GUÍA

HABILIDADES DE SEGURIDAD DIGITAL Y PREVENCIÓN DE VIOLENCIAS PARA **MADRES, PADRES Y CUIDADORES**

Asociación Aguayo
INTERNET BOLIVIA .ORG
educo educar cura

La guía *Habilidades de seguridad digital y prevención de violencias para madres, padres y cuidadores* ha sido desarrollada en el marco de un proceso colaborativo entre la Fundación InternetBolivia.org, Asociación Aguayo y la Fundación Educación y Cooperación - Educo.

Elaborado por:
Camilo Arratia y Wilfredo Jordán

Revisado por:
Equipo InternetBolivia.org:
Cristian León, Lisette Balbachan y Lu An Méndez

Equipo Educo:
Marcelo Claros, Mauricio Otasevic y Wendy Rivera

Proyecto asociado:
Alfabetización digital para la seguridad de la navegación en línea de niñas, niños y adolescentes *(Educo, InternetBolivia.org y Asociación Aguayo).*

Diseño y diagramación:
Marcelo Lazarte

Impresión:
CODIGO M

Enero, 2025

La Paz – Bolivia

GUÍA

HABILIDADES DE SEGURIDAD DIGITAL Y PREVENCIÓN DE VIOLENCIAS PARA **MADRES, PADRES Y CUIDADORES**

ÍNDICE

INTRODUCCIÓN

En la era digital actual, el acceso a Internet y a las Tecnologías de Información y Comunicación (TIC) ha transformado la manera en que nuestras/os hijas/os aprenden, se comunican y se relacionan con el mundo que les rodea. Sin embargo, junto con estas oportunidades, también surgen nuevos desafíos que requieren una atención cuidadosa, especialmente en lo que respecta a la violencia digital, el uso crítico de las tecnologías y su privacidad.

La violencia digital se ha convertido en una preocupación creciente, ya que se manifiesta de diversas formas, como el ciberacoso, la suplantación de identidad, el grooming, entre otros. En este marco, es fundamental que madres, padres y cuidadores comprendan qué es la violencia digital y puedan identificarla.

De igual manera, es necesario comprender que estas situaciones se generan a través del uso de datos personales, por lo que se requiere adquirir habilidades mínimas de seguridad digital a fin de proteger no solo a nuestras/os hijas e hijos, sino a cada integrante de nuestras familias.

Además, es crucial fomentar un pensamiento crítico en el uso de las tecnologías que se conectan a Internet, a fin de aprovechar sus potencialidades, como la colaboración, el acceso al conocimiento y la productividad. Con un enfoque en la protección de la privacidad, el uso de Internet puede darnos varios beneficios.

La presente guía propone consejos prácticos dirigidos a madres, padres y cuidadores con el objetivo de prevenir la violencia digital, fomentar el pensamiento crítico en el uso de tecnologías y promover el uso de Internet como una herramienta favorable y segura.

1. **ENTENDIENDO** LA VIOLENCIA DIGITAL

¿ES AMOR?

Clara está sentada en la sala con su teléfono, luciendo confundida. Su mamá, Laura, se sienta junto a ella con una taza de té, notando su preocupación.

La violencia digital es todo acto que busca dañar a otra persona mediante el uso de las Tecnologías de Información y Comunicación (TIC) o los medios digitales, como Internet, las redes sociales o a través del uso de dispositivos como celulares, tabletas o computadoras.

Se trata de una extensión de la violencia que ocurre en el mundo físico, pero a través de los dispositivos móviles o computadoras con Internet puede darse sin importar la distancia, puede ejercerse desde el anonimato y dura más tiempo porque lo que se publica en el ciberespacio puede difundirse rápida y ampliamente dificultando o incluso imposibilitando su eliminación.

1.1 **LAS FORMAS** DE LA VIOLENCIA DIGITAL

La violencia digital puede tomar distintas formas, pero todas generan daños, por lo que, como madres, padres o cuidadores, debemos conocerlas e identificarlas.

