Ciberseguridad

Cómo protegerte en internet

UNICEF México / Rodrigo López Orozco

El 70% de los mexicanos usan internet y los principales usuarios son adolescentes y jóvenes como tú. Tan solo entre el 80 y 94% de los jóvenes 12 a 17 años, tienen acceso a internet o una computadora[1].

Internet es un lugar buenísimo para encontrar información, chatear, estar en contacto con las personas que quieres, seguir con tus estudios y también encontrar mucho contenido para divertirte. Lo malo es que internet también representa riesgos, por ejemplo, según algunas encuestas nacionales, 25% de las y los adolescentes de entre 12 y 17 años ha vivido alguna forma de ciberacoso en México[1].

Además del ciberacoso, estamos sujetos a otros riesgos como el robo de información, las noticias falsas y el *sexting* sin medidas de seguridad. Por eso UNICEF y U-Report lanzamos una encuesta para conocer cuánto saben las y los jóvenes sobre ciberseguridad, participaron más de 12 mil jóvenes por medio de WhatsApp y Facebook Messenger.

Sexting

¿Qué es? Es enviar fotos o videos de uno/a mismo/a con carácter sexual a otra persona mediante un dispositivo como teléfono o tablet[2]. Aunque hacerlo es una decisión muy personal, es importante saber que **es una práctica riesgosa.**

UNICEF México / Rodrigo López Orozco

UNICEF México / Rodrigo López Orozco

Quienes lo practican de manera más seguras toman estas precauciones

1. **Asegurarse de que la persona es digna de confianza** y que hay un mutuo acuerdo de cuidar la privacidad e intimidad de los involucrados.

2. **Buscar la confirmación** de que la otra persona desea recibir este tipo de contenido ya que puede ser que la persona esté

coqueteando y no quiera sextear, o puede ser que quiera escribir, pero no recibir y/o enviar fotos.

3. **Excluir la identidad** de la foto o video: dejar fuera el rostro, cicatrices, tatuajes u objetos alrededor que puedan identificar a la persona..

4. **NUNCA usar redes de wifi** abiertas y revisar que el teléfono u otro dispositivo no tengan *malware* o virus.

5. **Elegir el canal con cuidado** (hay aplicaciones donde todos los contenidos están encriptados y protegidos). Los emails o las redes sociales pueden implicar riesgos como difusión sin consentimiento, pérdida del control, no poder borrar la información, capturas de pantalla y más.

Lo más importante: ***Pensar muy bien antes de hacerlo****, decidir sin presiones y estar consciente del riesgo que se corre al practicarlo.*

Si se ha recibido contenido de carácter sexual sin consentimiento, es importante denunciar ante la Guardia Nacional[5]:

- Centro Nacional de Atención Ciudadana, número telefónico 088
- Correos de Denuncia: cnac@gn.gob.mx y guardia.nacional@gn.gob.mx

- Y vía Twitter en @CNAC_GN

Privacidad y protección de datos

Cuando navegas en internet, redes sociales y otras aplicaciones tienes que preocuparte por implementar mecanismos de seguridad para evitar robos de información, de identidad, perdidas de datos y otros múltiples riesgos.

¿Qué es *malware*?

Es un código malicioso diseñado para infiltrarse en tu dispositivo cuando lo instalas o descargas, aunque no necesariamente te das cuenta[3]. Cuando hay uno en tu computadora, teléfono o tableta, puede:

- Acceder a toda tu información, incluyendo ubicación en tiempo real y lista de contactos.
- Acceder a tus fotos y archivos y publicarlos en internet o en páginas maliciosas y tu ni en cuenta
- Hackearte contraseñas, email, redes sociales y demás.

Hay algunas prácticas que hacen que sea más sencillo que tu dispositivo adquiera un *malware*, a veces son acciones tan cotidianas que no nos damos cuenta de que pueden ser riesgosas.

Por ejemplo, en la encuesta, solo el 34% declaró NO descargar aplicaciones, películas, videojuegos y demás, en sitios "pirata", 7% nunca actualiza

sus apps o el sistema operativo del dispositivo y 27% se conectan seguido a redes públicas de WiFi.

