UNODC | La Declaración de Doha: PROMOVER UNA CULTURA DE LEGALIDAD | educación para justicia

BARRIO SEGURO

MINI GUÍA DE SEGURIDAD EN INTERNET

¡TODO LO QUE TIENES QUE SABER!

¡EL INTERNET ES UNA HERRAMIENTA MUY ÚTIL...

SI LA SABES MANEJAR ADECUADAMENTE

- Las Tecnologías de la Información y Comunicación (TIC) han transformado al mundo entero y van mejorando día con día, en esta nueva era digital es mucho más fácil resolver problemas de la vida cotidiana.
- El internet es una herramienta versátil que te permite adquirir nuevos conocimientos y sirve como herramienta de entretenimiento.
- 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.
- Las tecnologías de la información y comunicación ofrecen muchas oportunidades de comunicación y aprendizaje para las niñas, niños, adolescentes y adultos, usados de manera correcta.

¡Ocupa el Internet para tu beneficio y no para tu perjuicio!

CYBERBULLYING / CIBERACOSO

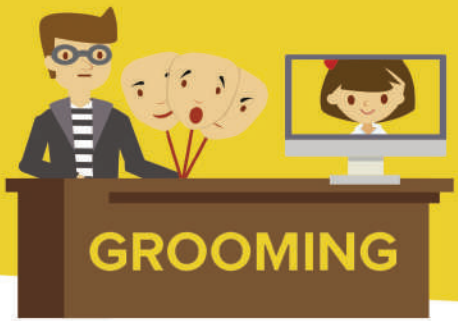
¿Alguna vez te has sentido acosado, discriminado, o alguien te ha hecho comentarios hirientes a través de redes sociales, e-mail o mensajería instantánea?

¿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?

- La mayoría de las redes sociales tienen mecanismos de seguridad, denuncia y bloqueo. Actívalas cuando te sientas ofendido, acosado o amenazado.
- No contestes a las provocaciones o insultos.
- Si te acosan, pide ayuda con urgencia a tus padres, maestros o un adulto de tu confianza.
- Compórtate con respeto hacia los demás en la red.



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

¿Qué suele utilizar?

Correos electrónicos

Videochats

Intercambio de imágenes

Redes Sociales

Se le llama grooming al conjunto de estrategias que una persona adulta realiza para ganarse la confianza de un niño, niña o adolecente, a través del uso de las tecnologías de la información y comunicación, con el propósito de abusar o explotar sexualmente de él o ella.

Conoce las etapas del grooming

Identifica a la víctima através de redes sociales o chats, ocupando perfiles falsos.

Se gana la confianza del menor de edad.

Seduce a la potencial víctima a través de conversaciones.

Obtiene contenido íntimo del menor de edad que le permite ejercer presión sobre él o ella.

Acosa, chantajea, amenaza y manipula al menor de edad para lograr sus objetivos.

SEXTING

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

El sexting es la autoproducción, intercambio y transmisión de imágenes de desnudos o casi desnudos, sexualmente sugerentes, a través de las tecnologías de la información y comunicación.

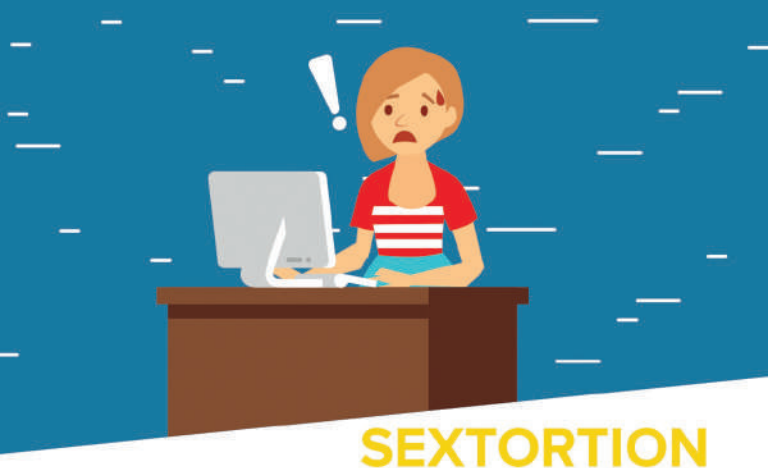
Recuerda que una vez que envías imagenes o vídeos (incluyendo los que envías en una conversación con webcam), pierdes totalmente el control de los mismos.

LOS PELIGROS MÁS COMUNES DEL SEXTING:

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.

Por más que se utilices contraseñas y otros mecanismos de seguridad, tus datos pueden ser hackeados o robados e incluso difundidos en Internet.

