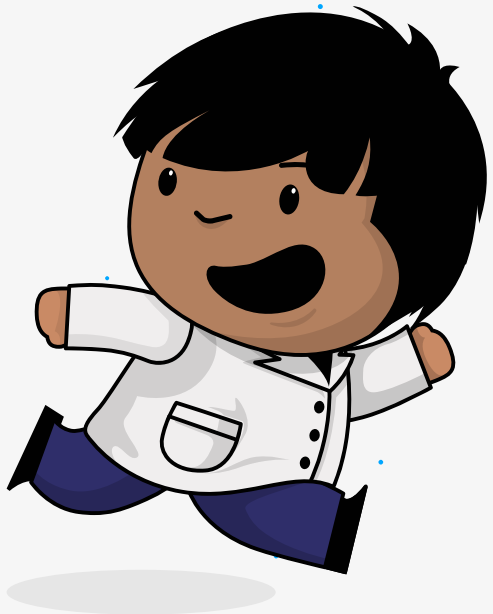
¡ZAMBA Y TINA!

CUIDADOS Y SEGURIDAD EN INTERNET



CONTENIDOS PÚBLICOS | SOCIEDAD DEL ESTADO

PAKA PAKA

Secretaría de Innovación Pública

Jefatura de Gabinete de Ministros Argentina

¡Hola!, ¿Sos Zamba? ¿Qué hacés por acá?

Hola, ¿vos quién sos?

Yo soy TINA. Soy un chatbot basado en Inteligencia Artificial...

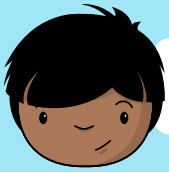
¿Qué? ¿Inteligencia artificial? Y eso ¿qué es?

La inteligencia artificial es la capacidad que tiene una computadora para procesar información. Con esto puedo producir resultados de manera similar al proceso de pensamiento de los seres humanos, como aprender, tomar decisiones y resolver problemas.

Fuaaa. ¡Qué bueno Tina! Entonces vos sabés todo... Decime, qué es internet?

Bueno, bueno Zamba, vamos de a poco.

¿QUÉ ES INTERNET?



Tina, y ¿qué es internet?

¡Qué buena pregunta Zamba! Porque todos y todas usamos Internet, pero ¿qué es?

Internet es una gran red de redes. Es un sistema conectado de manera continua y simultánea, que permite a las personas intercambiar información a través de computadoras, celulares, televisores, parlantes, juguetes y hasta heladeras y lavarropas. Con el avance de las tecnologías, hoy no es necesario el uso de cables para conectarse a la red.

En Internet trabajamos, estudiamos, jugamos, escuchamos música, aprendemos a cocinar, vemos series y pelis, compartimos fotos, videos e ideas. Y las personas adultas también pueden comprar y vender cosas, conocer gente, realizar transacciones o ver en vivo cosas que pasan en cualquier lugar del mundo.

¿Sabías que la primera prueba de conexión de lo que después sería Internet se hizo en 1969? El desarrollo fue del Departamento de Defensa de EEUU que creó la red ARPANET, por la que se estableció el primer enlace entre dos universidades por medio de una línea telefónica.

¿CÓMO NOS CUIDAMOS EN INTERNET?

Tina, ¿y por qué en Internet hay que cuidarse? ¿De qué nos tenemos que cuidar?

Eso es muy importante Zamba ¿Sabías que cada año, las niñas y los niños pasan más tiempo en Internet?

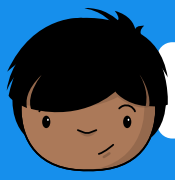
Y si aumenta el tiempo que estamos en Internet, también aumentan los riesgos digitales. Por eso es importante cuidarnos.

Lo más importante es la prevención. Así como nos lavamos las manos para prevenir enfermedades, en Internet también tenemos que tomar medidas de cuidado.

Antes de conectar tu computadora a Internet hay que instalar un antivirus seguro y confiable.

Y hay algo más: los chicos y chicas saben mucho de tecnología y la usan desde que son muy chiquitos. Pero ¡Atención! Es importante que las personas adultas que nos cuidan conozcan las redes que usamos, los juegos y las plataformas con las que nos vinculamos con amigas y amigos, hasta que aprendamos hacerlo con responsabilidad y autonomía.