UNICEF México / Rodrigo López Orozco

UNICEF México / Rodrigo López Orozco

OJO con lo que compartes

Además del *malware* que puede robar tus datos, tú mismo/a puedes ponerte en riesgo al compartir información personal con otras personas y ser susceptible al robo de identidad. Por ejemplo, al tener las redes sociales públicas te expones riesgos como, suplantación de la identidad, ciberbullying, extorsión cibernética, grooming, robo de datos y más.

Tips para que no compartas de más:

- No guardes tus contraseñas física o virtualmente en un lugar donde cualquier persona tiene acceso. Mejor asegura tus contraseñas usando un gestor o administrador como LastPass o 1Password.
- Te recomendamos hacer todas tus redes sociales privadas y no aceptar nunca a alguien que no conoces.
- No uses conexiones de wifi abiertas y si tienes que hacerlo NUNCA pongas información sensible (como tus contraseñas, datos bancarios, dirección, etc.)

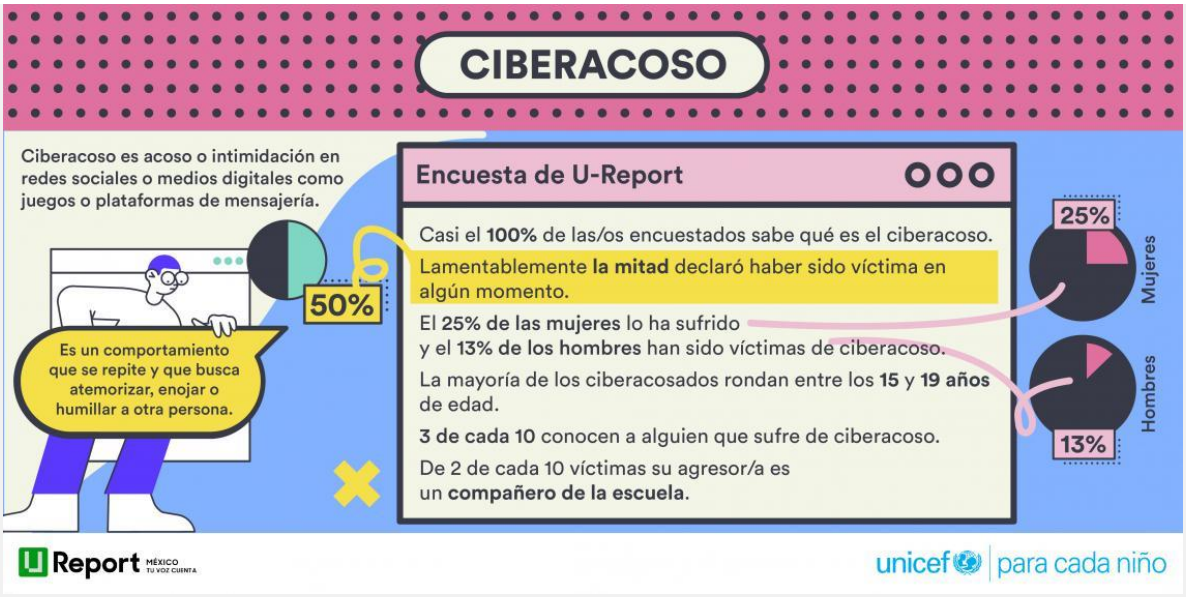
UNICEF México / Rodrigo López

Ciberacoso

Ciberacoso es acoso o intimidación por medio de las redes sociales o medios digitales como juegos o plataformas de mensajería. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas[6]. Por ejemplo:

- **Difundir mentiras, burlas** o publicar fotografías vergonzosas de alguien.

- **Enviar mensajes hirientes** o amenazas a través de las plataformas de mensajería.
- **Hacerse pasar por otra persona** y enviar mensajes agresivos en nombre de dicha persona.



UNICEF México / Rodrigo López

Más datos…

- 7 de cada 10 de han sido principalmente victimizados por redes sociales.
- 4 de cada 10 no conocen la identidad de su agresor.
- A las y los que respondieron haber sido víctimas de ciberacoso escolar, les preguntamos si han faltado a la escuela por este motivo.
- Poco más de 3 de cada 10 han faltado a la escuela debido al ciberacoso. El 43% dijo que no ha faltado, sin embargo, al 16% les gustaría hacerlo.

UNICEF México / Rodrigo López

Sé amable en línea

46% de los encuestados respondió “prefiero no contestar” a la pregunta: ¿tu círculo de amig@s hace ciberacoso a otras personas?

