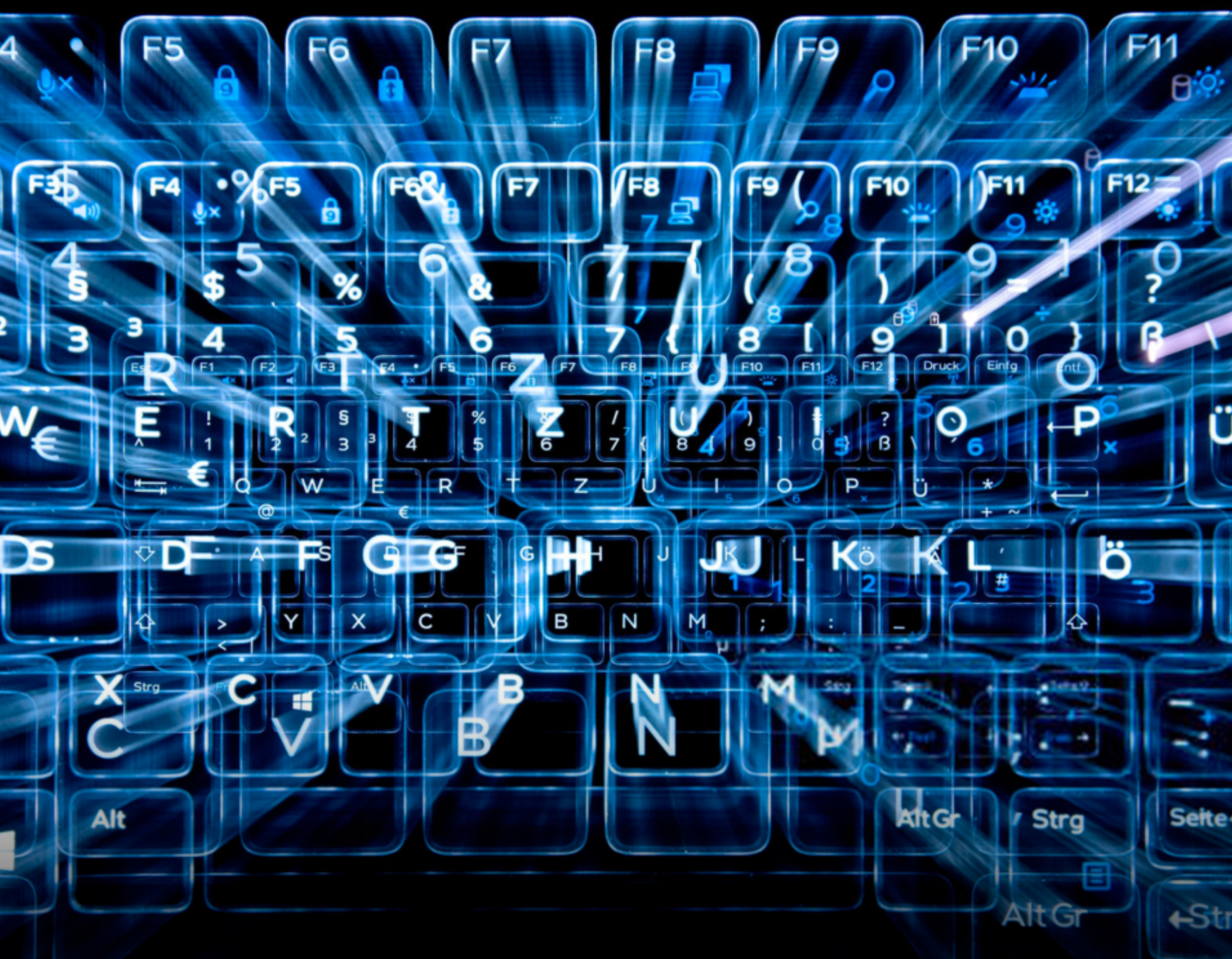
DOXING

PELIGRO EN LAS REDES



Defensoría
Provincia de Buenos Aires

OBSERVATORIO DE DERECHOS
DE NIÑOS, NIÑAS Y ADOLESCENTES

¿QUÉ ES EL DOXING?

El doxxing o doxing es el término procedente de la abreviación de documentos en inglés (dox). Es una forma de acoso que consiste en revelar en internet datos o documentos personales o, directamente, la identidad completa de una persona, sin su consentimiento: dirección, correo electrónico, números de teléfono y hasta nombres de sus familiares más cercanos. El objetivo es causar angustia, pánico o alarma. Adolescentes, jóvenes y personas adultas pueden ser victimas de este accionar.

METODOLOGÍAS MÁS USADAS PARA OBTENER INFORMACIÓN PERSONAL

REDES SOCIALES

Se recopilan todo tipo de mensajes que volcamos en plataformas como Twitter, Facebook o Instagram.

BÚSQUEDA EN INTERNET

Uno de los métodos principales es recopilar mensajes públicos puestos en la red. Ejemplo: un foro abierto donde cualquiera, tenga o no usuario, puede ver qué hemos escrito en un determinado momento. También los comentarios que podamos dejar en alguna noticia.

