UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

MINI GUÍA DE SEGURIDAD INFORMÁTICA

¡TODO LO QUE TIENES QUE SABER!

INTRODUCCIÓN

Navegar en Internet, hacer uso de las redes sociales y comunicarnos usando la tecnología es una experiencia gratificante y positiva. Cada vez resulta más fácil acceder a Internet usando distintos tipos de dispositivos. Pero el uso de Internet y de otras tecnologías de la información y comunicación tecnologías de la información y comunicación, como los teléfonos, puede tener grandes riesgos para las niñas, niños y adolescentes.

Es por estos riesgos que es necesario que seamos conscientes que existen peligros y amenazas que pueden ser encontradas en Internet y que conozcamos cuáles son las mejores maneras de protegernos de estos.

Esta mini guía de seguridad informática, ha sido preparada por la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) con la finalidad de que las niñas, niños y adolescentes conozcan y puedan protegerse de los distintos tipos de cibercrímenes, sean conscientes de sus derechos en Internet y puedan utilizar las tecnologías de la información y comunicación de manera constructiva. Te invitamos que la leas, y que la compartas con tu familia y amigos.

PELIGROS EN INTERNET

Aunque las tecnologías de la información y comunicación ofrecen muchas oportunidades de comunicación y aprendizaje para las niñas, niños y adolescentes, estas también tienen grandes riesgos. A continuación, te contamos sobre algunas amenazas, a las que podrías estar expuesto en Internet y cómo puedes prevenirlas y cuidarte de ellas.

CYBERBULLYING / CIBERACOSO

¿Alguna vez te has sentido discriminado, o alguien te ha hecho comentarios hirientes a través de redes sociales, email o mensajería instantánea?

¿Alguna vez alguien te ha atormentado, amenazado, hostigado, humillado o molestado a través de redes sociales o por teléfonos móviles?

El Cyberbullying engloba el uso de las tecnologías de información y comunicación, para causar daño de manera repetida, deliberada y hostil. Esto puede incluir, pero no limitarse, al uso de Internet, teléfonos móviles u otros dispositivos electrónicos para difundir o colocar textos o imágenes que dañan o avergüenzan a una persona.

¿QUÉ PUEDO HACER?

- Ten mucho cuidado con la información que pones en Internet. Pon tu configuración privada, de manera que solo tu familia y amigos conocidos puedan interactuar contigo.
- No contestes a las provocaciones o insultos.
- Si te sientes acosado, guarda las pruebas.
- Si te amenazan, pide ayuda con urgencia a tus padres, maestros o un adulto de tu confianza.
- Compórtate con respeto hacia los demás en la red.

GROOMING

¿Has entablado una relación de amistad con alguna persona que conociste en la red, pero desconoces en la vida real?

¿Te han hecho comentarios de carácter sexual o te han pedido que hagas cosas inapropiadas que te han hecho sentir incómodo en Internet?

Se le llama grooming al conjunto de estrategias que una persona adulta realiza para ganarse la confianza de un niño, niña o adolescente, a través del uso de las tecnologías de la comunicación información, con el propósito de abusar o explotar sexualmente de él o ella. El adulto suele crear un perfil falso en una red social, foro, sala de chat u otro, se hace pasar por un chico o una chica y entablan una relación de amistad y confianza con el niño o niña con la intención de acosarlo.

¿QUÉ PUEDO HACER?

- Nunca compartas o publiques información o imágenes comprometedoras por el chat, o redes sociales.
- Nunca utilices la webcam cuando chateas con desconocidos.
- Configura la privacidad de tus redes sociales. Evita tener redes sociales públicas.
- Si eres víctima de grooming, denuncia al acosador ante tus padres, maestros o un adulto de tu confianza.
- Guarda todas las pruebas, no borres conversaciones y realiza capturas de pantalla para documentar el comportamiento del acosador.

SEXTING

¿Alguna vez has enviado o recibido contenido sexual a través de tu teléfono, redes sociales o email?