Todos los amigos se hacen bromas entre ellos, pero hay ocasiones en que es difícil saber si alguien solamente se está divirtiendo o si está tratando de herirte, sobre todo en internet. A veces te dirán, riéndose, que “era solo una broma” o que “no te lo tomes tan en

serio”. Pero si te sientes herido o piensas que alguien se está riendo de ti y no contigo, entonces la broma ha ido demasiado lejos[5].

Si ves que esto le está ocurriendo a alguien que conoces, procura ofrecerle apoyo y no ser parte del acoso.
Cuando el acoso ocurre en línea, la víctima siente como si la estuvieran atacando en todas partes, hasta en su propia casa. Tu salud mental, emocional y hasta física se pueden ver afectadas y parecería que no hay salida. Pero sí hay, recuerda que no estás sola, no estás solo.

UNICEF México / Rodrigo López

Recomendaciones ante el ciberacoso:

- Si piensas que te están acosando, lo primero que debes hacer es buscar ayuda de alguien en quien confíes, por ejemplo, tu padre o tu madre, un familiar cercano u otro adulto de confianza.
- Cuida la privacidad de tus redes y medios digitales.

- No respondas o tomes represalias: En algunas ocasiones es peor que reacciones, porque justamente es eso lo que el agresor está buscando.
- Guarda todas las evidencias
- Si alguien que conoces está siendo acosado, actúa.
- Bloquea. Cada red social ofrece la posibilidad de bloquear al acosador y reportar sobre su comportamiento. Las empresas de redes sociales tienen la obligación de velar por la seguridad de sus usuarios.
- Si estás en peligro inminente, puedes llamar al 911 o denunciar ante la Guardia Nacional5:
  Centro Nacional de Atención Ciudadana, número telefónico 088.
  También puedes denunciar por internet.
  Correos de Denuncia: cnac@gn.gob.mx y guardia.nacional@gn.gob.mx
  Y vía Twitter en @CNAC_GN

Noticias falsas

A veces las noticias falsas son más compartidas que las verdaderas por eso debemos ser cuidadosos con lo que compartimos en redes sociales, ¡la desinformación puede llegar a ser muy peligrosa! **Hay estudios que indican que es 7 veces más probable que las noticias falsas se vuelvan virales[4].**

Más del 80% de las y los encuestados por U-Report sabe que las *fake news* pueden volverse más virales, sin embargo, el 50% de ellos no sabe detectar una.

Además, el 60% opina que implica mucha responsabilidad y riesgo compartir, dar *like*, comentar o viralizar una noticia falsa.

2 de cada 10 declaran compartir noticias con solo haber leído el título y sólo el 50% de las y los encuestados consultan la fuente de la noticia o artículo.

Todas y todos tenemos responsabilidad cuando se trata de compartir fake news o noticias falsas. Tienes que ser consciente del peligro que puede causar la desinformación y pensar muy bien antes de compartir una noticia.

UNICEF México / Rodrigo López

Recomendaciones para NO compartir información falsa:

- Siempre, siempre, tienes que leer la noticia entera y no solo el titular.
- Cuando un título es muy extremista o te genera emociones muy fuertes, normalmente es un ciberanzuelo (o *clickbait*) a una noticia falsa.
- Verifica las fuentes, nos llegan muchos mensajes reenviados en WhatsApp y no siempre es información verdadera. Asegúrate que es algo real buscando la información en los principales buscadores.
- Cuando la noticia incluya el nombre de un autor o el medio donde se publicó, búscalo en Google o los principales buscadores y si es una cadena sin autor; desconfía y preferentemente no la compartas.
- Comparte esta información con tus amigos y tu familia para que más personas sepan identificar las noticias falsas.

UNICEF México / Rodrigo López

Desconectarse

Cuidar tu salud mental también es importante, pasamos mucho tiempo conectadas/os, más en estos tiempos de pandemia por lo que es muy importante desconectarse de vez en cuando y hacer otras cosas que te gusten.

1 INEGI. Módulo sobre Ciberacoso (MOCIBA-2015)

2 Internet segura 4 kids https://www.is4k.es/necesitas-saber/sexting

3 https://www.avast.com/es-es/c-malware

4 Instituto Tecnológico de Massachusetts

5 https://www.gob.mx/guardianacional/articulos/denuncia-por-internet-ante-la-guardia-nacional-251876?idiom=es

6 https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo