talleres TI

Cibercuidados para Adolescentes

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología

Internet, las Redes Sociales y la Información Personal

¿Qué son las redes sociales?

Vamos a comenzar hablando de algo que posiblemente la mayoría de ustedes utilizan: las redes sociales.

De modo general, podríamos decir que una red social es un medio de comunicación social en línea, en donde cada persona usuaria tiene la posibilidad de, a través de un registro, hacerse de un espacio propio y contactarse con otras personas.
Las redes sociales permiten compartir contenidos (como textos, imágenes y videos, dependiendo de la plataforma) con los otros participantes de la red, así como también interactuar de forma virtual con otras personas.

¿Cuáles son las redes más usadas?

Internet como espacio público

Imaginen que viviéramos en una ciudad en la que todas las personas habitantes tuvieran una cartelera en la puerta de su casa, donde comparten información con sus vecinos.

Si alguien pone un cartel que diga “voy a la escuela n° 5” o “me fui de vacaciones”, todas las personas que pasen por esa cuadra van a saberlo. ¿Le darían esa información a cualquier persona desconocida? Lo más probable es que no.

Información personal

Ahora imaginen que una persona desconocida ingresa a alguno de los perfiles de ustedes en redes sociales, ¿con qué información se encontraría?

- Nombre y apellido
- Nombre de familiares y amigos
- Imágenes de tu rostro y aspecto físico
- Gustos e intereses
- Información sobre la escuela a la que vas
- Lugares que frecuentás y eventos a los que asistís

Esa persona tendría toda o parte de esta información, ¡sin ni siquiera conocerte en persona! Entonces, si bien no pondríamos un cartel en la puerta de nuestra casa con todos esos datos, muchas veces, sin darnos cuenta, hacemos eso mismo en las redes sociales. Nunca sabemos quién va a encontrarse con esa información y para qué puede utilizarla; y así como siempre hay personas en las que podemos confiar, también hay mucha gente que tiene malas intenciones.

Para reflexionar: te sugerimos que en otro momento hagas la prueba de poner tu nombre en el buscador y ver qué información aparece. ¿Cómo tenés configurada la privacidad de las redes sociales? ¿Aparecen sitios e información que no te imaginabas que aparecería?

Falseo de identidad virtual

Uno de los grandes riesgos que presenta internet tiene que ver con las personas que se hacen pasar por otras, construyendo una identidad virtual falsa. De esta forma, buscan averiguar información personal de los demás, utilizando nombres y datos falsos. Pueden intentar conseguir datos como tu nombre y apellido, tu DNI, tu correo electrónico, dirección, gustos o contraseñas, así como fotos personales y hasta íntimas. Por eso, hay que tener muy presente que cuando enviamos fotos personales, de familiares o amigos/as a otros contactos, o cuando las

compartimos en redes sociales, éstas pueden ser utilizadas para cosas muy diferentes a las que imaginamos.

RESPONSABILIDAD SOCIAL EN INTERNET

A lo largo de esta charla, vamos a ver algunas prácticas que se llevan a cabo en contextos digitales, frente a las cuales es necesario adoptar una actitud de responsabilidad social. Es importante conocerlas para poder prestar atención y saber cómo prevenir posibles daños, ya sean personales o hacia otras personas.

Luego de ver de qué se trata cada una de ellas, veremos algunas medidas generales de prevención que podemos tomar en las distintas redes sociales para evitar riesgos.

Ciberbullying o ciberacoso

El ciberbullying tiene lugar cuando una persona sufre amenazas, hostigamiento, humillación u otro tipo de molestias de forma reiterada y deliberada (es decir, a propósito) a través de medios electrónicos. Generalmente, se realiza entre pares. Este acoso se puede dar mediante la publicación de textos, imágenes, videos y audios a través de los distintos medios digitales como redes sociales, mensajería instantánea (Whatsapp), mails, aplicaciones, videojuegos, etc.

Además de la angustia generada por la agresión en sí misma, se le suma el agravante de la posibilidad de viralización; es decir, que un contenido humillante empiece a ser compartido y difundido a una cantidad creciente de personas usuarias.