FORMAS DE VIOLENCIA DIGITAL	EJEMPLO
Ciberbullying (acoso escolar en línea) Es el conjunto de acciones que se realizan a través de medios digitales para generar malestar o molestar, atacar o alarmar a un/a compañero o compañera de una unidad educativa.	Un/a compañero/a de curso crea stickers de WhatsApp con imágenes editadas sobre otra/o compañera/o y lo comparte en un grupo para burlarse o hacerle quedar mal.
Doxing Es el uso y/o difusión de datos personales sin autorización para generar daño.	Cuando alguien introduce sus datos personales (Ej. teléfono o dirección) en algún registro electrónico y posteriormente estos datos se hacen públicos o son usados para enviar mensajes intimidantes.
Suplantación de identidad Cuando alguien usa los datos personales de otra persona para hacerse pasar por ella, con el propósito de engañar a otros y causarle daño.	Una compañera o compañero crea un perfil falso en una red social usando las fotos y nombre de otra/o compañera o compañero y publica comentarios ofensivos o difunde rumores como si fuera titular (dueña o dueño) de la cuenta.
Amenazas Mensajes agresivos a través de Internet donde una persona dice que va a hacer daño a alguien o a su familia si no hacen lo que él o ella quiere.	Una hija o hijo recibe mensajes en sus redes sociales diciendo que si no hace lo que le dicen, su familia sufrirá daño.
Grooming Cuando una persona adulta intenta engañar a un niño, niña o adolescente a través de Internet para ganarse su confianza y luego hacerle daño.	Una persona adulta se hace pasar por una niña, niño o adolescente en Internet para hablar con otra niña, niño o adolescente a fin de promover encuentros personales, solicitar fotos o videos, chantajear o acosar con fines sexuales.
Control Es el seguimiento constante de lo que una persona hace en Internet o fuera de él, ésta es una forma de violencia que pueden hacerse usando diferentes tecnologías. Por lo general esta forma de violencia suele darse durante las relaciones de enamoramiento o noviazgo.	Una pareja o ex pareja instala una aplicación en el teléfono de un o una adolescente sin que lo sepa, para luego rastrear su ubicación o ver sus mensajes privados. Luego utiliza esa información para hacer comentarios inapropiados sobre esas actividades o chats.
Difusión de imágenes íntimas Cuando alguien comparte o publica fotos privadas de otra persona.	Un o una adolescente, después de terminar con su pareja, decide compartir fotos íntimas de su ex pareja para dañar su reputación.

Fuente: Elaboración propia con la información de "La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta" [Preparado por la Secretaría General de la Organización de los Estados Americanos]

Si bien estas formas de violencia digital pueden ocurrirle a cualquier persona, se ha visto que en su mayoría se ejerce contra niñas y mujeres, así como hacia personas que tienen orientaciones e identidades sexuales diversas.

1.2 LOS **EFECTOS** DE LA VIOLENCIA DIGITAL Y POR QUÉ ES IMPORTANTE PREVENIRLA

En ocasiones se piensa que la violencia digital no afecta como cuando ocurre en espacios físicos, pero no hay nada más alejado de la realidad, ya que los efectos pueden ser iguales o peores, por ejemplo:

- **Afectaciones emocionales.** Puede ser causante de estrés, miedo, depresión, baja autoestima y pensamientos de aislamiento. Nuestras hijas o hijos pueden sentirse solas/os y culpables por lo que les ocurre.
- **Afectaciones físicas.** La violencia digital también puede provocar problemas de salud física en nuestras hijas o hijos, debido a la angustia emocional que les genera, pueden existir casos de autolesiones o situaciones más graves, como el suicidio.
- **Impacto en la vida diaria.** La violencia digital puede afectar también el desempeño escolar de nuestras hijas o hijos o desmotivación y abandono de actividades que eran de su agrado o rutinarias.
- **Desconfianza en la tecnología.** De igual manera puede provocar que nuestras hijas o hijos tengan miedo de usar ciertas herramientas tecnológicas y queden excluidas/os de sus beneficios, como por ejemplo el acceso al conocimiento o la productividad.

Por lo explicado, antes de que se presenten estos casos, es importante saber cómo prevenir las diferentes situaciones de violencia digital.

1.3 **EL ACOMPAÑAMIENTO FORTALECE** A NUESTRA FAMILIA

Así como incorporamos hábitos de alimentación saludable y ejercicio para prevenir enfermedades físicas, es importante también, en esta era digital, adoptar acciones orientadas a prevenir riesgos y violencias digitales, no solo para proteger a nuestras hijas e hijos sino para el cuidado de todos los miembros de nuestra familia. Por ejemplo, se puede:

La prevención consiste en la adopción de medidas y acciones anticipadas para evitar que ocurran expresiones de violencia digital o riesgos potenciales antes de que se presenten.