No olvides que durante una conversación con otra persona a través de una webcam, ésta puede capturar y/o grabar imágenes que pueden ser publicadas en Internet.



SEXTORTION

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

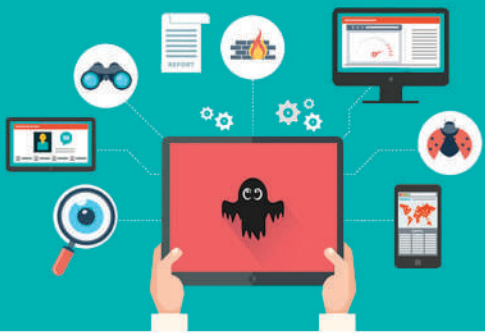
Sextortion es una forma de extorsión en la que se chantajea a una persona por medio de una imagen o vídeo de sí misma desnuda, que pudo haber compartido a través de Internet o mensajes.

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).

Recomendaciones

1. *Detén la conversación y/o relación y no accedas al chantaje bajo ninguna circunstancia.*
2. *Configura tus redes sociales para que solo tus amigos puedan ver tu perfil.*
3. *Guarda toda la comunicación para que puedas denunciarlo.*

MALWARE



Es un software malicioso diseñado para dañar un sistema, robar información y/o hacer modificaciones al sistema operativo y tomar control absoluto del equipo infectado. ¡Ten cuidado! Hay muchas clases de malware: los virus, el caballo de Troya o troyano, los gusanos, keyloggers, los ackdoor o Bot, el exploit, los software espía, el Ransomware y muchos más.

¿Cómo te infectas?

Mientras buscas contenido y bajas información.

Al bajar aplicaciones maliciosas en tu movil.

Al conectar dispositivos infectados en tu teléfono o computadora.

¿Cómo los previenes?

Mantén actualizado tu software de seguridad y tu sistema operativo.

Analiza todo dispositivo de almacenamiento antes de conectarlo a tu computadora.

No descargues archivos sospechosos.

PHISHING

¿Cómo Funciona?

Hay estafadores que envían mensajes de texto, enlaces electrónicos o correos electrónicos falsos, imitando casi a la perfección la imagen de las entidades bancarias u otras entidades, para conseguir que personas desprevenidas revelen su información personal o bancaria, para posteriormente robar el dinero de sus cuentas.

Tipo de información robada:

1. Datos personales
2. Información financiera
3. Contraseñas

Recomendaciones

- Nunca hagas clic en enlaces contenidos en mensajes sospechosos.
- Nunca descargues archivos de mensajes sospechosos, éstos pueden contener un software malicioso.
- Realiza copias de seguridad "backups" de tu información de manera periódica.
- Actualiza regularmente tu sistema operativo, navegador, antivirus y otros programas.
- Evita ingresar a sitios web de dudosa reputación o con contenido censurado.

JUEGOS ONLINE, GAMING

Cada vez hay más juegos online que se descargan en los móviles, computadoras o se juegan a través de las consolas Xbox, Nintendo, etc; en donde miles de usuarios de la comunidad virtual están conectados.

A veces, estos juegos obligan a entregar información sensible como números de tarjeta de crédito, datos personales, dirrección, etc.

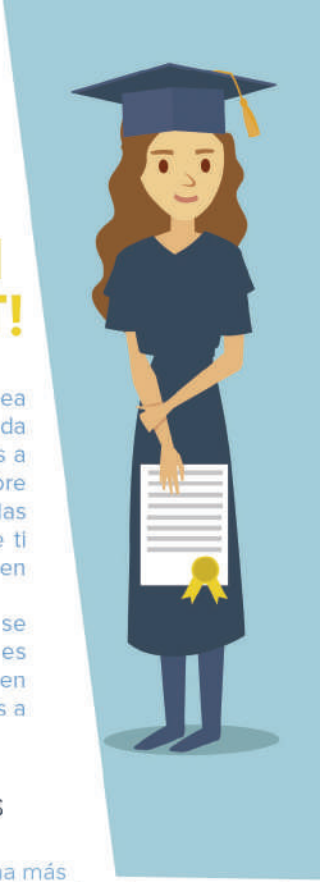
Algunos delincuentes utilizan estas plataformas para:

Acercarse con malas intensiones a menores de edad, robar información y estafarte a ti y/o tus padres.

Recomendaciones para gamers:

- *Instala un buen antivirus.*
- *Manten actualizados los programas.*
- *Utiliza contraseñas seguras.*
- *Compra exclusivamente en las tiendas online oficiales.*
- *No reveles información personal.*
- *No aceptes encontrarte con ningun jugador virtual en el mundo real sin el conocimiento de tus padres.*

¡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 videos sobre ti que pueden ser encontrados en Internet.

