



GOBIERNO DE
MÉXICO

COMUNICACIONES

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES



2024
AÑO DE
Felipe Carrillo
PUERTO



GUÍA DE CIBERSEGURIDAD

PARA NIÑAS, NIÑOS & ADOLECENTES

Versión Español





EL INTERNET ¿LO CONOCES?

Internet es una herramienta poderosa para tu desarrollo porque te acerca a nuevos conocimientos, te permite comunicarte con familiares y amigos, así como con personas que están a miles de kilómetros de distancia. Internet también te permite crear y compartir contenidos como imágenes, textos, audios y videos.

Internet ofrece una lista interminable de beneficios, pero su uso intensivo también te expone a muchos riesgos y amenazas, como pueden ser el robo o publicación, sin tu consentimiento, de tu información personal o privada, sufrir acoso o abuso por parte de personas desconocidas, robo o suplantación de tu identidad, entre otros riesgos que pueden hacer que tu experiencia en Internet sea desagradable, incómoda e insegura.



Por eso, es muy importante que, como usuario de Internet, puedas identificar y comprender los riesgos y amenazas más comunes a los que te enfrentas al navegar en Internet, y que cuentes con los conocimientos adecuados para hacer un uso seguro y responsable de esta herramienta.



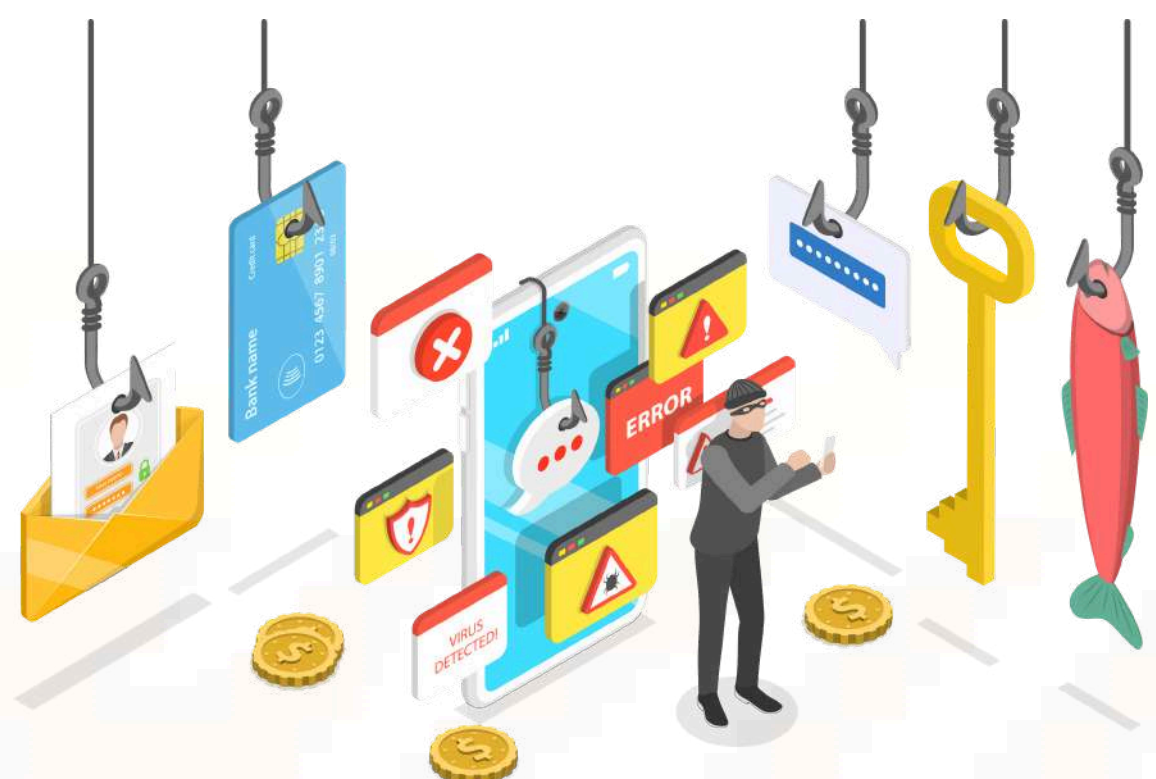


¿CONOCES CUÁLES SON LOS RIESGOS MÁS COMUNES A LOS QUE SE ENFRENTAN NIÑAS, NIÑOS Y ADOLESCENTES AL UTILIZAR DISPOSITIVOS ELECTRÓNICOS E INTERNET?

Códigos Maliciosos o Malware



Técnicas de Ingeniería Social



Ciberacoso o Cyberbullying



Grooming & Sexting



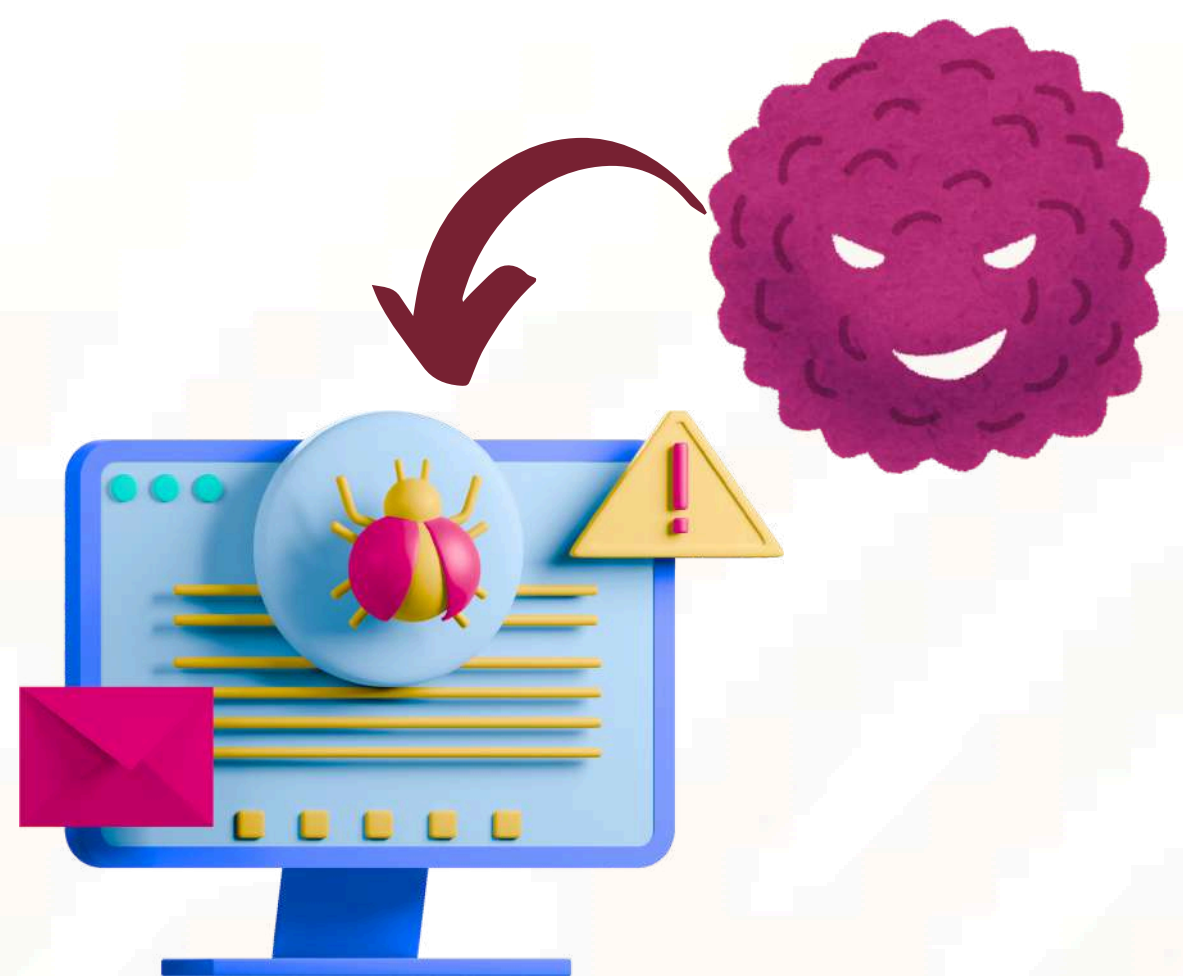
¿QUÉ ES EL MALWARE?

Son programas o códigos maliciosos que están diseñados para introducirse en tu computadora, teléfono celular, tableta y en la red de Internet (red Wi-Fi), sin que te des cuenta.

¿Cómo pueden infectarse con malware las redes, dispositivos y sistemas?

Cualquier dispositivo puede infectarse con malware por medio de los siguientes métodos:

- Descarga de mensajes o archivos en redes sociales
- Descarga de archivos o ingreso a enlaces sospechosos a través del correo electrónico o mensajes de texto.



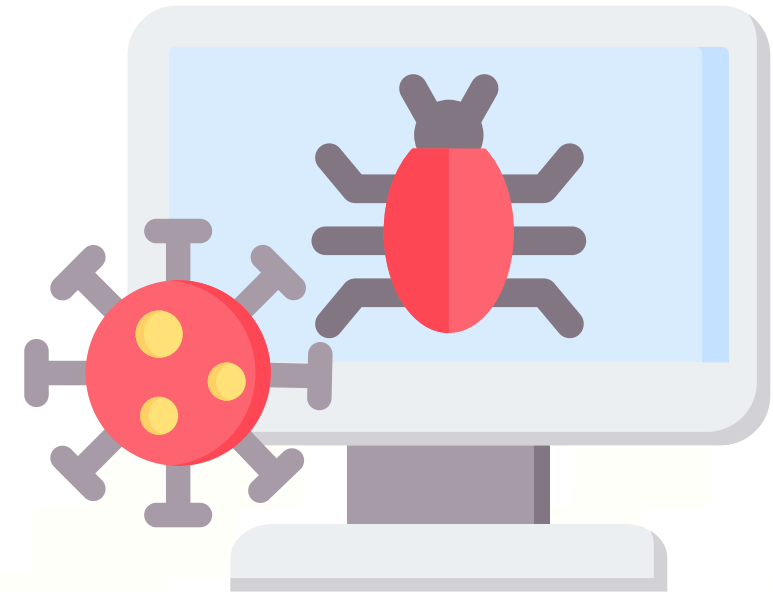
- Descarga de aplicaciones o actualizaciones poco confiables
- Visitas a sitios web sospechosos
- Conexiones a redes públicas o poco seguras
- Conexiones a Bluetooth
- Ejecución de USB, CD o DVD infectados
- Anuncios publicitarios falsos, entre otros



LOS TIPOS MÁS COMUNES DE MALWARE SON:

1. Virus informáticos

Programas o códigos informáticos maliciosos creados para infectar equipos, provocar problemas en el funcionamiento de los mismos o robar información.



2. Adware

Programa o código informático malicioso que tiene características y funciones muy variables como:

- Bombardear al usuario con anuncios masivos no solicitados.
- Descarga de complementos o de aplicaciones no solicitados.
- Descarga de actualizaciones falsas.
- Rastreo de actividades de los usuarios en Internet.



3. Spyware (Programa espía)

Programa o código malicioso cuya función principal es rastrear y registrar la actividad de los usuarios tanto en equipos físicos como en dispositivos móviles.



4. Scareware o Rogueware

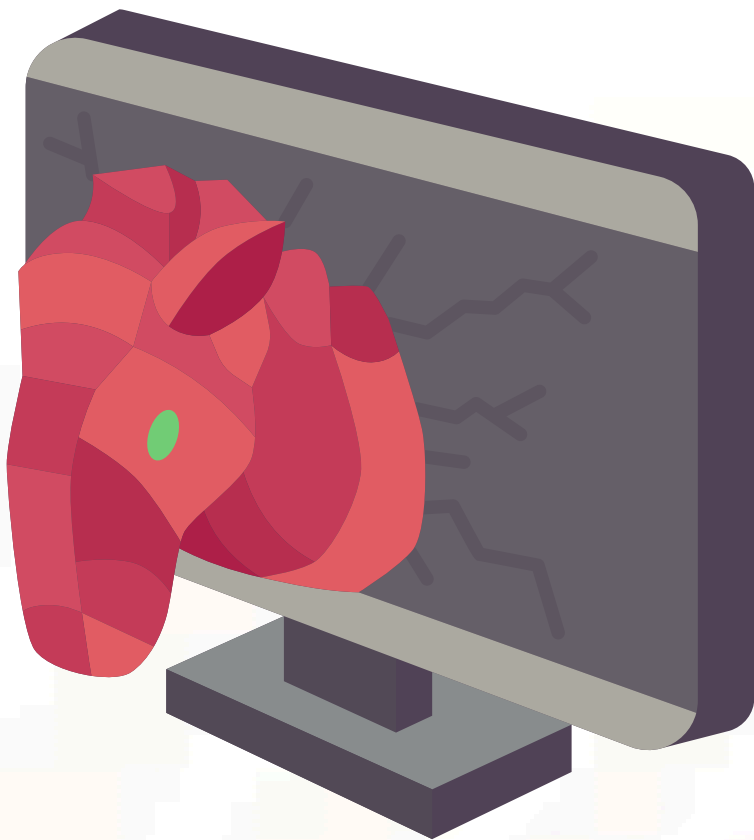
Programa o código malicioso que utiliza alertas de seguridad emergentes de antivirus, así como otras técnicas de ingeniería social para alertar al usuario y motivarlo a que realice un pago para adquirir una solución que resuelve supuestas infecciones.



¿QUÉ SON LOS CÓDIGOS MALICIOSOS O MALWARE?

5. Ransomware de cifrado

Programa o código malicioso que tiene la capacidad de “secuestrar” la información de los usuarios, impidiendo el acceso a la misma, exigiendo la realización de un pago, generalmente en efectivo, para devolver la información secuestrada.



7. Gusanos

Programa o código malicioso que tiene la capacidad de replicarse y expandirse rápidamente infectando la red y a múltiples equipos conectados a una red.

Los gusanos no suelen infectar los archivos pero son el vehículo para la descarga de cualquier tipo de malware

6. Troyanos

Archivos, programas o fragmentos de código malicioso que se empaquetan y entregan dentro de software legítimo (de ahí su nombre). Cuando esto ocurre, el troyano comienza a instalar malware en los dispositivos



8. Rootkits

Programa o código malicioso que los ciberatacantes utilizan para acceder de forma remota a un equipo, manipularlo sin el conocimiento o consentimiento del usuario legítimo.





¿CÓMO PUEDES SABER SI HAS DESCARGADO CÓDIGOS MALICIOSOS EN TU COMPUTADORA, TABLETA O TELÉFONO CELULAR?

Tus equipos se comportarán de manera extraña, por lo que debes estar atento a las siguientes señales:

**Consumo rápido de
batería**

**Fallas extrañas en tus
APPS**

Aplicaciones desconocidas

**Consumo rápido de
datos**

Anuncios todo el tiempo

**Dispositivos raros
y/o lentos**



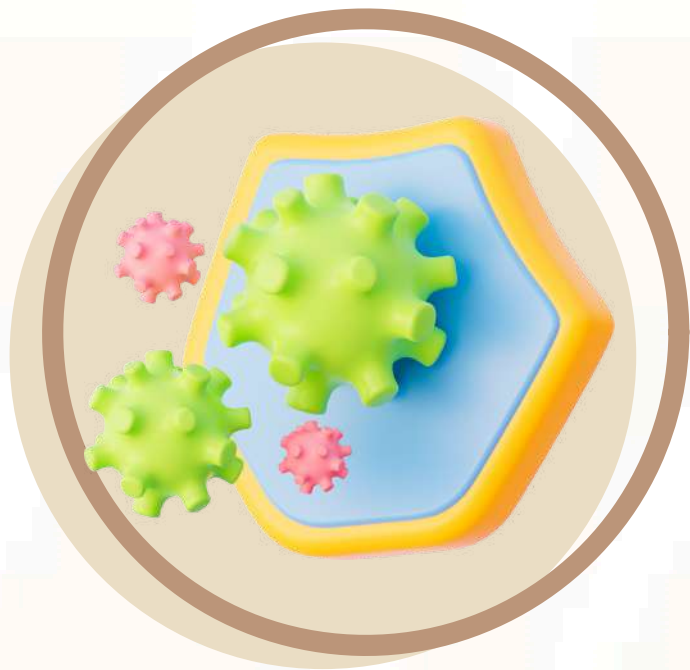


¿SABES CÓMO PREVENIR UN MALWARE?

**Utiliza APPS confiables y no de
paginas piratas**



**Instala antivirus y
actualízalo
periódicamente**



**Mantente alerta de
correos e información de
personas desconocidas**



**Usa
contraseñas
seguras en tu
red y Wi-Fi
y no divulgues
tu información**



**Pide ayuda a los
adultos de
confianza**

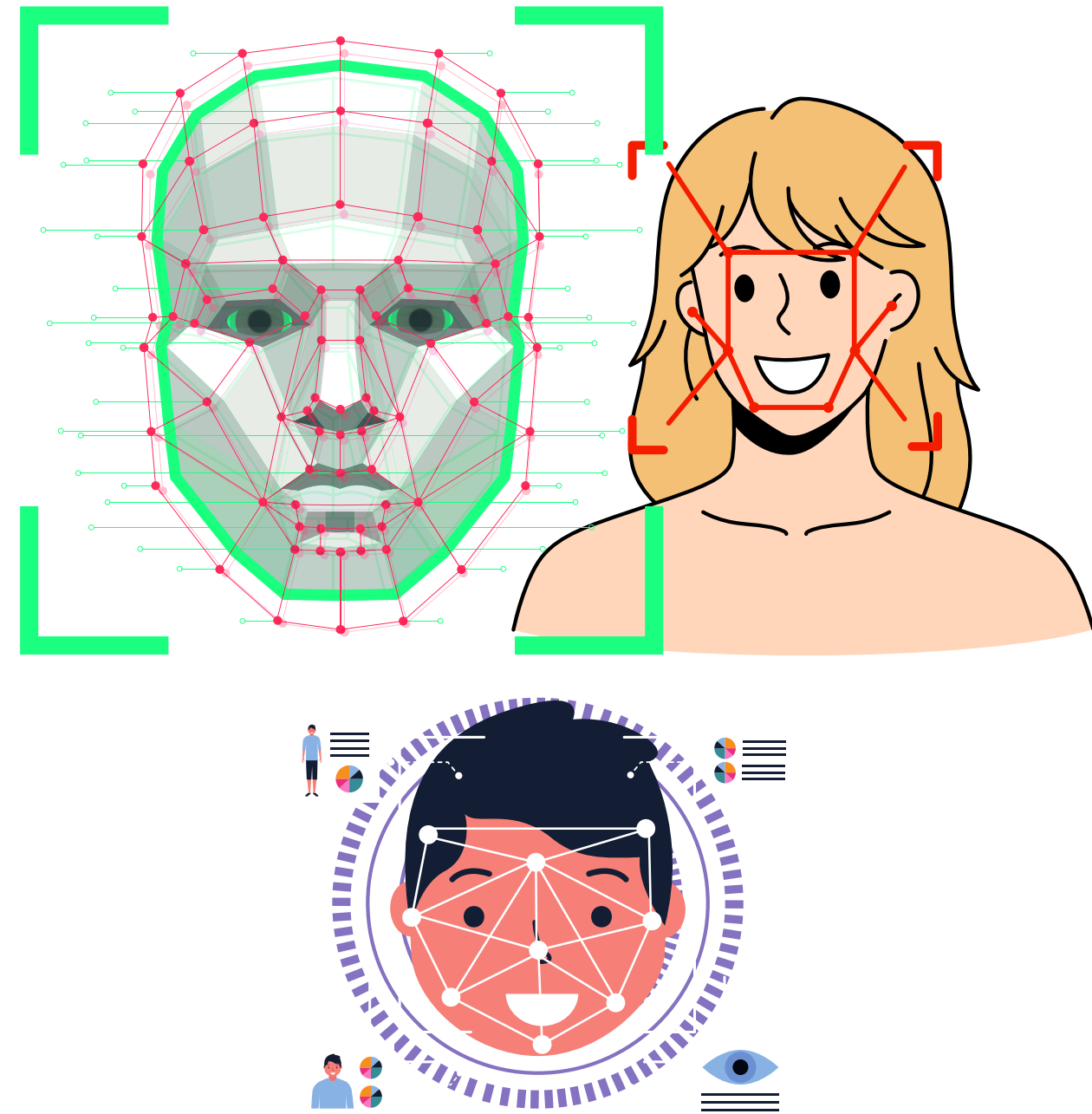


MORPHING

¿Que es?

El morphing es una **técnica de transformación o edición digital**. Consiste en un efecto especial que transforma la fotografía de un objeto real o una persona en la imagen de otro objeto real o persona.

El procedimiento consiste en **recabar dos imágenes o fotos de los usuarios que se van a transformar**; el elemento de origen y el final. Luego, se digitalizan ambas imágenes en un dispositivo. Tras digitalizar las imágenes, se utiliza un software de tratamiento de imágenes para hacer dicha transformación.



Riesgos

La entusiasmo con el que las personas comparten imágenes suyas o de su familia y amigos incluyendo menores de edad puede traer, **problemas de índoles muy dañinas para la integridad y seguridad física y salud mental de las personas.**

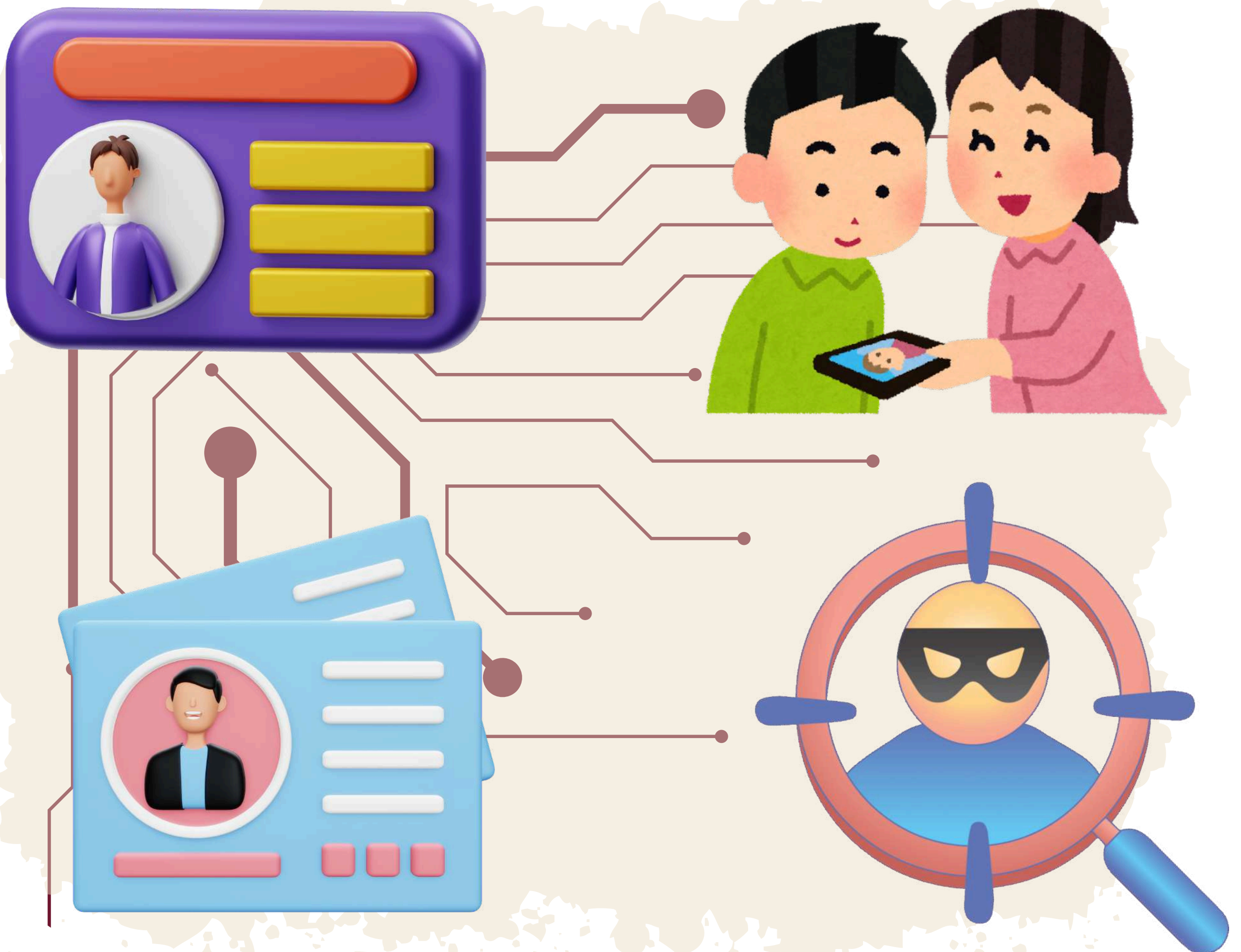
- Falsificando documentos oficiales.
- Suplantación de identidad.
- Herramienta para generar ciberacoso.



¿ Cómo prevenir Morphing?

La detección de casos de morphing obligará a extremar las medidas de seguridad:

- No compartas fotografías con desconocidos.
- No subas fotografías de alta resolución tuyas o de tus hijos o algún menor de edad que muestren características particulares de su rostro.
- No compartas con desconocidos identificaciones como: INE, Pasaporte, Credencial escolar u otra identificación que tenga tu fotografía.





¿QUÉ SON LAS TÉCNICAS DE INGENIERIA SOCIAL?

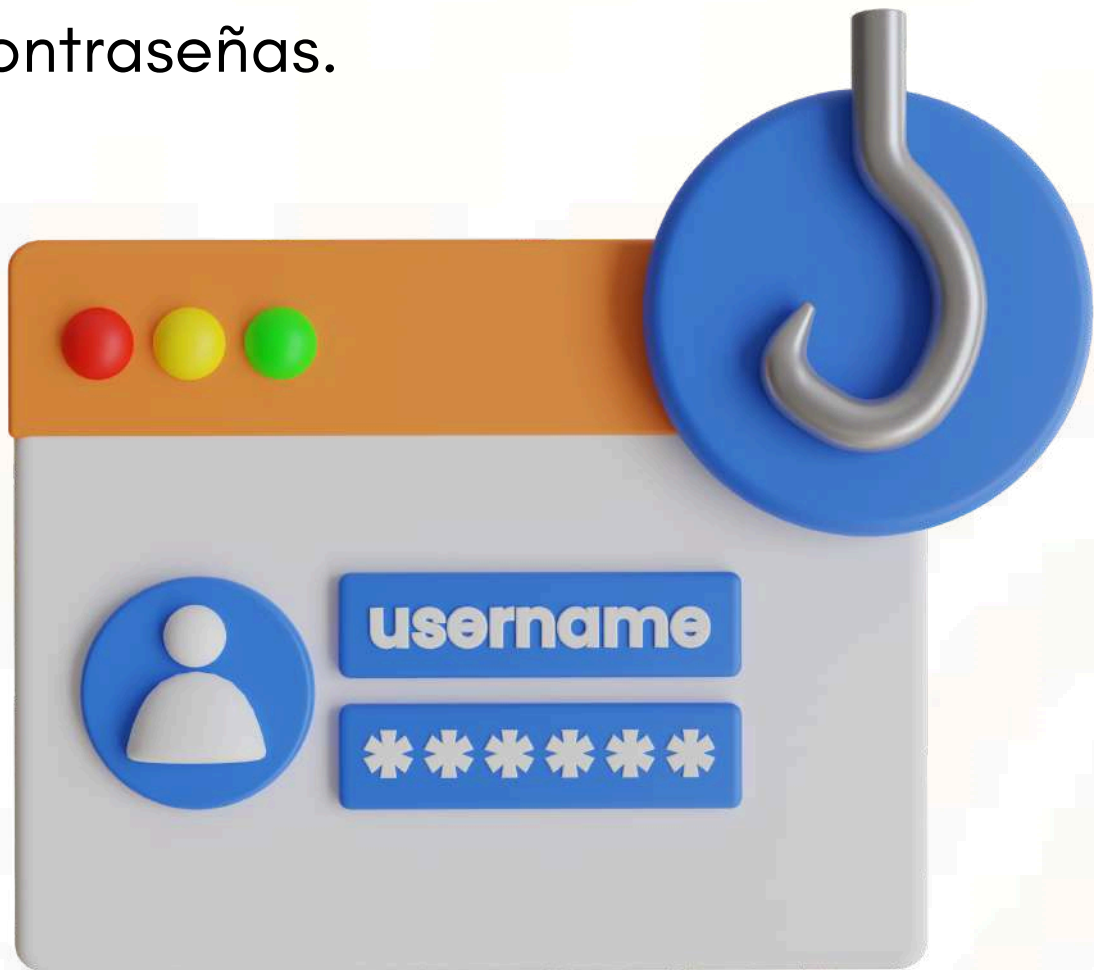
Se le llama ingeniería social a las diferentes técnicas de manipulación, engaño o estafa que usan los ciberatacantes para obtener tu información personal y la de personas cercanas a ti, haciéndose pasar por una persona de confianza, para convencerte de visitar páginas de internet desconocidas, descargar archivos o rellenar alguna encuesta.



¿CONOCES LAS TRES TÉCNICAS MÁS COMUNES POR LAS QUE PUEDES SER VÍCTIMA DE UN ATAQUE DE INGENIERÍA SOCIAL?

PHISHING

Cuando recibes un correo electrónico de personas desconocidos en los que te piden descargar algún archivo adjunto, hacer click en una liga electrónica, llenar algún formulario proporcionar información privada, personal o familiar, así como tus contraseñas.



VHISHING

Cuando recibes un llamado telefónico o mensaje de voz de personas desconocidos, quienes se hacen pasar por personas de confianza, para solicitarte datos personales, de tus familiares y amigos o solicitarse que lleves o cabo alguna acción como visitar un sitio en Internet (generalmente maliciosos).



SMISHING

Cuando recibes un mensaje de texto corto (SMS) de personas desconocidas en los que te solicitan llamar o algún teléfono, ir a un sitio web o descargar información desde un enlace desconocido.





¿CÓMO TE ENGAÑAN?

Por medio de mensajes o frases que llamen tu atención para que realices alguna acción de manera inesperada y urgente. Los ciberatacantes explotan tu sentido de urgencia, incertidumbre, miedo, asombro.





¿QUÉ SON LAS TÉCNICAS DE INGENIERIA SOCIAL?

LOS CIBERATACANTES UTILIZAN ESTAS TÉCNICAS PARA:

Obtener tus datos personales, confidenciales o sensibles

Llevar acabo actividades ilegales como acoso, suplantación de identidad, amenazas, etc.

Infectar tu red, computadora, tablet, celular y otros equipos con archivos que contienen Códigos Maliciosos (Malware)

Abrir enlaces a páginas de Internet Maliciosas





¿CÓMO PROTEGERTE?

No respondas a solicitudes de información personal o familiar por correo electrónico, mensajes de texto o llamadas telefónicas.

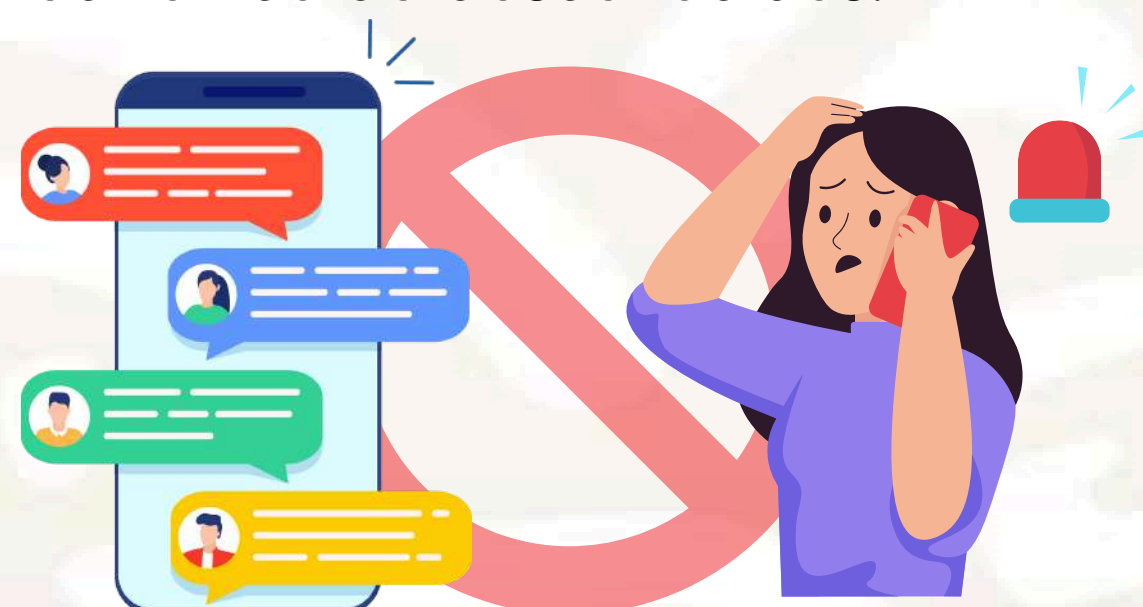
Antes de abrir cualquier enlace o archivo debes de preguntarte: ¿espero esa información? ¿reconozco a la persona que envía esa comunicación? y ¿solicitan algo con urgencia?



No introduces ninguna de tus contraseñas después de hacer clic en un enlace sospechoso.

No abras archivos adjuntos o enlaces que provienen de cuentas de correo electrónico de desconocidos.

Finalmente, cuando recibas correos, mensajes de texto o llamadas de desconocidos BLOQUEA los números y elimínalos de tus contactos.





¿QUÉ ES EL CIBERACOSO O CYBERBULLYING?

El ciberacoso es un comportamiento que busca atemorizar, enfadar, agredir o humillar a otras personas utilizando Internet y las tecnologías digitales como medio de ataque:

A través de mensajes SMS, WhatsApp o cualquier servicio de mensajería instantánea.



En las redes sociales como Facebook, Instagram y TikTok y los servicios de mensajería de estas plataformas.



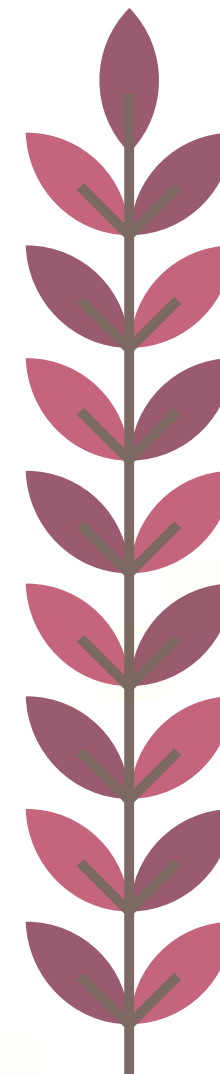
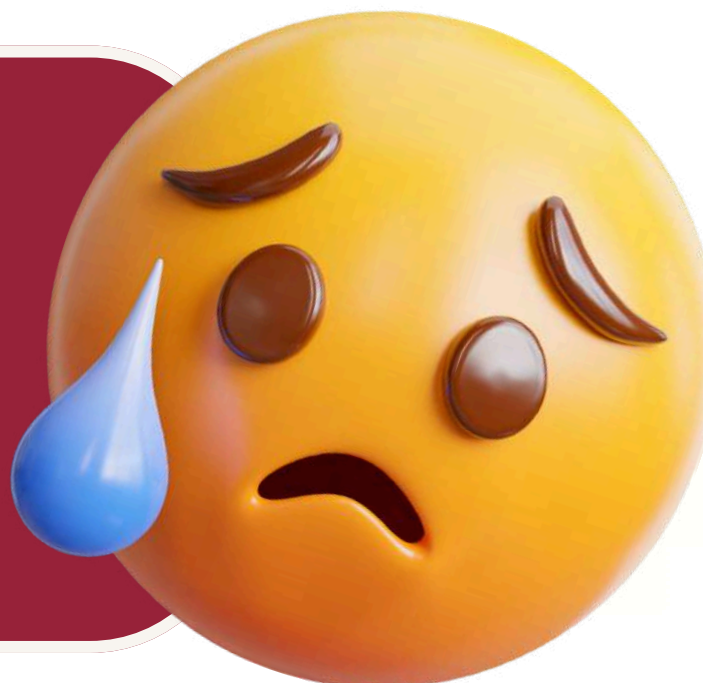
Al utilizar juegos en línea, grupos de chat o por medio de llamadas y mensajes cortos a los teléfonos celulares.



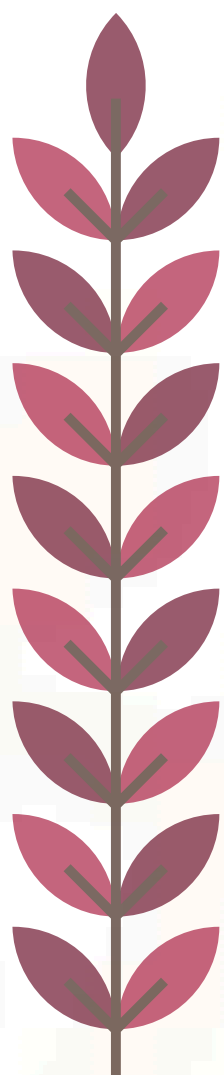


FORMAS DE CIBERACOSO

Difundir en Internet, principalmente en redes sociales información privada, falsa o vergonzosa de una persona, como fotografías o vídeos privados.



Hacerse pasar por otra persona y/o utilizar cuentas falsas, para enviar mensajes agresivos o amenazantes a otras personas.



Enviar mensajes, imágenes o videos hirientes, abusivos o amenazantes a través de plataformas de mensajería.



El ciberacoso daña las emociones y la mente de las niñas, niños y adolescentes que lo sufren. Como consecuencia, las víctimas suelen perder la motivación, aislarse de los demás, perder la confianza en otras personas y perder su autoestima.





¿QUÉ HACER SI ERES VICTIMA DE CIBERACOSO O CYBERBULLYING?

Dirígete a alguien de confianza, ya sea tus padres, hermanos, familiares cercanos, un profesor o un amigo.

Cuéntale lo que te está ocurriendo para que juntos puedan discutir la problemática e identificar las soluciones.



Si no te sientes cómodo o cómoda hablando con alguien que conoces, comunícate a la línea telefónica de ayuda de la policía cibernética para recibir apoyo profesional o bien, hacer una denuncia.



**55 5242 5100 EXT.5086 O AL CORREO ELECTRÓNICO:
POLICIA.CIBERNETICA@SSC.CDMX.GOB.MX**



GROOMING ¿QUÉ ES EL GROOMING?

Consiste en que una persona mayor de edad establece comunicación permanente y agradable con niñas, niños y adolescentes, buscando ganarse su amistad y confianza, para posteriormente convencerlos de realizar actividades como las siguientes:

- Acudir a una cita secreta para conocerse.
- Enviar fotos o videos en los que aparezcan desnudos o con poca ropa.



El grooming tiene muchas consecuencias negativas en la salud mental y el desarrollo de niñas, niños y adolescentes quienes pueden sentir estrés, vergüenza, culpa, ansiedad, depresión y miedo.



Es muy común que este tipo de acosadores lleguen a intimidar a las niñas, niños y adolescentes de la siguiente forma:

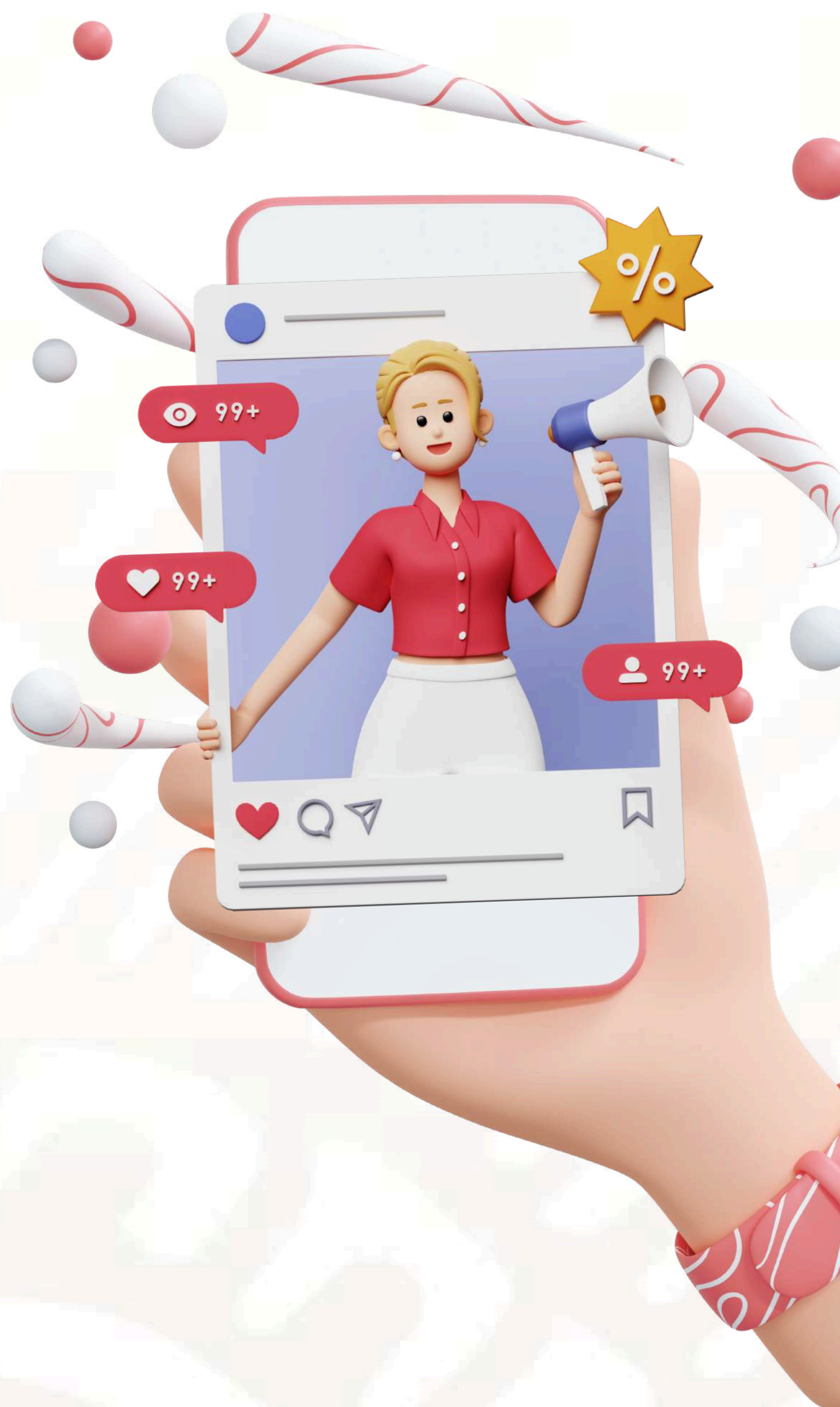
- Amenazarlos con publicar aquellas fotos o videos que enviaron y avergonzarlos frente a padres, familiares, amigos u otras personas.
- Amenazarlos con hacerles daño a sus familiares y amigos si los menores dejan de enviar este tipo de contenidos o hablan con sus familiares.



¿QUÉ PUEDES HACER PARA EVITAR SER VICTIMA DE GROOMING?



- **No** compartas información confidencial o de tipo personal con desconocidos.
- **Utiliza un alias/nombre alternativo** o apodo como nombre de usuario si te comunicas con otros de manera virtual.
- **No** aceptes solicitudes de amistades de personas que no conoces.
- **No** publiques en redes tus actividades cotidianas ni las de tus familiares o amigos.
- **No** envíes fotografías o vídeos personales a desconocidos, especialmente, si apareces con poca ropa o sin ella.
- **Por ningún motivo** aceptes tener una cita con personas desconocidas.



- **Informa inmediatamente a un adulto, amigo o persona de confianza** si algún extraño te pide el envío de fotos o videos íntimos con poca ropa o sin ella o bien si te piden que se vean en algún sitio.



SEXTING

¿QUE ES EL SEXTING?

Es la conducta por medio de la cual cualquier persona de forma voluntaria produce y envía a otra persona, a través de un dispositivo como teléfono, computadora o tablet, textos, fotos o videos de carácter sexual de sí misma.

Aunque hacerlo es una decisión personal, es importante que pienses muy bien antes de llevar a cabo este tipo de actividades pues se trata de una práctica riesgosa, porque una vez que envías esos contenidos, éstos permanecen en Internet por tiempo indefinido y pueden ser utilizados de forma mal intencionada por otros.



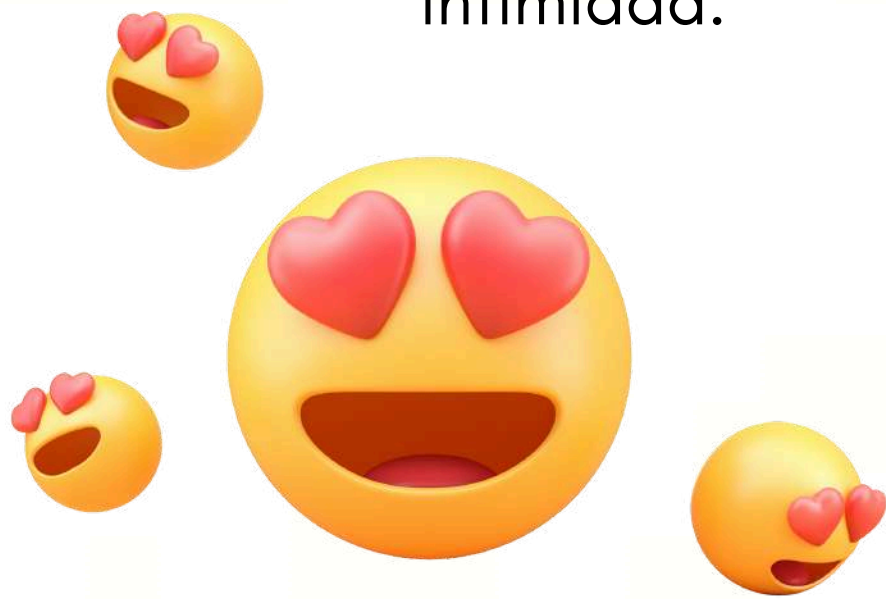
Si recibes contenido de carácter sexual de otra persona, con o sin su consentimiento, es importante que no lo compartas por ningún medio electrónico y que lo elimines de tus equipos.



¿QUÉ TIPO DE ACCIONES DEBES REALIZAR AL PRACTICAR EL SEXTING, PARA EVITAR INCIDENTES NEGATIVOS?

1

Asegúrate de que las personas con las que compartes textos, imágenes o videos tuyos, es digna de tu confianza y que existe un mutuo acuerdo de respetar la privacidad e intimidad.



2

Confirma que la otra persona desea recibir este tipo de contenidos ya que puede ser que no lo desee y lo sienta como un ataque o intimidación.

3

Si compartes textos, fotografías o videos de ti mismo, con contenido sexual, borra o excluye cualquier información que pueda identificarte, (rostro, cicatrices o tatuajes).





CIVISMO DIGITAL

Al aplicar los consejos de esta Guía de Ciberseguridad aportas tu granito de arena para crear una cultura de valores en torno al aprendizaje y uso de Internet y las tecnologías digitales de manera positiva y constructiva.



Por ello, es importante comprender el concepto de Civismo Digital y su importancia:

El Civismo Digital tiene como objetivo que cada persona se convierta en ciudadana o ciudadano digital capaz de conocer y ejercer sus derechos y responsabilidades en el uso de Internet y las tecnologías digitales.

Los ciudadanos digitales establecen acuerdos de convivencia para que su experiencia en el uso de Internet y las tecnologías digitales sea lo más agradable, positiva y propositiva como para que puedan aprovechar estas herramientas en todo su potencial, con base en el respeto mutuo.



LOS COMPROMISOS DE CONVIVENCIA DEL CIUDADANO DIGITAL

SON:

- Utilizar un lenguaje amable en redes y dirigirse a los demás con respeto.
- Respetar las opiniones y expresiones de los demás.
- Pedir permiso a las personas antes de publicar su información, fotos o vídeos.
- Comunicar a otras personas lo que pueden publicar y lo que no, sobre tu persona.



- Saber que NO representa un problema rechazar o ignorar solicitudes de amistad, invitaciones a eventos, grupos o comunidades en línea.
- Si surge un problema, buscar solucionarlo de manera personal y directa y no a través de redes sociales o medios digitales.
- Tratar de reaccionar de manera calmada y no violenta ante algo que te moleste.

CONCLUSIÓN

Al practicar las recomendaciones básicas de esta Guía de Ciberseguridad y adoptar una ciudadanía digital responsable, contribuyes a hacer del mundo digital un mundo más seguro, incluyente, productivo, ameno y respetuoso de la privacidad y de los derechos de las niñas, niños y adolescentes.





Secretaría de Infraestructura, Comunicaciones y Transportes

Lic. Jorge Nuño Lara

Secretario de Infraestructura, Comunicaciones y Transportes

Arq. Rogelio Jiménez Pons Gómez

Subsecretario de Comunicaciones y Transportes

Subsecretaría de Comunicaciones y Transportes

Lic. Carlos Gorostiza Zatarain, Director General

Lic. Susana Cruz Soriano, Directora de Área

Rocío Salas Mancilla, Jefa de Departamento

Ahlani Rodrigo Valencia Martínez, Servicio Social





GOBIERNO DE
MÉXICO

COMUNICACIONES

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES



2024
AÑO DE
Felipe Carrillo
PUERTO



GUÍA DE CIBERSEGURIDAD

PARA NIÑAS, NIÑOS & ADOLECENTES