¿QUÉ SON LOS DATOS PERSONALES?



Yo me llamo José, me dicen Zamba. Nací en Clorinda, Formosa....

Claro Zamba, esos son algunos de tus datos personales. Pero en Internet son tu identidad digital. Y dar esos datos puede ponerte en peligro. Todo lo que compartís en Internet, fotos, videos y textos, es información. Ahí aparecen las caras de tus familiares y amigos, tu escuela, los horarios de tus rutinas, el club del que sos hincha. Toda esa información que publicás puede estar a disposición de cualquiera.

Por ejemplo, cada vez que te piden información: tu nombre, tu edad, dónde vivís, o cuando ingresas a una red social, con tu correo electrónico. Pero también damos información sin darnos cuenta: cada vez que el historial de navegación queda registrado en un dispositivo, con las interacciones con otros/as usuarios y usuarias, o cuando activás funcionalidades del sistema que brindan información a terceros, por ejemplo, el acceso a la ubicación o a la galería multimedia.

Para ingresar a una cuenta, además de completar la contraseña, podés validar que sos vos a través de un código que puede llegar por mensaje de texto, por correo electrónico o mediante una llamada a tu número de teléfono. Los adultos y adultas que te cuidan te pueden ayudar.

¡Y algo más! Es muy importante cuidar toda la información que tenemos en el celu o en la compu, porque todos los dispositivos que usamos guardan una gran cantidad de datos personales que usamos para estudiar, vincularnos y jugar.

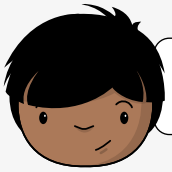
Por eso, protegerlos también es cuidar nuestros datos y nuestra identidad.

Te voy a dar un par de consejos para que puedas cuidar los dispositivos desde los que entras a tus cuentas :

- Usar un patrón, huella digital, reconocimiento facial o clave de ingreso según lo que prefieras y dentro de las posibilidades de tu dispositivo.
- Hacer una copia de seguridad que incluya fotos, documentos, imágenes y archivos importantes.
- Activar las conexiones por Bluetooth, NFC y WiFi sólo cuando vayas a utilizarlas.
- Tratar de que otras personas sólo utilicen tus dispositivos con tu autorización.
- Cerrar todas las sesiones iniciadas al terminar de usarlas.
  Mantener el software del dispositivo siempre actualizado.
  Instalar y mantener el antivirus actualizado.
- Descargá aplicaciones únicamente de sitios de confianza u oficiales.
- Configurá la autenticación de dos factores para las aplicaciones.
- Habilitá sólo los permisos necesarios.

Y algo super importante: no hay que dejar los dispositivos al alcance de otras personas y siempre hay que llevarlos en un lugar seguro cuando viajás.

¿CÓMO ELEGIMOS CONTRASEÑAS SEGURAS?



Mirá estoy poniendo una contraseña nueva.. Zamba2023 ¿Te gusta?

Mmmm. Las contraseñas son llaves o candados que protegen la información e impiden que alguien ingrese a nuestros dispositivos o cuentas. ¡Las claves o contraseñas compartirlas sólo con personas de confianza, como los adultos y adultas que te cuidan! Para que las contraseñas sean seguras, hay que cambiarlas regularmente y seguir estos consejos:

- Usar letras en mayúsculas y minúsculas, números y caracteres especiales. Que tengan al menos ocho caracteres o más.

- Puede ser una frase que otros no conozcan. Por ejemplo: Verdl4ydos ("Verano del 42")

- Una palabra sin sentido pero pronunciable que te sea familiar y sumar algún carácter especial. Por ejemplo, Kiri_Cocho. Reemplazar letras por signos o números. Por ejemplo, M3s51_C4mpe0N