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 REPUTACION EN INTERNET ES IMPORTANTE

Internet se ha covertido 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 reputacion en Internet, tu información privada puede ser difundida y tu imagen se verá afectada.

CONSEJOS GENERALES

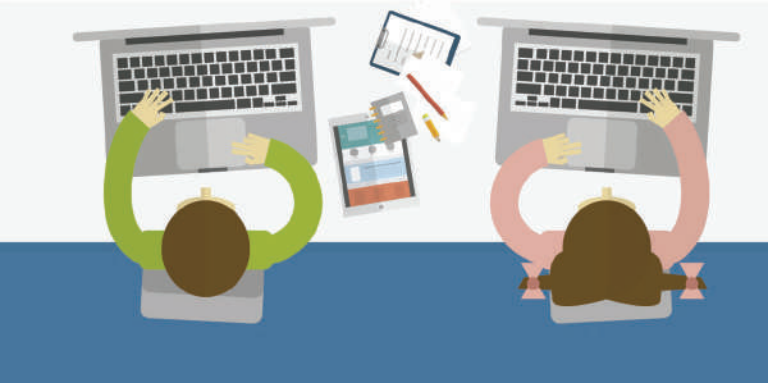
- Piensa antes de compartir cualquier contenido en Internet.
- No aceptes invitaciones de amistad de extraños o de personas en las que no confías.
- No hagas a otros lo que no quieres que te hagan a ti.
- Mantén privada tu información, hazte difícil de encontrar.
- Trata de aplicar las mismas reglas 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!

¿QUÉ DEBES HACER CUANDO ERES VÍCTIMA DEL CIBERDELITO?

- No borrar nada de las redes sociales, correos, etc, pues se convierte en evidencia.
- Parar cualquier comunicación con la cuenta que te está extorsionando, acosando, etc.
- Tomar imágenes de pantalla "pantallazos" o "Screen shots"
- Documenta la URL´s
- Pon la denuncia ante la Policía o Fiscalía (Unidad de Investigación de Delitos Informáticos de la PNC).



SOY VÍCTIMA DE ESTOS DELITOS ¿A QUIÉN PUEDO ACUDIR?

Cuando no puedas esquivar el acoso y se vuelva peligroso, denúncialo al Centro de Llamadas de la Policía Nacional Civil PNC.

¿ EN QUÉ CONSISTE EL SISTEMA DE EMERGENCIAS 911?

Es un servicio gratuito brindado a toda la ciudadanía a nivel nacional, a través del número 911 de la Policía Nacional Civil al momento de presentarse una emergencia.

Recuerda usar el 911 SOLO en caso de emergencia, cuando tu vida o la de otras personas esté en riesgo.

¿CÓMO FUNCIONA EL 911?

Al marcar el 911, telefonistas capacitados te atienden. A ellos debes proporcionar la dirección y puntos de referencia del lugar donde está sucediendo el hecho.

¿Qué puedo hacer en caso de emergencia?

Mientras llega la policía o la asistencia, dependiendo del tipo de emergencia, busca apoyo con las personas a tu alrededor.

"El 911 NO ES UN JUEGO"

Es un servicio por medio del cual, a diario se salva la vida de muchas personas, haciendo buen uso del 911 nos ayudas a que la asistencia llegue de inmediato a quien lo necesita.

Todas las llamadas que se hacen al 911 son registradas y el mal uso es castigado por la ley.

¡Sé un héroe anónimo, marca el 911 únicamente por emergencia!

¡ADVERTENCIA!

Por medio del internet muchas personas quieren hacerte creer que te ayudarán a cumplir tus sueños y a ganar dinero de manera fácil y rápida... ¡Ten cuidado! Podrían engañarte, secuestrarte y obligarte hacer cosas que te dañarán física y emocionalmente.

También hay personas que por medio del internet te ofrecen ir a otro país, diciéndote que tendrás un mejor futuro, que te podrás reunir con tu familia atravesando muchos peligros.

Recuerda ¡el coyote no es tu amigo!; para él eres sólo mercancía ¡Sólo quiere tu dinero! Mejor quédate, estudia, trabaja y supérate, tu país tiene mucho para ti.

¡El ser humano no está en venta!

campaña corazón azul
contra la trata de personas

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

UNODC | La Declaración de Doha: PROMOVER UNA CULTURA DE LEGALIDAD | educación para todos

BARRIO SEGURO

Al escanear este código podrás encontrar más información en nuestra App