- **Manifestar interés por la actividad digital de nuestras hijas e hijos,** preguntándoles, por ejemplo, sobre los juegos en línea o redes sociales que más les gustan o incluso compartir estas actividades, siempre y cuando ellas o ellos lo deseen.
- **Cultivar habilidades de seguridad digital y compartirla con la familia,** por ejemplo, averiguar o investigar sobre las configuraciones de privacidad de los juegos o aplicaciones más utilizadas y pasar esa información a nuestras hijas o hijos para que puedan comprender su importancia y usarlas.
- **Participar en talleres y campañas de prevención.** Diferentes instituciones públicas, privadas o educativas organizan eventos de capacitación, es recomendable asistir a ellos, así como participar en campañas, pues son espacios donde se pueden adquirir recursos de prevención.
- **Lograr acuerdos con nuestras hijas e hijos sobre el uso de las tecnologías,** por ejemplo, horarios, tiempos de uso, acuerdos sobre compartir información con amigos o amigas en línea, etc.

ACTIVIDADES DE APOYO

ACTIVIDAD 1

ANÁLISIS DE CASOS DE VIOLENCIA DIGITAL

Objetivo: Identificar las formas de violencia digital y tomar acciones de prevención en el entorno familiar.

Instrucciones:

Lectura de ejemplo: Lee atentamente el siguiente ejemplo de violencia digital:

Una persona adulta se hace pasar por una niña, niño o adolescente en Internet para hablar con otra niña, niño o adolescente a fin de pedirle fotos íntimas.

Encierra en un círculo el tipo de violencia al que corresponde:

Ciberbullying Grooming Doxing Suplantación de identidad

Plan de acción personal: Ahora que conoces el peligro de esta forma de violencia digital, como madre, padre o cuidador/a, ¿qué acciones de prevención tomarías y de qué manera?

2. **HABILIDADES DE SEGURIDAD DIGITAL** PARA PROTEGER A LA FAMILIA

LA IMPORTANCIA DE LA PRIVACIDAD

Lucía está en su teléfono, publicando una foto en Facebook.
Ana, su mamá, se acerca y observa preocupada.

2.1 **QUÉ INFORMACIÓN** DE INTERNET PUEDE PONER A UNA PERSONA EN RIESGO

El acceso a Internet ha permitido que una gran variedad de voces y experiencias puedan expresarse y manifestarse. Sin embargo, también se ha convertido en un espacio donde existen riesgos, y la fuente principal para que esto ocurra es la captación y mal uso de los datos personales, pues las o los agresores utilizan esa información para ejercer violencia. Veamos cómo funciona.

Los datos personales son la información que permite identificar, localizar o contactar de forma directa o indirecta a una persona, por ejemplo, su nombre completo, la fecha de nacimiento, el número de cédula de identidad, una foto privada, entre otros.

2.2. **QUIÉNES** UTILIZAN ESTA INFORMACIÓN

- **Empresas:** La forma que usamos Internet es a través de empresas. Facebook, WhatsApp, TikTok son empresas transnacionales que dan servicios supuestamente gratuitos. No pagamos por ellos, pero de alguna manera tienen que generar ganancias. Una de las principales formas en que estas empresas generan ganancias es tomando nuestros datos personales (nombre, edad, gustos, situación emocional, videos que vemos, frecuencia de conexión, familiares, etc.) y usándolos para desarrollar campañas de marketing, por eso es que si le damos un me gusta en Facebook a una ropa, nos saldrán publicaciones relacionadas con ropa.
- **Gobiernos y empresas locales:** Los gobiernos y empresas locales (farmacias, bancos, etc.) también administran nuestros datos personales y cada vez más con la ayuda de sistemas informáticos. En este caso lo utilizan para ofrecernos servicios, por ejemplo, para trámites de impuestos, seguro de salud, etc.
- **Delincuentes y agresores/as:** Las personas que ejercen violencia digital, así como las o los delincuentes también utilizan nuestros datos personales, pues se valen de ellos para entrar a nuestras cuentas, suplantar nuestra identidad o publicar nuestras fotos privadas.