- La fecha de un hecho importante para vos. Por ejemplo: @rGenTina-18-12-22

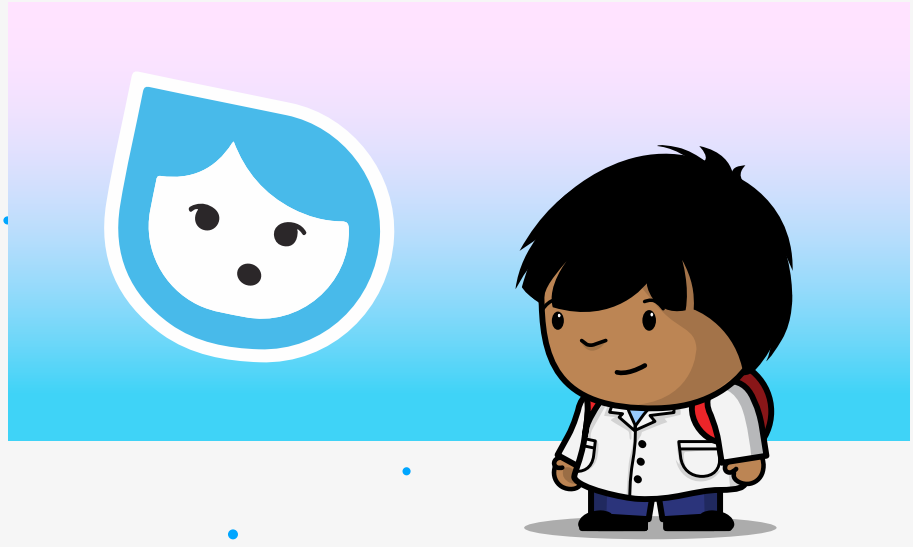
Además, tenés que:

- Evitar palabras comunes o nombres que se puedan adivinar fácil. ¡No pongas tu nombre!
- No usar datos personales (como el número de documento o la fecha de nacimiento).
- No repetir la misma contraseña en dispositivos o redes sociales.
- No guardar las contraseñas en dispositivos que no sean nuestros.

Recomendaciones para adultos y adultas responsables

En lugares de trabajo u otros espacios donde utilizamos dispositivos compartidos es recomendable cerrar todas las sesiones abiertas al terminar la jornada y dejar el dispositivo. Nunca guardes las contraseñas en computadoras que no sean personales.

Existen aplicaciones que guardan tus contraseñas, te brindan sugerencias robustas y sirven de ayuda a la memoria para recordarlas.



¿CÓMO PUEDO CUIDAR MI PRIVACIDAD EN INTERNET?

Todo lo que subimos en las redes tiene más información de la que queremos compartir: nombres, equipos de fútbol, fechas importantes, barrio en el cual vivimos o hasta las caras de chicas y chicos que no quieren estar en las redes. Esa información sirve para que otras personas puedan obtener más datos nuestros o de amigos, amigas o familiares. Y también a veces tenemos contactos que no son tan cercanos o no queremos que algunas fotos o posteos los vea cualquier persona.

¡Eso lo sé! Por eso hay configurar nuestros perfiles como privados. Y también hay funciones que permiten compartir contenido con algunos contactos y no con todos. ¿Cuándo usamos videojuegos también?

Sí, Zamba. Porque estas plataformas te permiten vincularte con personas de cualquier parte del mundo y de cualquier edad. Te relacionás por medio del avatar que te representa pero también por chats que tienen algunos juegos.

¡Prestá mucha atención! Los videojuegos en línea no son peligrosos, siempre y cuando estemos atentos a cosas como:

- No poner tu nombre ni datos reales.
- Evitar usar auriculares.
- Configurar la seguridad de tus dispositivos.
- Usar contraseñas seguras para todas nuestras cuentas.
- No usar la misma contraseña en todas tus redes.
- Cambiar las contraseñas al menos cada 30 días.

Recomendaciones para adultos y adultas responsables

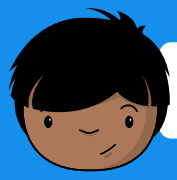
- Habilitá filtros para los menores.
- Recordá que las consolas tienen navegador por lo que se recomienda utilizar filtros o controles parentales para evitar el acceso a sitios para mayores de edad.
- Habilitar la privacidad de tus dispositivos para que sólo puedan ver tus estados y tu información las personas de confianza.
- Limitá el uso del chat a la consola. Evitá que las niñas, niños y adolescentes participen en grupos de WhatsApp u otros servicios de mensajería porque algunas personas pueden tener otros fines.
- Evitá que las niñas, niños y adolescentes usen auriculares para monitorear sus charlas en los chats.

Además, cuando compramos un juego es importante hacerlo o descargarlo de tiendas oficiales para evitar estafas o archivos peligrosos. También es importante que revisemos si:

- Piden datos personales o de la tarjeta de crédito.
- Envían formularios para completar o te piden descargar archivos prometiendo actualizaciones o mejoras en el videojuego.
- Piden los datos de tu usuario del videojuego para habilitar opciones de juegos digitales.

- Por último y más importante: Hablá con los chicos y chicas, preguntales de qué trata el juego, cuál es el objetivo. Interiorizate en el mundo del juego digital.

¿QUÉ ES Y CÓMO ME CUIDO DEL PHISHING?

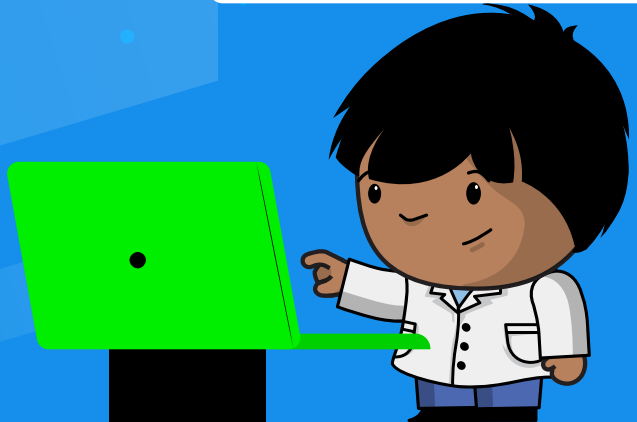


Phi-shin...¿pishing? ¿Y eso qué es Tina?

El phishing es una forma de estafa mediante correos electrónicos y sitios web engañosos, generalmente avisando de ofertas o premios falsos. Esto hace que entreguemos información personal o contraseñas, y eso permite que nos roben nuestra identidad digital.

Anotá estas recomendaciones:

- Verificá que el correo electrónico que te llega sea de una dirección confiable. Si no estás seguro, no ingreses nunca a los links que estén en los correos ni descargues o abras los archivos adjuntos.
- Protegé las contraseñas y no las compartas.
- No des información personal.
- Comprobá la dirección web a la que te redirigen. Por lo general, estas direcciones están mal escritas o tienen un dominio diferente.
- Mantené actualizadas las herramientas de seguridad en computadoras y dispositivos móviles.
- Chequeá que sean sitios seguros: se identifica con la letra "s" en "https" o con un candado cerrado en el navegador ubicado donde está la dirección web.
- Siempre pedí ayuda a algún adulto o adulto de tu confianza.



¿QUÉ ES Y CÓMO ME CUIDO DEL GROOMING?

¿Y sabés que es el grooming Zamba?

Si, Tina. Eso me lo enseñó la Srita. Silvia. Es el acoso que hace una persona mayor, por medio de las tecnologías, hacia un niño, niña o adolescente con el objetivo de cometer un delito contra la integridad sexual de las o los menores. El acoso puede darse con o sin presencia física y el/la acosador/a puede ser una persona conocida que se acerca a la víctima de forma amigable o una persona desconocida que puede acercarse mintiendo o no sobre su edad.

Información para adultos y adultas responsables

El objetivo del "groomer" es establecer una relación de confianza para enviar imágenes íntimas y luego pedirle a la niña, el niño o adolescente que también envíe fotos suyas.

Si el niño, niña o adolescente no envía estas fotos, puede que la o el/la acosador/a desaparezca o amenace a la víctima con difundir las imágenes que le mandó antes. También puede utilizar esa amenaza para lograr un encuentro fuera de la virtualidad.

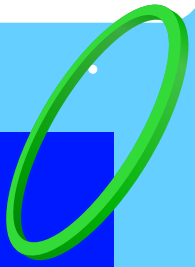
Para cuidarnos del grooming, podemos usar perfiles privados en las redes sociales y no aceptar a personas desconocidas como contactos. Evitemos publicar fotos nuestras o de amigos y amigas en lugares como plazas, shoppings o en la calle. También tenemos que rechazar mensajes o conversaciones sexuales y usar contraseñas fuertes y secretas.

¿QUÉ HAGO SI ESTOY EN UNA SITUACIÓN DE GROOMING?