El sexting comprende el envío y/o recepción de contenido sexual a través de medios electrónicos. El mismo consiste en el intercambio de imágenes y vídeos sexuales a través de mensajes, redes sociales, e-mail y sobre todo con el teléfono móvil.

LOS PELIGROS MÁS COMUNES DEL SEXTING:

- Recuerda que una vez que envías imágenes o vídeos (incluyendo los que envías en una conversación con webcam), pierdes totalmente el control de los mismos.
- Daño a tu privacidad: la exposición de estas imágenes sexuales produce un daño irreparable a la privacidad e intimidad de la persona que comparte sus propias imágenes.
- Robo de fotos o vídeos sexuales guardados en dispositivos electrónicos para luego publicarlos en Internet
- Si usas una webcam durante una conversación con otra persona, esta imagen puede ser capturada y grabada por el receptor, para luego ser publicada en Internet.

SEXTORTION

¿Alguna vez alguien ha obtenido imágenes íntimas tuyas mediante webcam, email, mensajes, teléfono u otros dispositivos móviles?

¿Te has sentido chantajeado por alguien que te amenaza con difundir imágenes o vídeos tuyos si no haces lo que te dicen?

Sextortion es una forma de extorsión en la que se chantajea a una persona por medio de una imagen o vídeo de sí misma desnuda, que puedo a ver compartido a través de Internet o mensajes. La víctima es coaccionada a ejecutar acciones que den gratificación sexual al malhechor (tener relaciones sexuales con el chantajista, producir pornografía u otras acciones que ponen en serio peligro a la víctima).

Cometer sextortion implica diversos ilícitos como: amenazas, explotación sexual, abuso sexual de menores, corrupción de menores, daños al honor, producción y tenencia de pornografía infantil, etc. Si estás siendo víctima de sextortion denúncialo de inmediato ante tus padres, maestros o un adulto de confianza.

PHISHING

¿Alguna vez has recibido un e-mail, mensaje al teléfono o mensaje en redes sociales pidiéndote información personal?

Mientras navegabas por Internet, ¿Alguna vez un sitio web te ha solicitado información personal?

Hay estafadores que a través del phishing envían mensajes de texto, e-mail o cuadros de diálogo pop-up falsos para conseguir que personas desprevenidas revelen su información personal o bancaria. La información que se ha entregado al estafador es luego utilizada para dañar a la víctima, por ejemplo robando dinero de su cuenta bancaria.

Si alguna vez te encuentras en esta situación:

- No respondas a ningún mensaje de texto, e-mail, mensaje en redes sociales que pida tu información personal.
- Nunca hagas clic en enlaces contenidos en mensajes sospechosos.
- Nunca descargues archivos de mensajes sospechosos, estos pueden contener un software malicioso.

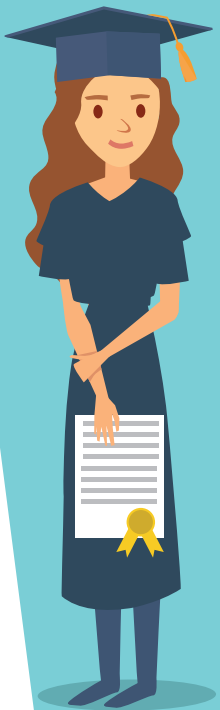
¡CONOCE TUS DERECHOS!

En Internet tienes los mismos derechos que tienes en la vida real. Debes exigir que se te respeten tus derechos y procurar respetar los derechos de los demás.

Tienes derecho a:

- Utilizar Internet, tus redes sociales y las Tecnologías de la Información y la Comunicación en general para aumentar tus conocimientos, capacidades y habilidades
- Divertirte en Internet. Tienes derecho a jugar, a investigar y participar en línea.
- Expresar tus ideas y ser tratado con respeto
- Decir NO ante cualquier petición que te haga sentir incómodo a través de Internet.
- Encontrar y proveer información adecuada para tu edad en línea.
- Denunciar ante La Policia Nacional Civil (PNC) en caso hallas sido víctima de una ofensa cometida a travéz de medios informáticos.

¡CUIDA TU REPUTACIÓN EN INTERNET!



