www

Presta atención:

Para. Piensa. Conéctate.

.com

haz click aqui

Hola!

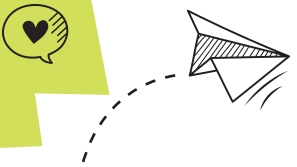
Hola!

Estar en línea es parte de tu vida. Miras y creas contenido, publicas fotos y videos, participas en juegos y compartes el lugar dónde estás y lo que estás haciendo con tus amigos y familia. Pero cuando posteas algo, participas en un juego y te conectas a internet hay riesgos. Algunas personas y situaciones que enfrentas no siempre son lo que parecen.

Aunque tus dedos viajen a alta velocidad por el teclado de tu computadora, teléfono o tablet, las mejores herramientas que tienes para evitar los riesgos cuando estás en línea son tu cerebro y tu tiempo. Para y piensa atentamente cada situación para protegerte y proteger a tus amigos y familiares, tus cuentas y tus dispositivos. O podrías terminar compartiendo más información de la que deseas, avergonzándote o avergonzando a los demás, o hablando con personas que no son quienes dicen ser.

- ✓ COMPARTE CON CUIDADO
- ✓ SER AMABLE ES GENIAL
- ✓ HAZLE FRENTE AL CIBERACOSO
- ✓ CONEXIÓN A LA PROTECCIÓN

COMPARTE CON CUIDADO



Piensa antes de compartir

Lo que haces mientras estás en línea tiene consecuencias en la vida real. Las fotos, videos y mensajes que compartes afectan tu privacidad y tu reputación y la de quienes te rodean, ahora y en el futuro. Para y piensa antes de publicar algo.

Lo que publiques puede tener más "público" de lo que pensabas.

Aunque actives las funciones de privacidad o uses aplicaciones que eliminan el contenido después de ser visto o dentro de las 24 horas, es imposible controlar totalmente quiénes ven tu perfil, fotos, videos o textos. Cualquier persona que vea tu post puede hacer capturas de pantalla o grabaciones. Pregúntate lo siguiente: "¿Te gustaría que alguien se ponga de pie en el medio del almuerzo y comparta esa foto o video con todos los que están en la cafetería de la escuela?"

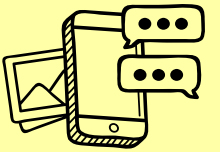
Lo que compartas podría afectar a otras personas. Enviar o publicar fotos y videos sin el permiso de las personas involucradas puede causarles vergüenza, y además puede ser injusto e incluso peligroso.

Primero, pide permiso. Antes de postear algo, pregúntales: “¿Estás de acuerdo en que publique esto en las redes sociales?” Si te dicen que no, no lo publiques.

Una vez que publicas algo en internet, ya no lo puedes quitar.

Aunque elimines algo que posteaste, o aunque la publicación expire, esa foto o comentario que ya no quieres que la gente siga viendo podría guardarse, compartirse y seguir disponible en línea de manera permanente.

Sexting: No lo hagas



Es posible que en la escuela o en las noticias hayas escuchado acerca de personas que hacen “sexting”, que consiste en enviar fotografías con desnudos desde el teléfono. No lo hagas. Punto. Crear, enviar o incluso guardar fotos, videos o mensajes con imágenes sexuales explícitas, pone en peligro tus amistades y tu reputación. Peor aún, podrías estar infringiendo la ley.

Una nota sobre los medios sociales

Según el Director General del Servicio Federal de Salud Pública, el uso de las redes sociales puede perjudicarnos, dependiendo del tiempo que pasemos en las plataformas, el tipo de contenido que veamos y en qué medida interrumpe cosas como el sueño o el ejercicio, actividades esenciales para nuestra salud.

SER AMABLE ES GENIAL

La cortesía es importante

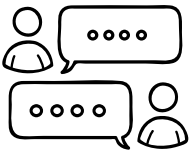
Cuando te comunicas en línea y no puedes ver las expresiones faciales de otra persona, o su lenguaje corporal u otras señales visuales, es posible que te sientas cómodo publicando o diciendo cosas que no harías en persona. Pero enviar mensajes de texto, postear, comunicarte por chat, participar en videojuegos y enviar emails es lo mismo que hablar cara a cara con otra persona. Presta atención a cómo te comunicas y piensa antes de hablar o publicar algo.