En la escuela o el barrio, lamentablemente solemos ver que hay chicos que maltratan o se burlan de otros. El ciberbullying es esta misma práctica llevada al contexto digital. El acoso es virtual, pero el daño es real.

Roles en el ciberacoso

Veamos cuáles son los roles típicos en un caso de ciberacoso:

a. La persona que acosa: normalmente necesita manifestar su poder humillando a otras personas.

b. La persona que es acosada: es quien sufre la humillación y/o discriminación.

c. Las personas espectadoras: son quienes ven la agresión desde fuera, y de alguna forma, están siendo cómplices del acto. En internet, quienes comparten y potencian la información difamatoria, por más que no sean quienes la producen, también están participando de la agresión.

Cortar el círculo de la humillación también es una forma de ayudar. Si somos testigos de una situación en la web que nos parece agresiva, debemos denunciarla y desalentar su difusión, siempre de forma respetuosa, sin responder con el mismo odio o violencia.

Formas de ciberbullying

Estos perfiles que acabamos de ver no son fijos, es decir, que alguien que está en el rol de la persona que acosa puede en otro momento estar en el lugar de la persona humillada, en el de la persona espectadora o a la inversa. Además, tengamos en cuenta que las consecuencias negativas del ciberbullying no son únicamente para la víctima (que obviamente es quien sale más dañada), sino también para quien acosa y sus cómplices. Esto cobra especial sentido si tenemos en cuenta una de las cuestiones que vimos anteriormente: todo lo que un usuario publica en la red quedará asociado a su nombre.

¿Cómo prevenir?

- **Elegir qué subimos a las redes y con quién lo compartimos**. Hay información que es mejor reservarla para un ámbito íntimo o de confianza, porque al exponerla públicamente puede descontextualizarse y ser entendida o usada con otro sentido.

- **Configurar la privacidad**. Los dispositivos y las redes sociales brindan herramientas de configuración de la privacidad, para proteger la seguridad de nuestras cuentas y equipos. Usar contraseñas seguras y difíciles.

¿Qué hacer?

- **Charlar con una persona de confianza**. En el caso de que sintamos que estamos siendo víctimas de una situación que nos angustia, lo mejor siempre es hablarlo y en ningún caso responder con la misma violencia, ya que eso no va a solucionar el conflicto. A veces es mejor no esperar a que la situación se vaya de las manos, sino que una vez que reconocimos el malestar y su causa, acercarnos a alguna persona adulta de confianza con quien sintamos comodidad para charlar sobre el tema.

- **Bloquear el perfil de quien acosa**. Si detectamos a alguien que nos está molestando o agrediendo por medio de las redes sociales, lo mejor siempre es bloquear o reportar a ese contacto.

¿Qué hacer si veo que molestan a un compañero/a?

¡No te quedes indiferente!

- Cuando se burlan o molestan a un compañero, no te rías.
- Si ves una publicación ofensiva o humillante en redes sociales, no la compartas.
- Pensá cómo te sentirías si te lo hicieran a vos.
- Acercate a quien está solo e intentá acompañarlo.
- Buscá a una persona de confianza y hablá de lo sucedido.

SEXTING

Sexting: ¿qué es?

El sexting implica la circulación de un contenido sexual propio (como fotos o videos íntimos) a través de dispositivos móviles (celulares, computadoras, tablets) mediante diversas aplicaciones (Whatsapp, Facebook, Instagram, Twitter, mail, foros, etc.).

Su nombre surge de la combinación de las palabras en inglés sex (sexo) y texting (enviar mensajes de texto por teléfono celular).

Si bien el sexting no es una conducta dañina en sí misma, conlleva algunos riesgos.

Las imágenes que componen el fenómeno del sexting son obtenidas, en la mayoría de los casos, de manera voluntaria. Es decir, quien envía el material aparece revelando su identidad y es consciente de ello, lo hace en un contexto de intimidad y confianza.

Pero esto no significa que exista un consentimiento para la divulgación de esos contenidos.

El problema se presenta si esas imágenes son reenviadas por la persona receptora a otros contactos, publicadas en Internet y redes sociales o encontradas por terceros que las hacen públicas, derivando en ciberacoso.

Causas de viralización

Estas imágenes pueden comenzar a circular viralmente a causa de:

- Descuido o traición del destinatario.
- Hackeo o robo de dispositivos en manos de un tercero.

Sexting: consecuencias negativas
La circulación de una imagen de contenido sexual puede conducir a:

- **Sextorsión:** la imagen sexual puede ser usada por un tercero para extorsionar al protagonista con hacerla pública. Esta actitud configura un delito penado por la ley.
- **Ciberbullying:** la difusión de una imagen íntima puede llevar al acoso de la víctima, sea por críticas a su apariencia o por prejuicios sobre su conducta.
- **Grooming:** si quien consigue esas imágenes es una persona adulta y las utiliza para acosar a la persona menor, estaríamos frente a un caso de grooming y, como veremos más adelante, es un delito penado por la ley.
- **Daño a la reputación online:** como vimos, en internet el material perdura a través del tiempo, exponiendo la identidad del protagonista en cualquier búsqueda online, presente o futura. Podría ser encontrada, por ejemplo, por una potencial persona empleadora.

Sexting: ¿cómo prevenir consecuencias negativas?

Como podemos imaginar, el hecho de que adquiera circulación masiva una imagen o video que tenía un sentido específico en un contexto íntimo y privado, puede llevarnos a un nivel de exposición que nos genere mucha incomodidad. Por eso, es necesario pensar dos veces antes de enviar fotos o videos con contenido sexual ya que, una vez enviados, perdemos el control sobre su recorrido. Si te sentís con dudas o presión para mandar una foto o video, siempre es preferible negarse antes que arrepentirse luego con las consecuencias.

Si la otra persona realmente te quiere, tiene que respetar tu decisión y no presionarte a hacer cosas que no querés.

Recomendaciones para el sexting seguro

- En el caso que decidas practicar sexting, siempre tomá las medidas necesarias para preservar tu identidad: **evitá exponer tu cara o partes del cuerpo que te identifiquen** (como tatuajes, marcas de nacimiento, etc.).
- Además, conviene **usar herramientas que eliminen el contenido** segundos después de ser enviado e impidan la captura de pantalla.
- Por otro lado, es indispensable la **elección de contraseñas confiables y la configuración de privacidad** en redes sociales.

Sexting: ¿qué hacer?

Así como tenemos que cuidarnos con la información personal que enviamos a través de las redes, tampoco debemos compartir, reenviar o difundir fotos o videos con contenido sexual de personas que no brindaron su consentimiento. Es importante que aprendamos a generar una convivencia digital respetuosa, en la que podamos cuidar la imagen propia y ajena.

En el caso de que seamos testigos de la circulación de imágenes de sexting en nuestras redes sociales, debemos reportar las imágenes y pedir su baja. Este pedido es anónimo, por lo que no hay que tener miedo de hacerlo.

GROOMING

Grooming: ¿qué es?

Se denomina grooming a la situación en la que una persona adulta acosa sexualmente a una persona menor mediante el uso de internet buscando un encuentro personal o conseguir imágenes íntimas de la víctima (generalmente en ropa interior). Es decir que, a diferencia del cyberbullying en el que las partes involucradas son pares, aquí quien acosa es una persona adulta que hostiga a una persona menor.

En Argentina, el grooming es un delito penado por ley, con una penalización que incluye prisión de 6 meses a 4 años.

Formas de grooming

Existen dos maneras en las que la persona adulta puede conseguir las imágenes personales de la persona menor.

1. A partir del hackeo de cuentas
2. Con fase previa de generación de confianza

1. Formas de grooming: hackeo de cuentas

En este tipo de grooming, la persona que acosa logra tener fotos o videos sexuales de chicos mediante la obtención de contraseñas o hackeo de cuentas; es decir, a la fuerza. Una vez que consigue el material, extorsiona a la víctima con mostrarlo si esta no le entrega más material o si no accede a un encuentro personal. En estos casos, la víctima puede no saber cómo consiguió el material.

2. Formas de grooming: con fase previa de generación de confianza

La otra manera en la que suele darse el grooming es a partir de una fase previa de generación de confianza, lo que implica que sea el propio menor quien le entregue el material a la persona acosadora. En estos casos, la persona adulta

miente sobre su identidad, haciéndose pasar por una persona menor de edad. Esto lo logra a partir de hacerse un perfil falso en una red social, foro o videojuego, en donde simula ser también un menor para entablar una relación de "amistad" con la víctima. Una vez que logra su confianza, suele pedirle una foto o video íntimo con contenido sexual. Pasado un cierto tiempo, la persona acosadora suele pedir también un encuentro personal; si el menor no accede, puede amenazar con divulgar las imágenes. Este es el punto más riesgoso, al que jamás se debe acceder.

Es importante que los participantes comprendan al grooming no como un acto aislado, sino como un proceso que puede durar días y hasta meses de persuasión, manipulación y extorsión. Esto da cuenta de que los niños/as y adolescentes pueden detener el vínculo con quien acosa en cualquier momento del proceso, seguido de una comunicación inmediata de la situación a la familia o personas adultas de referencia.

¿Cómo prevenir?

La mejor manera de prevenir el grooming (así como cualquier tipo de acoso) es:

- **Ser muy cuidadosos/as a la hora de compartir o enviar información o imágenes íntimas** en redes sociales o chats, especialmente si se trata de personas usuarias a las que nunca conocimos en persona. También tener en cuenta que la información pública que exponemos en nuestras redes puede ser utilizada por quien acosa para aparentar similitud de intereses y así generar un vínculo.
- **Apagar la cámara web cuando chateamos**, ya que del otro lado pueden estar grabando nuestra imagen.

- **Utilizar un sobrenombre como nick o usuario** cuando jugamos online. Es preferible no usar nuestro nombre completo y evitar usar el apellido.
- **Configurar la privacidad** y seguridad de nuestras cuentas y dispositivos.

¿Qué hacer?

- **Charlar con una persona de confianza.** Si detectamos que estamos siendo víctimas de un caso (o un posible caso) de grooming, lo mejor siempre es acercarnos a una persona de confianza con quien podamos hablar sobre el tema. Para realizar una denuncia penal, esa persona debe ser adulta. No hay que avergonzarse de la situación, tenemos que saber que fuimos víctimas de un chantaje y eso bajo ningún punto de vista es nuestra culpa.

Como mencionamos anteriormente, en **Argentina el grooming es un delito penado por ley**, con una penalización que incluye prisión de 6 meses a 4 años. Por eso, en el caso de hacer la denuncia penal acompañados por una persona adulta, debemos guardar las pruebas del acoso (no borrar conversaciones o datos que puedan ser útiles a la justicia).

- No borres ningún contenido de la computadora o teléfono celular: las conversaciones, imágenes y videos que la persona acosadora envió deben ser guardados como prueba.
- No amenaces, increpes ni mantengas una conversación con la persona abusadora.

Ante un caso o posible caso de grooming, existen los siguientes canales de asesoramiento y denuncia:

- Línea 137: ayuda y atención a víctimas de violencia familiar y sexual. Es gratuita, nacional y brinda contención, asistencia y acompañamiento las 24 horas, los 365 días del año.

- Línea 102: servicio gratuito y confidencial, de atención especializada sobre los derechos de niñas, niños y adolescentes. Podés llamar ante una situación de vulneración de derechos, si necesitás asesoramiento o simplemente si necesitás hablar con alguien.

-Por Whatsapp al (54911) 3133-1000.

- En cualquier dependencia policial o fiscalía del país tienen la obligación de tomar la denuncia.

Estafas online

Phishing

Es un tipo de estafa en la que un ciberdelincuente recurre a la suplantación de identidad para obtener información confidencial de sus víctimas, como contraseñas o claves bancarias.

Término derivado de las palabras en inglés “password harvesting fishing”, que pueden traducirse como “cosecha y pesca de contraseñas”.

