# Módulo 4 INTERNET - PELIGROS

***Internet – Peligros***

## ¿QUÉ RIESGOS Y AMENAZAS EXISTEN EN INTERNET?

Hay muchas y muy diversas formas de ataque a los datos personales. Las mismas van cambiando a lo largo del tiempo y van adquiriendo múltiples y nuevas modalidades a medida que se generan avances tecnológicos.

Si bien pueden ser muy distintas unas de otras, todas tienen la misma finalidad: acceder a información personal de los usuarios, ya sea para fines delictivos, fines de espionaje o fines comerciales. Las amenazas informáticas más conocidas son los distintos tipos de malware o software maliciosos (ver glosario) que tienen el objetivo de introducirse en cualquier dispositivo electrónico para alterar sus sistemas, robar datos y tomar control remoto de ellos.

En general, solemos ver los riegos relacionados con la tecnología como factores externos al uso que cada uno le da a Internet, y muchas veces no los percibimos como derivados de las propias prácticas.

Es por eso que creemos necesario nombrar tres prácticas actuales que tienen consecuencia en la protección de nuestros datos personales y en nuestra privacidad: el *sexting*, el *ciberbullying* y el *grooming*.

### ¿QUÉ ES EL *SEXTING*?

**Sexting es un término inglés conformado por la unión de dos palabras: sex (contenido sexual) y texting (textear/enviar mensajes), y que refiere al envío de imágenes/videos de contenido sexual a otra/s persona/s tanto a través de distintos servicios de mensajería instantánea como de redes sociales, correo-e y foros.**

**En general, lo que se difunde son imágenes personales y más específicamente, imágenes relacionadas con la sexualidad (a los que antes llamamos datos sensibles). Si bien el envío de fotos se hace entre dos personas o un grupo, la circulación de la imagen puede derivar en que la misma sea publicada en un sitio web o viralizada.**

**Si bien el sexting se lleva a cabo tanto por jóvenes como por adultos, es una práctica muy usada entre los adolescentes.**

## ¿QUÉ ES EL *CIBERBULLYING*?

El ciberbullying es llevar la ya conocida práctica del bullying –u hostigamiento escolar– al plano online. Consiste en el uso y difusión de datos difamatorios y discriminatorios a través de las diferentes plataformas y herramientas que ofrece Internet, como las redes sociales y la mensajería instantánea.

En general, el ciberbullying tiene características propias:

- La viralización: los chicos en general no tienen noción sobre el alcance que puede tener una publicación dado que, como se señaló antes, Internet produce una circulación constante de información que puede generar que desconocidos o personas ajenas al grupo donde se realiza la acción accedan al contenido difundido.

- Rapidez: la circulación de la información se produce en segundos, por lo que no sólo se expande por toda la red sino que lo hace a gran velocidad.

- La sensación de anonimato: al llevar adelante la acción mediante un dispositivo, se crea una sensación de anonimato que genera la creencia de minimizar la agresión.

## ¿QUÉ ES EL *GROOMING*?

El grooming es la acción deliberada de un adulto de contactar a un niño o niña a través de distintos canales de Internet para ganar su confianza con el fin de acosarlo sexualmente.

Estos adultos suelen crear un perfil falso en una red social o sala de chat haciéndose pasar por un chico o una chica, y entablan una relación de amistad y confianza con la persona que quieren acosar.

Una vez que se establece esta relación de confianza, el adulto –siempre haciéndose pasar por un menor– suele pedir una foto o video con contenido sexual y, ya en poder de ese material, comienza un periodo de extorsión en el que se amenaza al niño o niña con hacerlo público si no accede a un encuentro personal.

En nuestro país, desde 2013 el grooming encuentra regulación en el Código Penal (Ley 26904) con una pena de hasta 4 años de prisión por considerarse una práctica preparatoria para un abuso sexual.

# Qué es el skimming y cómo proteger tu tarjeta

El skimming se produce cuando a un cajero automático se le agrega una boquilla falsa en la ranura donde se inserta la tarjeta y una cámara que filma el ingreso del código PIN. El cibercriminal utiliza los datos robados para cometer operaciones fraudulentas.

## ¿Cómo me protejo?

**1. OCULTÁ**
tu código PIN
al ingresarlo

**2. REVISÁ**
que el cajero no tenga
piezas flojas o agregados
extraños

**3. EVITÁ**
los cajeros que no están
dentro de los bancos

Fuente del material:

Defensoría del Pueblo
Ciudad Autónoma de Buenos Aires

BBVA Francés