Por eso es que debemos conocerlos y saber protegerlos. Los datos personales que debemos cuidar son:

DATOS PERSONALES GENERALES	DATOS PERSONALES SENSIBLES	DATOS PERSONALES BIOMÉTRICOS
Información que permite identificar, localizar o contactar de forma directa o indirecta a una persona.	Datos personales que se refieren a la esfera íntima de una persona y que pueden llevar a estigmatizaciones o discriminación.	Aquellos datos personales referidos a las características físicas, fisiológicas o conductuales de una persona que posibiliten o aseguren su identificación única.
• Nombre completo. • Fecha de nacimiento. • Número de cédula de identidad. • Dirección de nuestro domicilio. • Dirección de la unidad educativa de nuestra hija o hijo. • Número de celular	• Origen racial o étnico. • Datos relativos a la salud. • Preferencia u orientación sexual. • Creencias o convicciones religiosas, filosóficas o morales.	• Huella dactilar. • Reconocimiento facial. • Reconocimiento del iris. • Reconocimiento de retina. • Reconocimiento de voz.

Ante esta situación, debemos cultivar algunas habilidades de seguridad digital a fin de que, además de proteger nuestra información personal, podamos también ayudar a proteger la información personal de nuestras/os hijas/os.

2.3 CÓMO UNA **CONTRASEÑA SEGURA** PUEDE PROTEGERNOS

Las contraseñas son las llaves de acceso a nuestra información personal en Internet, por tanto, deben estar bien protegidas y se recomienda que combinen letras, números y símbolos. Asimismo, es recomendable cambiarlas regularmente y no compartirlas con otras personas.

Ejemplos de contraseñas seguras:

- G3l@t0!2024 (mezcla de letras mayúsculas, minúsculas, números y símbolos)
- 2B@3stD@y!456 (frase modificada que incluye números y caracteres especiales)
- S@f3Pa$$w0rd#2024 (combinación de palabras con alteraciones)

Consejos prácticos:

- **Longitud:** Asegúrate de que la contraseña tenga al menos 12 caracteres. Cuanto más larga, mejor.
- **Combinaciones:** Usa una combinación de palabras, números y símbolos que tú puedas recordar, pero evita usar información personal que otros puedan adivinar fácilmente, como fechas de nacimiento o nombres.
- **Generadores de contraseñas:** Utiliza herramientas de Internet para crear contraseñas fuertes y únicas, por ejemplo: https://www.dashlane.com/es/features/password-generator también puede ingresar a esta herramienta escaneando el siguiente QR:
- **Cambio regular:** Es recomendable cambiar nuestras contraseñas cada 3 a 6 meses.

2.4 **VERIFICACIÓN** EN DOS PASOS (2FA)

La verificación en dos pasos es como tener una cerradura adicional en la puerta de nuestra casa para hacerla más segura. Imagina que necesitas dos llaves para abrirla: una es tu contraseña y la otra es un código especial que solo tú puedes recibir en tu teléfono. Primero, usas la contraseña (la primera llave) y luego introduces el código que recibes (la segunda llave).

Esta verificación en dos pasos ayuda a proteger nuestra información porque, aunque alguien descubra nuestra contraseña, no podrá acceder sin el código especial. Así, evitamos que nuestra información personal, como fotos y mensajes privados, se usen de manera indebida.

A continuación, se describe el ejercicio con WhatsApp:

- En WhatsApp, abre Ajustes.
- Toca Cuenta > Verificación en dos pasos > Activar o Configurar PIN.
- Ingresa un PIN de seis dígitos y confírmalo.
- Proporciona una dirección de correo electrónico a la que tengas acceso o, si no quieres hacerlo, toca Omitir.
- Toca Siguiente.
- Confirma la dirección de correo electrónico y toca Guardar u OK