Baja la velocidad. Es fácil tener malentendidos en línea. Antes de enviar un mensaje, pregúntate: "¿Cómo se sentirán las otras personas con este mensaje?"

Cuando estés en línea, considera y respeta las perspectivas y sentimientos de los demás, de la misma manera que lo harías en persona. Recuerda que detrás de los avatares y nombres de perfiles hay personas de carne y hueso.

Baja el tono. No uses TODO EN MAYÚSCULAS, largas filas de signos de exclamación o un tipo de letra muy destacada. Eso es lo mismo que gritar.

No pongas todo en el chat grupal. Antes de enviar un mensaje grupal o de hacer clic en Responder a todos, para y piensa: ¿quién necesita ver este mensaje?



No finjas ser otra persona

Crear perfiles, escribir comentarios o postear algo que parece provenir de otra persona, por ejemplo, de algún compañero de clase o de un maestro, está mal y podría causar daño.

No te quedes callado

Si ves que un amigo está posteando algo desconsiderado o peligroso, díselo. Puedes evitar que tu amigo se meta en líos y pase vergüenza.

Si ves algo inapropiado en línea, repórtalo y cuéntaselo a un adulto de confianza. La mayoría de las aplicaciones y plataformas tienen una manera de reportar a las personas que tienen un comportamiento amenazante o inapropiado.

Hazle frente al ciberacoso

Todos merecen sentirse seguros en sus interacciones diarias con otras personas, ya sea en línea o cara a cara.

Si alguien publica comentarios malintencionados, memes hirientes, fotos embarazosas o envía chats o mensajes privados sobre ti, eso es acoso. Y eso no está bien. Habla con un adulto de confianza para que te ayude a lidiar con la situación y decidir cómo deberías responder.

Si alguien te acosa en línea, esto es lo que tienes que hacer:

- **Ignora** a la persona o bloquéala para que no te vuelva a contactar.

- **Guarda** los registros y pídele ayuda a un adulto de confianza.
- **Repórtalo.** Muchas aplicaciones y plataformas tienen herramientas para reportar a las personas que tienen un comportamiento amenazante o inapropiado.

El acoso suele provocar malestar en la persona intimidada, y da una mala imagen del acosador. Acosar a alguien también puede ponerte en problemas con las autoridades de tu escuela y con la policía.

Si eres testigo de un ciberacoso, busca formas de convertirte en algo así como un defensor, es decir, alguien que interviene, interrumpe o habla para detener el acoso. Por lo general, este mal comportamiento se frena bastante rápido cuando alguien sale en defensa de la persona acosada.

Se amable ☺

CONEXIÓN a la PROTECCIÓN

Protege tu privacidad

Cuando haces algo en línea, dejas un rastro. Sigue estos pasos para asegurarte de que ese rastro no lleve hacia información que quizás no tenías intención de compartir.

Usa las funciones de privacidad. Averigua cómo activar las funciones de privacidad de los dispositivos, aplicaciones y cuentas de medios sociales, y luego actívalas. Esto te ayuda a limitar quién puede ver dónde estás, lo que publicas y quién puede conectarse contigo.

Revisa tu configuración de localización. Algunas aplicaciones te permiten ver dónde están tus amigos. Y también comparten el lugar dónde estás tú. Piensa si tiene sentido estar compartiendo tu localización. Cuando no tenga sentido, desactiva la función de compartir ubicación. Algunas funciones de tu dispositivo, por ejemplo, tu cámara, podrían tener información sobre el lugar donde te encuentras cuando tomas una fotografía. Si no quieres difundir el lugar donde estabas en cada selfie, desactiva la función de localización en la

cámara de tu teléfono. Pregúntate siempre: "¿Es necesario que esta aplicación sepa dónde estoy?"

Limita tu lista de amigos en línea únicamente a la gente que realmente conoces. Conectarse con amigos a través de mensajes de texto, redes sociales o videojuegos puede ser divertido, pero en internet hay algunas personas que no son quienes dicen ser. Y si no eres cuidadoso, podrías compartir información personal con un extraño.

Protege tu información

Una vez que le das tu información personal a un desconocido, por ejemplo, tu número de Seguro Social, contraseñas o datos de cuentas bancarias, no hay manera de recuperarla.

A continuación, te decimos cómo proteger tu información en línea:

No respondas los mensajes que pidan información personal. Aunque el mensaje parezca que fue enviado por un amigo, un familiar o una compañía que conoces, o diga que te va a pasar algo malo si no respondes. Es probable que sea falso y que te lo hayan enviado para robarte información. Pídele a un adulto de confianza que te ayude a reportar el mensaje como basura o spam.