Tu reputación en Internet es la idea que los demás tienen sobre ti, formada a partir de la información que subes a Internet, y que los demás suben sobre ti. Se construye a través de las publicaciones, fotos y vídeos sobre ti que pueden ser encontrados en Internet. También incluye los registros de participación en foros y juegos. Recuerda que la reputación se construye a lo largo de los años y es difícil de borrar o modificar ya que en Internet no hay olvido. Lo que subes a Internet, queda ahí para siempre.

¡LA REPUTACIÓN EN INTERNET ES IMPORTANTE!

Internet se ha convertido en la forma más común de conocer a una persona. Cuando quieras conseguir un trabajo, tu entrevistador buscará información sobre ti en la web. Si no cuidas tu reputación en Internet, tu información privada puede ser difundida, y tu imagen se verá afectada.

CONSEJOS PARA USAR MEJOR LAS REDES SOCIALES

- Piensa antes de compartir cualquier contenido en Internet.
- No aceptes invitaciones de amistad de extraños o de personas en las que no confías.
- No hagas a otros lo que no quieres que te hagan a ti.
- Mantén privada tu información, hazte difícil de encontrar.
- Ten mucho cuidado, trata de aplicar las mismas reglas de seguridad que usas en el mundo real.

¿CÓMO CREAR UNA CONTRASEÑA EFECTIVA?

- No uses la misma contraseña para todo
- Haz una contraseña larga
- Al crear tu contraseña combina letras mayúsculas, minúsculas, números y símbolos
- Procura cambiarla periódicamente
- ¡No la compartas con nadie!

¡USA TU WEBCAM DE FORMA SEGURA!

- Recuerda que la webcam ofrece muchísima información sobre ti, ya que la webcam muestra tu imagen y datos específicos de tu familia y entorno.

- Lo que envías por la webcam puede ser grabado al otro lado. Cualquiera puede llegar a ver lo que hagas con tu webcam.

- Tu webcam puede ser manipulada de forma remota usando malware. Desgraciadamente, es muy sencillo. Incluso pueden desactivar la luz que indica que la cámara está encendida, y grabarte aunque no lo sepas; por ello no descargues programas y archivos que no conoces.

- Solo debes usar tu webcam con personas de tu confianza, y no hacer delante de ella nada que no harías en público.

¿CÓMO CUIDAR TU TELÉFONO MÓVIL?

- Habilita el bloqueo automático y protégelo con contraseña.
- Sólo descarga aplicaciones de sitios confiables
- Revisa los permisos antes de la instalación y durante el tiempo que tengas instalada la aplicación.
- Lee la política de privacidad de una aplicación antes de descargarla.
- Asegúrate de desinstalar todas las aplicaciones (y toda otra información personal) antes de regalar, vender o desechar tu teléfono.

¿CÓMO SACARLE EL MÁXIMO PROVECHO A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN?

INVESTIGA: Utiliza las tecnologías de la información y comunicación para saber más, ampliar tus conocimientos y mejorar tus opiniones a través de búsquedas en línea.

APRENDE Y ENSEÑA: Utiliza las tecnologías de la información y comunicación para aprender a través de información escrita, vídeos, imágenes y enseña a otros lo que sabes de manera constructiva.

PARTICIPA: Utiliza las tecnologías de la información y comunicación para estar al tanto del acontecer en tu ciudad, país y en otros lugares. Comparte información sobre cuestiones sociales e involúcrate en actividades comunitarias.

Recuerda hacer siempre uso responsable de las tecnologías de la información y la comunicación. Estas tienen muchas ventajas, pero hacer un uso excesivo de ellas no es bueno. Recuerda compartir tiempo con tus amigos, leer libros, practicar deportes y realizar otras actividades que no estén relacionadas con el uso de computadoras u otros dispositivos electrónicos.

UNODC
Oficina de las Naciones Unidas contra la Droga y el Delito

Esta publicación fue impresa gracias al apoyo financiero de la Oficina de Asuntos Antinarcóticos y Aplicación de la Ley (INL) de la Embajada de los Estados Unidos de América en El Salvador.