PÁGINAS WEB

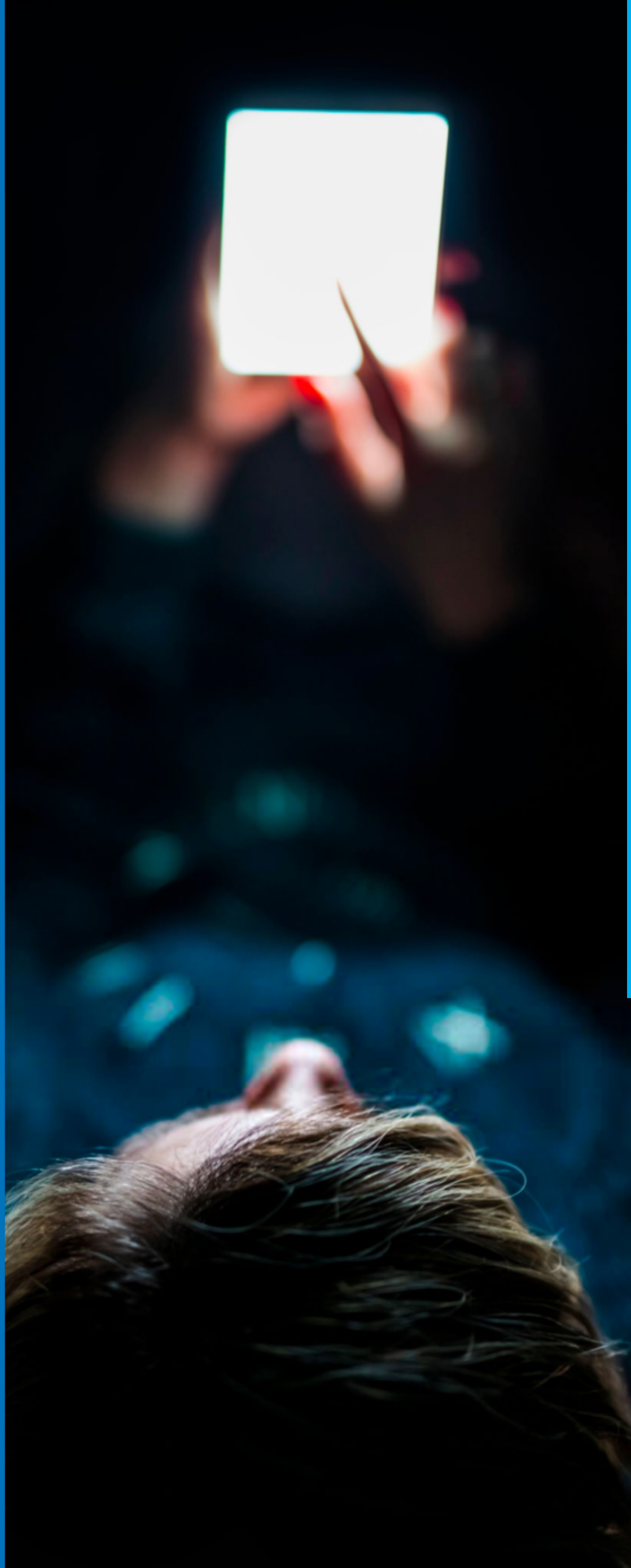
Si observamos con detenimiento el pie de imprenta de un sitio web o blog contiene datos concretos de personas y empresas.

DIRECCIONES Y GUÍAS TELEFÓNICAS:

También se pueden encontrar en línea bases de datos con direcciones y números de teléfono.

INGENIERÍA SOCIAL

Los/as atacantes se hacen pasar por personas de confianza en Internet y manipulan a las víctimas y a sus familiares para que entreguen la información voluntariamente.



¿CÓMO PREVENIR?

• Configurá adecuadamente la seguridad y privacidad de los perfiles sociales.

• Los perfiles de redes sociales tienen ajustes de privacidad que pueden resetearse fácilmente, y muchas webs como las White Pages (páginas blancas) dan la opción de no mostrarte.

• Evitá usar un único nombre de usuario/a para todas las redes sociales.

• Utilizá redes VPN (red privada virtual) para ocultar la dirección IP a terceros en la web. Las VPNs funcionan desviando tus datos de internet a través de un túnel a un servidor de terceros, evitando que se muestre tu dirección IP (y ubicación real).

• Revisá publicaciones antiguas de Twitter o Facebook y borrá las que sean susceptibles de ser manipuladas y/o que contengan datos sensibles.

• Buscá qué se dice sobre vos en Internet.

• Configurá alertas en Google de manera que, si un sitio muestra algún dato personal, automáticamente el buscador avise y puedas intentar poner remedio hablando con el /la responsable para que lo elimine.

• Herramientas como JustDeleteMe nos permite encontrar información sobre nuestros datos personales almacenados en la web y analizar si debemos eliminar los perfiles que ya no utilizamos.

• Vigilá con quiénes y dónde compartes tu número telefónico ya que permite saber la ubicación o acceder a la fotografía de perfil en aplicaciones de mensajería instantánea y redes sociales.

• Revisá las políticas de privacidad y verificá si los datos que solicitan son proporcionales al servicio que brindan con carácter previo a la instalación de aplicaciones.

• Conservá separadas las cuentas de correo personal y profesional.

• No expongas información personal de forma pública.

• Evitá servicios o plataformas dudosos.

• Utilizá programas de seguridad.

• Tener un buen antivirus puede ser la mejor solución para evitar la entrada de malware que pueda recopilar datos personales, contraseñas y, en definitiva, afectar la privacidad.

Fuente: Pantallas Amigas | *https://www.pantallasamigas.net/doxing-venganza-violacion-privacidad-internet-ciberseguridad/*

https://en.wikipedia.org/wiki/Doxing

https://psicologiaymente.com/forense/doxing