Antes de descargar una aplicación, revisa a qué información quiere acceder. Algunas aplicaciones piden permiso para acceder a información o funciones que no necesitan, como tu lista de contactos, cámara, almacenamiento, localización y micrófono. Pídele ayuda a un adulto de confianza para leer la política de privacidad de la aplicación y saber cómo se utilizarán tus datos y si se compartirán. Luego decide si ese juego de palabras realmente necesita acceso a tus fotografías.

Habla con un adulto de confianza antes de hacer compras a través de una aplicación, especialmente si las están pagando.

Protege tus cuentas

Tú guardas un montón de información personal en tus cuentas en línea. Estos son algunos pasos a seguir para evitar que otras personas se metan en tus cuentas.

Crea contraseñas sólidas. Cuando más extensa sea la contraseña, más difícil será descifrarla. Usa como mínimo 12 caracteres con una mezcla de letras mayúsculas y minúsculas, números y símbolos. Para que sea más fácil de recordar, considera la posibilidad de crear una frase de acceso con palabras elegidas al azar. Pero no uses frases

comunes, letras de canciones o citas de películas que sean fáciles de adivinar.

Sé único. Crea contraseñas diferentes para tus diferentes cuentas. De esa manera, si alguien obtiene tu contraseña para una cuenta, no puede usarla para acceder a tus otras cuentas. Una manera de llevar el control de todas tus contraseñas es utilizar un administrador de contraseñas.

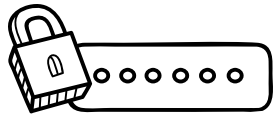
Mantenlas en privado. No compartas tus contraseñas con nadie, ni siquiera con tu mejor amigo o con la persona con la que estás saliendo.

Sé exigente con las preguntas de seguridad. Trata

de seleccionar preguntas de seguridad que solo tú puedas responder. Evita las preguntas cuyas respuestas se puedan encontrar en internet, como tu código postal, fecha de nacimiento o el apellido de soltera de tu madre. Si no puedes evitar esas preguntas ¡sé creativo! Trátalas como si fueran contraseñas y usa respuestas aleatorias y extensas. Asegúrate de recordar tus respuestas.

Usa un sistema de autenticación de múltiples factores. Muchas cuentas te ofrecen una protección adicional con un sistema de "autenticación de

múltiples factores" que te pide algo más que una contraseña. El sistema de autenticación de múltiples factores combina algo que tú sabes (como una contraseña) con algo que tienes (como un código de acceso generado por una aplicación) o por alguna característica personal (como una huella dactilar).



Si se produce un incidente de seguridad de datos, cambia tus contraseñas rápidamente. Si una compañía te dice que sufrió una filtración de datos y que un pirata informático podría haber conseguido tu contraseña, cambia de inmediato la contraseña que usas para esa cuenta. Y si usas una contraseña similar para alguna otra cuenta, cámbiala también.

Protege tus dispositivos

¿La mejor manera de disfrutar tu experiencia en línea? Asegurarte de que tus dispositivos sean seguros y estén protegidos. Comienza por aquí:

Configura tu programa de seguridad para que se actualice automáticamente en todos tus dispositivos, navegadores de internet y sistema operativo. Esto te ayuda a protegerte contra las nuevas amenazas de seguridad.

No hagas clic en los enlaces ni abras archivos adjuntos. Si recibes inesperadamente un mensaje

de texto, email o un mensaje que dice que tienes que hacer clic en un enlace o abrir un archivo. ¡no lo hagas! Aunque te estén ofreciendo algo gratis. Los enlaces y archivos adjuntos pueden ocultar virus o programas espías que podrían estropear tu teléfono, computadora o tablet.

Protege tus dispositivos con contraseñas. Esto te ayudará a evitar que tus fotografías, mensajes y cuentas caigan en las manos equivocadas.

Guárdalos en un lugar seguro. No descuides ni dejes a la vista del público tu teléfono, computadora portátil o tablet, ni siquiera por un minuto.

Aprende más en **ftc.gov/ChicosEnInternet**

Para obtener copias gratuitas
de este folleto visita

ftc.gov/ordenar

COMISIÓN FEDERAL
DE COMERCIO

Agosto 2023