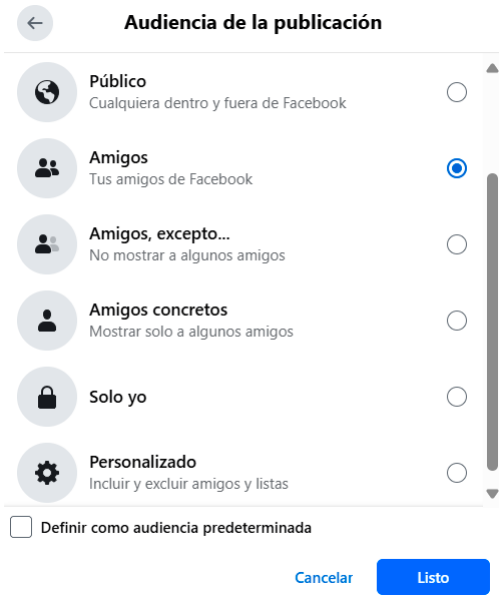
Cómo desactivar la verificación en dos pasos

- En WhatsApp, abre Ajustes.
- Toca Cuenta > Verificación en dos pasos > Desactivar.

2.5 **CONFIGURACIONES DE PRIVACIDAD** DE NUESTROS DISPOSITIVOS

Como usuarios de Internet y responsables de nuestras/os hijas/os, también debemos familiarizarnos con las configuraciones de privacidad de las redes sociales y otros servicios en línea, ajustándolas para limitar quién puede ver la información que nosotros/as o nuestras/os hijas e hijos comparten.

La mayoría de las redes sociales tienen la opción de configurar el nivel de privacidad. En el caso de Facebook, al publicar un contenido, podemos decidir si lo hacemos público (que todos/as lo vean), visibles para nuestros/as amigos/as o visibles solo para nosotros/as, como se muestra a continuación:



ACTIVIDADES DE APOYO

ACTIVIDAD 1
CREACIÓN DE **CONTRASEÑAS SEGURAS**

Objetivo: Aprender a crear y gestionar contraseñas seguras.

Instrucciones:

Reflexiona sobre una de tus contraseñas actuales. Piensa, recuerda o escribe en una hoja aparte una contraseña que utilizas en una red social (puedes modificar las contraseñas para mantener la privacidad) y evalúa si cumplen con los siguientes criterios:

» ¿Tienen al menos 12 caracteres?

SI NO

» ¿Incluyen letras mayúsculas, minúsculas, números y símbolos?

SI NO

» ¿Evitaste usar información personal fácil de adivinar?

SI NO

Crea una contraseña segura

Paso 1. Piensa en una frase larga y escríbela en el siguiente espacio (una letra por cuadro y sin espacios, por ejemplo: segurayprotegida):

Paso 2:

La I por 1, la E por 3, la T por 7. ña O por 0, la A por 4, la S por 5 y la B por 8

Paso 3. Ahora escribe la frase resultante (Siguiendo el ejemplo de segurayprotegida, la frase resultante sería: s3gur4ypr0t3g1d4):

ACTIVIDAD 2

EVALUACIÓN DE CONFIGURACIONES DE PRIVACIDAD

Objetivo: Familiarizarse con las configuraciones de privacidad de las redes sociales y comprender su importancia.

Instrucciones:

Elige una red social. Selecciona una red social que utilices regularmente (por ejemplo: Facebook, WhatsApp, Tik Tok).

Revisa la configuración de privacidad. Accede a las configuraciones de privacidad de la red social elegida, busca las siguientes opciones y anota tus hallazgos:

» ¿Tienes activada la verificación en dos pasos? Sí / No, ¿por qué es importante activarla?

» ¿Quién puede ver tus publicaciones y fotos? Es decir, ¿cómo está configurada la visibilidad de tus publicaciones? (Ajusta esta configuración si es necesario).

3. PROMOVIENDO EL **USO RESPONSABLE** DEL INTERNET DESDE UNA PERSPECTIVA CRÍTICA

APRENDIENDO SOBRE EL QR

Dos amigos, Franco y Luis, están en casa, viendo un folleto con un código QR en la mesa. Franco sostiene su teléfono móvil, mientras Luis observa.

Mientras sepamos utilizar Internet de forma segura, podemos beneficiarnos de sus potencialidades, por ejemplo, en la educación, la economía o las relaciones familiares.