Si alguien nos hace Grooming, lo primero que tenemos que hacer es contárselo a algún adulto o adulta de confianza. ¡Eso es muy importante!

Además, **siempre podemos decir que NO**. Nadie nos puede obligar a hacer algo que no queremos, que nos incomoda o que nos avergüenza. **Si nos amenazan, también podemos decir que NO.**

Y ¿sabés qué otra cosa es importante? No hay que bloquear al groomer ni borrar las conversaciones, fotos o amenazas porque puede servir a las y los investigadores para identificar quién es y así detenerlo.



Recomendaciones para adultos y adultas responsables

En caso que un niño o niña sea víctima de grooming y/o accedió al chantaje del acosador, se desaconseja retar o responsabilizar a la víctima ya que fue manipulada por un adulto. Siempre se la/lo debe contener, quitarle culpas y ofrecerle comprensión y generar un espacio de confianza donde se sienta segura/o.

No se recomienda escrachar ni bloquear las conversaciones del acosador, o fotos, amenazas, chats, etc. en los dispositivos de la víctima. Se indica recurrir a la fiscalía o comisaría más cercana para realizar la denuncia. El material guardado puede ayudar a identificar al acosador/a frente a una denuncia. Para recibir más información y asesoramiento, está disponible la línea 137 del Ministerio de Justicia y Derechos Humanos de la Nación. Atiende todo el año y es gratuita.

Recomendaciones para transmitirles a niñas y niños

Para intentar que los niños y las niñas no caigan en la trampa de groomers, debemos siempre dialogar y pedirles que:

- Usen perfiles privados en las redes sociales.
- No acepten personas desconocidas en las redes sociales.
- No publiquen fotos personales o de amigos en sitios públicos.
- Rechacen mensajes o conversaciones sexuales, eróticas o pornográficas.
- Se aseguren de que la foto que suban no tenga algún componente sexual.
- No acceder al chantaje, y avisar lo sucedido a algún adulto y/o autoridad.
- No sientan vergüenza o culpa y anímense a hablar con un mayor sobre lo que está pasando.
- Abrir un canal de diálogo ayudará a evitar un daño, muchas veces, irreparable.

Llamando **gratis al 137** podemos recibir más información y ayuda por parte del Ministerio de Justicia y Derechos Humanos de la Nación.

¿QUÉ ES EL SHARENTING?

Tina, Tina...¿los chicos y las chicas podemos pedir que los adultos no compartan nuestra fotos en las redes?

¡Claro Zamba! Muchas veces los padres y las madres comparten en redes sociales fotos y videos de sus hijos/as. Pero la mayoría de las veces este material se sube sin la aprobación de las y los chicos/as. Eso se llama sharenting.

Toda esa información de niñas, niños y adolescentes les puede dar datos a terceros que pueden no ser personas de tanta confianza. Por eso, podés pedirles que no publiquen tu información y las personas adultas deben respetar tu derecho a la intimidad.

Recomendaciones para adultos y adultas responsables

- Tené en cuenta que una vez que subís imágenes o videos, pasan a pertenecer al espacio público.
- Configurá la privacidad y seguridad de tus redes para que solo las personas que vos autorices puedan ver lo que compartís.
- Recordá que las fotos de personas menores desnudas pueden ser utilizadas por redes de pedofilia.
- Leé los términos y condiciones de las redes sociales para enterarte qué hacen con las imágenes o videos que subís.
- Las imágenes o videos que subís pueden guardarse en servidores que están fuera de Argentina y si necesitás borrarlas puede ser difícil porque no estás cubierto por las leyes argentinas.
- Cuidá la reputación en línea de tus hijas e hijos para minimizar el riesgo de exposición y viralización de todo contenido que incluya a menores. Podés resguardar su identidad con un emoji 😊

¿QUÉ ES EL PHUBBING?

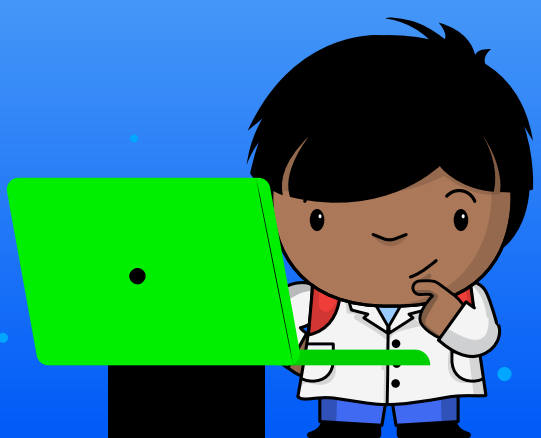
A mí me encanta jugar jueguitos y mirar videos en Internet. Pero a veces la Srita. Silvia nos dice que no podemos estar siempre conectados.