El ***phishing bancario*** consiste en que la víctima reciba un correo electrónico de un supuesto banco, que le solicita -por el hecho de ser cliente- que valide su usuario y contraseña de acceso a homebanking. Usualmente, el cuerpo del mensaje contiene un enlace que deriva a un sitio web falso creado por el estafador para que la víctima coloque sus credenciales de acceso a homebanking

Estafas por WhatsApp

Las estafas por WhatsApp consisten en dos etapas:

- **Suplantación de identidad**: el ciberdelincuente busca obtener el código de verificación de WhatsApp de la víctima para clonar la línea.
- **Pedido de dinero**: una vez que logró clonar la línea, suele escribirle a los contactos de esa cuenta pidiendo una transferencia de dinero, haciéndose pasar por el propietario original.

Prevención de las estafas online

Es importante recordar que nunca una organización, ya sea pública o privada (como un organismo de gobierno, un banco, una empresa, una tarjeta de crédito o una ONG, entre otras), va a solicitar datos personales de un cliente o usuario por vías alternativas de contacto tales como el correo electrónico, los servicios de mensajería del celular, SMS, redes sociales o sitios web. Por lo general, estos datos se piden cuando es el cliente quien se comunica con alguna de esas organizaciones.

- Nunca abras correos electrónicos o ingreses a enlaces que te resulten sospechosos o que no esperabas recibir. Revisá detalladamente la dirección del mail y chequeá cada letra para ver si es la original que ya conocés, es decir, la que figura en la página oficial de tu banco u organización conocida. Los cibercriminales suelen cambiarle a la dirección una letra, número o símbolo para engañarte.

- Otro factor a tener en cuenta son los errores gramaticales. Tené presente que ninguna empresa seria enviará un correo electrónico que esté mal redactado, no sea claro o tenga faltas de ortografía.
- Tampoco realices ninguna acción si recibís un correo que te indica actuar de forma inmediata, con límite de tiempo o te cause miedo.
- Nunca compartas tu código de registro ni el PIN de la verificación de Whatsapp con otras personas.
- Para evitar el clonado de tu línea: activá la verificación de dos pasos y proporciona una dirección de correo electrónico en caso de que olvides tu PIN.

CONSEJOS DE NAVEGACIÓN SEGURA

Vamos a ver algunos consejos generales para realizar una navegación segura en internet.

- Usar contraseñas seguras.
- Tener al día las actualizaciones.
- Usar antivirus.
- Bloquear los dispositivos con código, huella o patrón.
- Configurar la privacidad en redes sociales.
- Pensar dos veces antes de enviar o publicar una imagen.
- Estar atentos a las personas que buscan interacción con nosotros.
- No abrir correos ni enlaces de desconocidos.
- Descargar contenidos solo si la fuente es confiable.

¿Cómo crear contraseñas seguras?

Éstas son la primera línea de defensa frente a una invasión a la intimidad.

- No hay que incluir datos personales (cumpleaños, nombre, apellido) ni construcciones simples como “1234”.

- Elegir una frase o combinar palabras significativas.
- Lo ideal es combinar letras, números y signos de puntuación, así como mayúsculas y minúsculas.
- Se recomienda usar distintas contraseñas para distintos dispositivos y cuentas (así si vulneran uno, no caen en cadena los demás).
- Es recomendable cambiarlas periódicamente (dos veces por año).
- Si vas a anotarlas para no olvidarlas, hacelo en un cuaderno, nunca en el dispositivo.

Frenar lo que incomoda o asusta

Siempre es preferible frenar cualquier interacción cuando lo que sucede, nos asusta o incomoda. Así que no dudes en bloquear y/o reportar a quien te esté molestando o incomodando en las redes. En estos casos, lo mejor es confiar en la propia intuición.

Saber que el “mundo online” es parte de la “vida real”

Es importante tener en cuenta que en el “mundo virtual” no deberíamos hacer nada que no haríamos en nuestra vida fuera de internet.

talleres TI

Jefatura de Gabinete de Ministros
República Argentina

Secretaría de Innovación, Ciencia y Tecnología