3.1 USO DE **PLATAFORMAS EDUCATIVAS**

Internet no solo es una herramienta de búsqueda de información, sino también un medio para colaborar y aprender juntos/as. Hoy en día no es necesario inscribirse a un instituto para aprender, una persona puede formarse en lo que desee si conoce las fuentes adecuadas de Internet y, en el proceso, podemos guiar también a nuestras/os hijas e hijos. A continuación, presentamos algunas opciones:

a. **Plataformas de aprendizaje en línea:** Sitios web como Coursera o EDX ofrecen un entorno seguro para las personas que deseen aprender gratuitamente: https://www.coursera.org o https://www.edx.org. Como madres, padres o cuidadores, podemos compartir estas plataformas con nuestras/os hijas/os. En Bolivia, https://internetbolivia.org cuenta con una oferta de cursos gratuitos sobre cuidados digitales, uno de ellos y que puede interesarnos es: Alfabetización digital y crianza protectora en el mundo digital para madres, padres y cuidadores: https://bit.ly/4fgQVwA

b. **Banca digital, billeteras móviles y QR:** Una de las habilidades necesarias y que pueden servir a madres, padres y cuidadores son las transacciones financieras, así como el manejo de códigos QR. No obstante, esta habilidad debe aprenderse con asesoramiento y una vez que una persona sepa administrar las llaves de seguridad de sus cuentas, como contraseñas, verificación en dos pasos y los distintos niveles de seguridad.

c. **Documentos compartidos:** Plataformas como Google Docs permiten a las personas trabajar juntas en tiempo real, facilitando la colaboración en proyectos grupales, éste puede ser un buen hábito para compartir con nuestras/os hijas/os: https://drive.google.com/

Sin embargo, es preciso mencionar que la educación debe complementarse con métodos de aprendizaje tradicionales. Mientras que el acceso a Internet ofrece un sinfín de recursos educativos, es esencial fomentar un equilibrio entre el aprendizaje en línea y las experiencias de aprendizaje en el mundo real o físico.

3.2 CÓMO **MINIMIZAR RIESGOS** ASOCIADOS A VIOLENCIA DIGITAL, DESINFORMACIÓN O FRAUDES

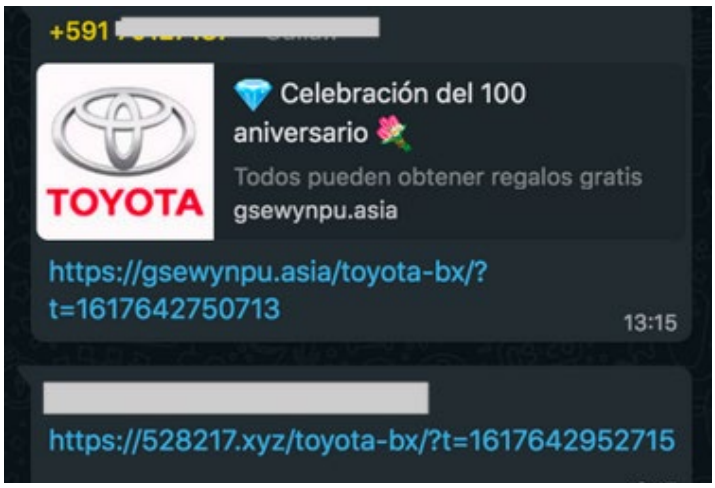
Una de las formas de uso de Internet es hacerlo críticamente, es decir evaluar lo que consumimos, analizar o indagar sus orígenes. Esta práctica puede hacer que evitemos situaciones de violencia o estafas, que hoy en día son muy habituales. En este marco, enumeramos algunas buenas prácticas que posibilitan un uso crítico de Internet:

- **Verificar la fuente.** Es fundamental comprobar quién publica la información que consumimos. Sitios web de agencias de información o medios de comunicación oficiales y organizaciones educativas suelen ser más confiables.
- **Comprobar la fecha.** La información desactualizada puede ser engañosa, así que es importante asegurarse de que el contenido sea reciente y relevante.
- **Contrastar con otras fuentes.** Resulta una muy buena práctica comparar la información que consumimos con al menos tres fuentes para asegurarnos de que esa información es precisa y veraz.
- **Reconocer enlaces maliciosos.** Son esos enlaces que podemos recibir en nuestras cuentas de WhatsApp o perfiles de Facebook o incluso como mensajes de texto (sms), pero que tienen intenciones oscuras (estafas, fraude, contenido falso). Se llama enlace malicioso porque su objetivo es engañar a la persona que recibe el enlace y robarle su información personal o ingresar a su cuenta.

Examinemos el siguiente mensaje:

Aparentemente, es un anuncio que invita a participar a una celebración donde se pueden ganar premios, incluido un vehículo Toyota. Si entramos al enlace, nos lleva a una página que pide información personal (nombre, número de teléfono, correo, contraseña, etc.).

No obstante, si examinamos la dirección de este sitio web, se trata de un sitio falso que se hace pasar por el oficial.



» **Dirección falsa** (no suele comenzar con el nombre de la empresa, tienda o servicio, sino con combinaciones de números o letras): https://528217.xyz/toyota-bx/

» **Dirección oficial** (comienza con el nombre oficial de la empresa, tienda o servicio): https://www.toyota.com/

¿Cómo reconocer los enlaces maliciosos?

» Pregúntate quién te envió el enlace: Si no conoces a la persona es mejor ignorar el enlace y no abrirlo.

» Suelen estar acompañados con mensajes relacionados a premios o intentan asustarte diciendo que ingresando al enlace encontrarás un vídeo o una foto tuya.

» Cuando ingresas usualmente te piden datos personales como tu nombre, número de teléfono, correo electrónico o contraseñas.

» Juegan con la urgencia, el mensaje puede decir que tenemos que actuar de inmediato, haciéndose pasar por un familiar lejano que se encuentra en problemas.

Si el enlace cumple con alguno de los puntos anteriores, no ingreses a él.

3.3 **ACUERDOS FAMILIARES** PARA EL USO DE TECNOLOGÍA

El uso de Internet, redes sociales o dispositivos como celulares, tabletas o computadoras debe complementarse con prácticas analógicas (mundo físico). Mientras que el acceso a Internet ofrece un sinfín de recursos y oportunidades, es esencial también fomentar un equilibrio entre el denominado "mundo real" y "mundo virtual", y estas son decisiones que se deben tomar en familia y que madres, padres y cuidadores pueden guiar. Por ejemplo:

» Acordar el tiempo en pantalla de las hijas o hijos y horas de desconexión.

» Dialogar sobre las amistades en línea de las hijas o hijos.

» Respetar las normas de comportamiento de comunidades en línea a partir del grupo de la familia.

» Establecer actividades físicas y al aire libre donde no se usen teléfonos celulares.

» Alertas ante posibles situaciones de violencia digital hacía cualquier miembro de la familia.

» Lectura de libros u otros materiales impresos que promuevan la concentración o comprensión lectora.

ACTIVIDADES DE APOYO

ACTIVIDAD 1

IDENTIFICANDO **ENLACES MALICIOSOS**

Objetivo: Enseñar a identificar y evitar enlaces maliciosos en Internet, comprendiendo los riesgos de hacer clic en sitios no seguros.

Instrucciones:

Lee el siguiente texto

Los enlaces maliciosos son aquellos que llevan a sitios web peligrosos que pueden robar tu información personal, instalar virus en tu dispositivo o engañarte para que descargues software no deseado. A veces, estos enlaces aparecen en correos electrónicos, mensajes de texto, redes sociales o anuncios en línea. Reconocerlos es clave para protegerte.

Identifica las señales de un enlace malicioso

Lee las siguientes descripciones de enlaces. Algunos son seguros y otros son maliciosos. Marca con una "✓" si crees que el enlace es seguro o con una "✗" si piensas que podría ser malicioso.

- Enlace 1: https://www.tiendaoficial.com/ropa
- Enlace 2: https://www.abc123fake.com/ganar-premios
- Enlace 3: https://www.facebook.com/mi-cuenta-segura
- Enlace 4: https://www.cs8xspremios-gratis-ya.com/registrarse

Reflexión:

- ¿Qué señales pueden indicarte que un enlace es malicioso?

- ¿Cómo puedes protegerte si encuentras un enlace sospechoso?

Recuerda que ante una situación de violencia en línea puedes escribir al **centro SOS Digital** de forma gratuita.

CENTRO SOS DIGITAL

EQUIPO DE ACOMPAÑAMIENTO Y RESPUESTA A VIOLENCIAS DIGITALES

LÍNEA DE APOYO:

+591 62342430

Signal Telegram WhatsApp

www.**sosdigital**.internetbolivia.org

Asociación Aguayo

INTERNET BOLIVIA .ORG

educo
educar cura