Claro Zamba. Eso también tiene un nombre. Se llama phubbing y se refiere a estar siempre conectados/as a Internet e ignorar a una persona o no prestar atención a lo que pasa alrededor por estar mirando el teléfono celular.

El Phubbing puede provocar aislamiento, accidentes al cruzar la calle, una vía de tren o simplemente esquivar un poste en la vereda.

Puede ser por tener un acceso ilimitado a internet o por el miedo a perderte algo importante en las redes. También tener notificaciones todo el tiempo o estar siempre con el celular a mano, aunque estés comiendo o jugando con tus amigos y amigas.

Para evitarlo, lo primero es usar las tecnologías en forma medida. Algunas cosas que se pueden hacer son: desactivar las notificaciones de algunas aplicaciones o silenciar los dispositivos en algunos horarios; instalar una app que mida el tiempo que pasás en la pantalla para darte cuenta de cuánto usás el celular; no usar el celular antes de dormir. Y también, guardar el celular cuando te encontrás a jugar con tus amigos y amigas.



Recomendaciones para adultos y adultas responsables

- Desactivar las notificaciones o silenciar tus dispositivos.
- Revisar los permisos de notificaciones que diste a las compañías y aplicaciones. Las notificaciones en exceso generan infoxicación.
- Instalar una aplicación que mida el tiempo que pasás consultando tu pantalla.
- Disfrutar de las personas con las que compartís el desayuno, el café, el almuerzo o la cena y conversá sin celulares cerca.
- Tomarse un día libre del teléfono y practicar lo que se llama "silencio digital" que es necesario para generar tiempos para pensar, para reflexionar o simplemente para hablar con uno mismo.
- No usar celulares justo antes de ir a dormir.
- Acordar horarios y normas de uso del celular en la casa.

¡Por eso es importante conocer el protocolo **PATRIA**!

P rotejamos nuestros dispositivos y cuentas en Internet. Elijamos contraseñas fuertes, que debemos renovar frecuentemente.

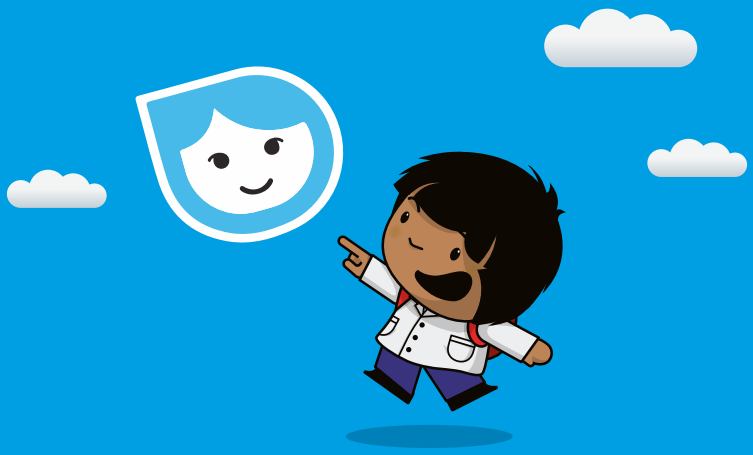
A ctualicemos los sistemas operativos y aplicaciones que usamos.

T odos nuestros datos son parte de la identidad digital, debemos cuidarlos.

R evisemos desde dónde nos envían un mail y las direcciones de páginas a las que accedemos.

I nformemos a una persona adulta si nos sentimos en riesgo, incómodas, incómodos o amenazados y amenazadas en línea.

A dministremos el tiempo que pasamos en redes sociales y aplicaciones.



CONTENIDOS PÚBLICOS | SOCIEDAD DEL ESTADO

PAKA PAKA

Secretaría de Innovación Pública

Jefatura de Gabinete de Ministros
Argentina