GUÍA DE SEGURIDAD DIGITAL

Instituto para la Protección de Personas
Defensoras de Derechos Humanos y Periodistas

6 tips básicos para tu Seguridad Digital

Respaldo

- Copia tu información y archivos de uso cotidiano en la nube;
- Guarda información y archivos históricos en discos duros;
- Respalda de manera cifrada información sensible.

Antivirus

- Instala, actualiza y escanea tus computadoras, tabletas y celulares periódicamente.

Contraseñas seguras

- Bloquea el acceso de tu computadora, tablet y celular;
- Usa contraseñas únicas y privadas;
- Utiliza frases con letras, números y símbolos, d3_10_C4R4CT3R3$;
- Usa un gestor de contraseñas por si la memoria falla;
- Activa la verificación en dos pasos.

Actualizaciones

- Actualiza tus aplicaciones;
- También el sistema operativo de computadoras, tabletas y celulares;
- El módem, router y cualquier otro dispositivo que conectes a internet.

No te dejes engañar

- Verifica la fuente del correo, página o enlace;
- Evita dar clic a correos o mensajes que te pidan información personal y contraseñas;
- No des clic ni descargues archivos de enlaces sospechosos.

Comunicaciones cifradas

- Elige servicios y apps que ofrezcan comunicación cifrada:
  - Chats;
  - Correos y envío de archivos;
  - Llamadas y video-llamadas;
  - Sitios y páginas web con HTTPS.

¿Cómo proteger tus cuentas en internet?

Sigue estos consejos para evitar accesos no autorizados:

¿Cómo prevenir?

- **Bloquea el acceso** de tu computadora, tablet o celular;
- **Usa contraseñas seguras:** únicas, privadas y con caducidad; usa frases que combinen letras + números + símbolos;
- **Activa la verificación en 2 pasos** y guarda los códigos de recuperación en un gestor de contraseñas;
- **Evita exponer información privada** (por ejemplo guardar tu contraseña en una libreta;
- **Revisa las configuraciones** de seguridad y privacidad de tus cuentas;
- **Ojo a los engaños** vía correos y mensajes que te piden datos privados, dar clic en enlaces o descargar archivos.

¿Cómo atender?

Si aún tienes acceso a tu cuenta:

- Actualiza tus contraseñas
- Activa la verificación de 2 pasos
- Revisa el registro de acceso y actividad
- Cierra sesiones en dispositivos vinculados

Si perdiste acceso a tu cuenta:

- Contacta al proveedor del servicio para recuperar tu cuenta, te pedirán comprobar tu identidad.

Consulta herramientas recomendadas en: https://protege.la/proteger-cuentas-en-linea/

¿Qué hacer ante ataques en redes sociales?

Personas o grupos pueden atacarte con el fin de ofender, amenazar, intimidar o hacerte daño. La violencia digital impacta también fuera de internet.

4 acciones para protegerte

1 Identifica

2 Documenta

3 Silencia, Bloquea o Reporta

4 Denuncia

Consulta herramientas recomendadas en: https://protege.la/ataques-en-linea/

¿Qué hacer ante ataques en redes sociales?

4 acciones para protegerte

1 Identifica

- El primer paso para combatir la violencia es aprender a identificarla. Algunas agresiones suelen ser normalizadas o minimizadas. Recuerda que una agresión puede habilitar o detonar otras violencias.

2 Documenta

- Recopila evidencia de los ataques con imágenes y archivos a detalle. Registra la fecha, hora, nombre y enlaces de los incidentes y grupos involucrados y capturas de pantalla. Apoyate en alguien de confianza para que te ayude a identificar información relevante.

3 Silencia, Bloquea o Reporta

- Conoce las normas de comunidad de las redes sociales y cómo se aplican, así como herramientas para bloquear y reportar. Reporta contenido agresivo, falso, violento y/o que intenta agredirte. Bloquea interacciones no deseadas y cuentas con quienes no quieres relacionarte.

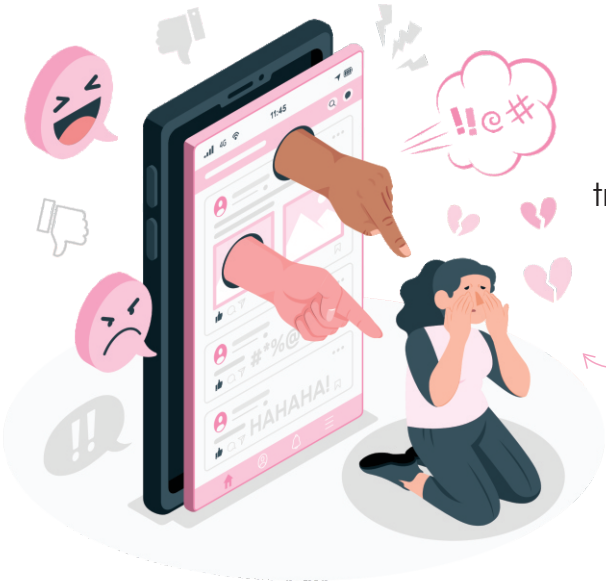
4 Denuncia

- Acude a las autoridades a denunciar, en caso de ser víctima de delito. Aumenta la seguridad en tus cuidados físicos y digitales, si decides presentar una denuncia pública en Fiscalía General del Estado.

Consulta herramientas recomendadas en: https://protege.la/ataques-en-linea/

Conductas ofensivas, intimidatorias

(Tipo: Conductas humanas - interacción directa)



Ejemplo:

Insultos y ofensas a través de redes sociales

Contenido con el fin de **ofender**, **avergonzar**, **humillar**, **desprestigiar** a otra persona. Pueden incluir **amenazas**, contenido discriminatorio y/o que incita a la violencia.

Acciones inmediatas:

- Utilizar las herramientas de silenciar, bloquear o reportar;
- Documentar y reportar el contenido;
- Si incurre en un delito y decides hacer una denuncia pública y con las autoridades, aumenta tu seguridad e identifica redes de apoyo.

¡El como responder es decisión de quien vive el ataque, no hay una respuesta correcta o incorrecta!

Consulta herramientas recomendadas en:
https://protege.la/ataques-en-linea/

¿Qué es el doxing? Acciones de prevención y reacción

Ejemplo:

Doxing (o doxxing) es la práctica de buscar, recopilar y publicar información personal, privada y/o sensible sobre alguien sin su consentimiento, con la intención de exponer y dañar a esa persona.

Cuidados digitales para prevenir doxing:

Además del reporte en plataformas, te recomendamos las siguientes acciones preventivas:

- Antes de compartir algo en un espacio digital, evalúa si es confiable hacerlo y si se trata de información de alguien más siempre pide su consentimiento.
- Revisa las configuraciones de seguridad y privacidad de tus cuentas en línea, y verificar qué información es pública.
- Revisar quiénes pueden ver información de tus redes sociales.
- Realizar un auto-stalkeo o también llamado "ego surfing". Consiste en buscar información sobre ti en Internet para posteriormente evaluar qué información personal podría ser usada para solicitar la baja de contenido de algún espacio digital.
- Crear alertas sobre tu identidad.

Puede asociarse a una dinámica de extorsión.

Este ataque también puede tomar la forma de divulgación de material gráfico y audiovisual explícitamente sexual o relacionado al rol de género, sin consentimiento y con el fin de causar daño.

Ejemplo:

- Una ex-pareja publica información íntima en redes sociales.
- Un grupo opositor tiene acceso a información privada de una persona y publica esta información en redes sociales.

Consulta herramientas recomendadas en:
https://protege.la/que-es-el-doxing-acciones-de-prevencion-y-reaccion/

Bots, granjas de bots y trolls

Los bots son un tema recurrente en nuestras discusiones en Internet: seguro has escuchado más de una vez a figuras públicas, periodistas y usuarios de redes sociales hablar de "bots", "granjas de bots" y hasta "trolls". Pero, ¿qué son? ¿cuál es la diferencia entre ellos?

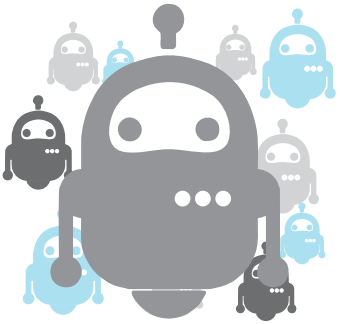
Bots

Un bot es un programa que realiza acciones repetitivas a través de Internet, como enviar mails, responder mensajes o tuitear, buscando simular el comportamiento humano. Un algoritmo lo hace funcionar y no directamente una persona, por eso viene de la palabra ro-bot.

Algo que hay que tomar en cuenta es que, aunque los bots están configurados para funcionar sin intervención humana, están programados por personas y pueden amplificar sesgos, discriminar e incitar al discurso de odio. Hay de todo tipo de bots en la viña del Internet.

Granjas de Bots

Las granjas de bots son una multitud de bots administrados por una misma persona o grupo. Esta estrategia busca crear usuarios (bots) con perfiles falsos en redes sociales para aumentar el número de seguidores de una cuenta, posicionar temas o hashtags e incluso propagar noticias falsas. No todas están ligadas a temas políticos, también pueden ser utilizadas por agencias de marketing para aumentar el tráfico de una marca o negocio.



trolls

Aunque algunas veces se confunden, los trolls son distintos a los bots. «Troll» describe a una persona o grupo, muchas veces con identidad desconocida, que publica mensajes provocadores con la intención de generar conflicto o una emoción negativa. Estos dos conceptos se pueden cruzar ya que algunos trolls pueden utilizar bots para amplificar su mensaje y desorientar una conversación.

El "trolleo" puede ir desde bromas inocentes, hasta bullying digital y acoso en línea.

¿Cómo identificar un bot en redes sociales?

Cuando hablamos de bots diseñados para posicionar un discurso o propagar una noticia, lo más sencillo es observar su comportamiento. Algunos comportamientos comunes en bots son:

- Seguir sólo a cuentas "famosas" y verificadas, especialmente las que comparten perfil político o ideológico (Ejemplo: sólo sigue a cuentas de integrantes de un partido político)
- Seguir otras cuentas no verificadas pero cuando las analizamos todas parecen "bots"
- Algunos bots son creados sólo para dar likes o RTs, no comentan ni tuitean
- En general tienen una actividad repetitiva y pueden replicar mensajes del mismo tipo de manera recurrente y "robotizada"

Señales de trolls o trolling

A veces puede ser difícil diferenciar entre un troll y personas que sólo quieren discutir sobre un tema. A continuación señalamos algunos indicios de que alguien está activamente troleando a otra persona:

- **Comentarios fuera del tema**: un comentario o publicación totalmente fuera del tema del post, artículo, noticia u otro escrito. Esto se hace con el fin de molestar y perturbar la integridad de otros comentarios. La principal tarea del troll es alejar al público del tema.
- **Negación de pruebas**: incluso cuando se les presentan hechos duros y fríos, los ignoran y fingen que nunca los han visto, aun así se resisten, demostrando que los hechos no son convincentes.
- **Tono aburrido y condescendiente**: una de las primeras señales de un troll puede ser una pregunta a otro usuario de la web (por ejemplo, en los comentarios o en los mensajes del foro/chat): "¿Por qué estás enojado, hermano?". Esto se hace con el fin de provocar a alguien aún más, y también es una gran manera de rechazar completamente el argumento de alguien.
- **Uso de imágenes o memes no vinculadas**: en lugar de comentar, dejan memes, imágenes y gifs que no forman parte del tema principal de discusión o del artículo / noticia. Una señal segura de un troll es su respuesta de texto muy largo a un post, artículo o comentario.
- **Olvido aparente**: parecen ignorar que la mayoría de la gente no está de acuerdo con ellos. Además, los trolls rara vez se enojan o son provocados.

Hay muchas otras formas de determinar si alguien está troleando. Como regla, si se piensa que alguien no es sincero, ni está interesado en una discusión real y es deliberadamente provocativo, lo más probable es que sea un troll de Internet.

Consulta herramientas recomendadas en: https://protege.la/bots-granjas-de-bots-y-trolls/

¡Tipos de phishing, cómo identificarlos y protegerte!

Los ataques de **phishing** son correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos diseñados para manipular a las personas para que descarguen malware, compartan información confidencial (ejemplo: números de la seguridad social y tarjetas de crédito, números de cuentas bancarias, información personal, contraseñas para inicio de sesión), o realicen otras acciones que expongan a los usuarios o a sus organizaciones al ciberdelito.

¿Qué puedes hacer ante casos de ataques de robo de información, infección y espionaje?

- Evita caer en este tipo de anzuelos y mejora tus habilidades para detectar "mensajes gancho" que a través del engaño buscan infectar tus equipos.

- Este tipo de técnica que busca engañar a las personas para infectar y/o robar información de un dispositivo digital, es conocida como Phishing.

- El Phishing es el anzuelo del espionaje electrónico: una técnica que puede tomar distintas formas (como: adjuntos de un correo electrónico, un mensaje de texto SMS con una URL, un archivo descargable de internet, entre otras) y que bien usada puede engañar a cualquier persona.

Consulta herramientas recomendadas en:
https://socialtic.org/blog/tipos-de-phishing-como-identificarlos-y-protegerte/

3 tipos de phishing, características y consejos para protegerte:

El que te roba tus datos

Características:
Busca obtener información personal para el robo de datos, para ello usa sitios y portales falsos de empresas o servicios (ejemplo: instituciones bancarias)

Consejos:
- Cambia la contraseña de la plataforma o acceso al servicio;
- Si la plataforma lo permite activa verificación de dos pasos;
- Antes de introducir tus datos a una página web pon atención a la **URL** y verifica que tenga **HTTPS**;
- Actualiza tus aplicaciones.

El que te infecta

Características:
Infecta dispositivos o equipos con conexión a internet a través de la descarga de archivos. Ejemplo: !ganaste un premio¡ dale clic aquí para reclamarlo.

Consejos:
- Instala y actualiza tu antivirus;
- Respalda tu información;
- Instala un bloqueador de anuncios en tu navegador
- Considera formatear el dispositivo

El que te infecta de forma especifica

Características:
Usa tecnología costosa y sofisticada para conocer intereses y gustos de la persona objetivo, infectado de manera dirigida dispositivos y equipos. Son los malware más peligrosos, difíciles de detectar y capaces de tomar el control del equipos a través de mensajes personalizados engañosos, provocativos y con amenazas.

Consejos:
- Si sospechas que tu equipo está infectado con este tipo de malware dirigido busca ayuda especializada

¡Evita que te pesquen, estos son los mejores consejos que puedes seguir!

Evita abrir y darle clic:

1. Si recibes mensajes extraños a través de celular, SMS, correo electrónico o navegador en internet;
2. Si desconoces el origen, la dirección o contacto que envía el mensaje y/o correo.
3. Mantén actualizado el sistema operativo de tus equipos (celular, tablet y computadora).

Consulta herramientas recomendadas en:
https://socialtic.org/blog/tipos-de-phishing-como-identificarlos-y-protegerte/

Páginas web para autoprotección en materia de seguridad digital:

•Genera contraseñas seguras
https://haveibeenpwned.com/

•Violencia en línea contra mujeres
https://onlineviolencewomen.eiu.com/

•Efectos de la violencia en línea
https://violenciadigital.tedic.org/es/b/guia/efectos-de-la-violencia-en-linea/

•Violencia digital
https://luchadoras.mx/internetfeminista/violencia-digital/

•Dirección de correo electrónico temporal desechable
https://internxt.com/temporary-email
https://www.guerrillamail.com/
https://temp-mail.org/

•Administrador de contraseñas
https://bitwarden.com/

•Nombre de usuario o de dominio
https://namechk.com/

¡El IPPPDDHyP de Sinaloa te orienta y protege!

¡Acude a nosotros!

Calle Carlos Lineo #1997, Plaza Botánico,
Primer Piso, Locales 206-210
Col. Chapultepec, Culiacán, Sinaloa.

Teléfonos: 667 709 7521 y
6677097500 Ext. 100

Teléfono de Guardia:
66 74 89 98 32