¿“Pescadores” de datos?

Grado 5° Guía 4

TIC

Estudiantes

Apoya:

Educación

BRITISH COUNCIL

Colombia Programa
{EL CÓDIGO A TU FUTURO}

¿“Pescadores” de datos?

Grado 5° Guía 4

TIC

Estudiantes

Educación

BRITISH COUNCIL

Colombia Programa
{EL CÓDIGO A TU FUTURO}

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Julián Molina Gómez
Ministro TIC

Luis Eduardo Aguiar Delgadillo
Viceministro (e) de Conectividad

Yeimi Carina Murcia Yela
Viceministra de Transformación Digital

Óscar Alexander Ballen Cifuentes
Director (e) de Apropiación de TIC

Alejandro Guzmán
Jefe de la Oficina Asesora de Prensa

Equipo Técnico
Lady Diana Mojica Bautista
Cristhiam Fernando Jácome Jiménez
Ricardo Cañón Moreno

Consultora experta
Heidy Esperanza Gordillo Bogota

BRITISH COUNCIL

Felipe Villar Stein
Director de país

Laura Barragán Montaña
Directora de programas de Educación, Inglés y Artes

Marianella Ortiz Montes
Jefe de Colegios

David Vallejo Acuña
Jefe de Implementación Colombia Programa

Equipo operativo
Juanita Camila Ruiz Díaz
Bárbara De Castro Nieto
Alexandra Ruiz Correa
Dayra Maritza Paz Calderón
Saúl F. Torres
Óscar Daniel Barrios Díaz
César Augusto Herrera Lozano
Paula Álvarez Peña

Equipo técnico
Alejandro Espinal Duque
Ana Lorena Molina Castro
Vanesa Abad Rendón
Raisa Marcela Ortiz Cardona
Juan Camilo Londoño Estrada

Edición y coautoría versiones finales
Alejandro Espinal Duque
Ana Lorena Molina Castro
Vanesa Abad Rendón
Raisa Marcela Ortiz Cardona

Edición
Juanita Camila Ruiz Díaz
Alexandra Ruiz Correa

British Computer Society – Consultoría internacional

Niel McLean
Jefe de Educación

Julia Adamson
Directora Ejecutiva de Educación

Claire Williams
Coordinadora de Alianzas

Asociación de facultades de ingeniería - ACOFI

Edición general
Mauricio Duque Escobar

Coordinación pedagógica
Margarita Gómez Sarmiento
Mariana Arboleda Flórez
Rafael Amador Rodríguez

Coordinación de producción
Harry Luque Camargo

Asesoría estrategia equidad
Paola González Valcárcel

Asesoría primera infancia
Juana Carrizosa Umaña

Autoría
Arlet Orozco Marbello
Harry Luque Camargo
Isabella Estrada Reyes
Lucio Chávez Mariño
Margarita Gómez Sarmiento
Mariana Arboleda Flórez
Mauricio Duque Escobar
Paola González Valcárcel
Rafael Amador Rodríguez
Rocío Cardona Gómez
Saray Piñerez Zambrano
Yimzay Molina Ramos

PUNTOAPARTE EDITORES

Diseño, diagramación, ilustración, y revisión de estilo

Impreso por Panamericana Formas e Impresos S.A., Colombia

Material producido para Colombia Programa, en el marco del convenio 1247 de 2023 entre el Ministerio de Tecnologías de la Información y las Comunicaciones y el British Council

Esta obra se encuentra bajo una Licencia Creative Commons Atribución-No Comercial 4.0 Internacional. https://creativecommons.org/licenses/by-nc/4.0/

CC BY-NC 4.0

"Esta guía corresponde a una versión preliminar en proceso de revisión y ajuste. La versión final actualizada estará disponible en formato digital y puede incluir modificaciones respecto a esta edición"

Prólogo

Estimados educadores, estudiantes y comunidad educativa:

En el Ministerio de Tecnologías de la Información y las Comunicaciones, creemos que la tecnología es una herramienta poderosa para incluir y transformar, mejorando la vida de todos los colombianos. Nos guia una visión de tecnología al servicio de la humanidad, ubicando siempre a las personas en el centro de la educación técnica.

Sabemos que no habrá progreso real si no garantizamos que los avances tecnológicos beneficien a todos, sin dejar a nadie atrás. Por eso, nos hemos propuesto una meta ambiciosa: formar a un millón de personas en habilidades que les permitan no solo adaptarse al futuro, sino construirlo con sus propias manos. Hoy damos un paso fundamental hacia este objetivo con la presentación de las guías de pensamiento computacional, un recurso diseñado para llevar a las aulas herramientas que fomenten la creatividad, el pensamiento crítico y la resolución de problemas.

Estas guías no son solo materiales educativos; son una invitación a imaginar, cuestionar y crear. En un mundo cada vez más impulsado por la inteligencia artificial, desarrollar habilidades como el pensamiento computacional se convierte en la base, en el primer acercamiento para que las y los ciudadanos aprendan a programar y solucionar problemas de forma lógica y estructurada.

Estas guías han sido diseñadas pensando en cada región del país, con actividades accesibles que se adaptan a diferentes contextos, incluyendo aquellos con limitaciones tecnológicas. Esta es una apuesta por la equidad, por cerrar las brechas y asegurar que nadie se quede atrás en la revolución digital. Quiero destacar, además, que son el resultado de un esfuerzo colectivo: más de 2.000 docentes colaboraron en su elaboración, compartiendo sus ideas y experiencias para que este material realmente se ajuste a las necesidades de nuestras aulas. Además, con el apoyo del British Council y su red de expertos internacionales, hemos integrado prácticas globales de excelencia adaptadas a nuestra realidad nacional.

Hoy presentamos un recurso innovador y de alta calidad, diseñado en línea con las orientaciones curriculares del Ministerio de Educación Nacional. Cada página de estas guias invita a transformar las aulas en espacios participativos, creativos y, sobre todo, en ambientes donde las y los estudiantes puedan desafiar estereotipos y explorar nuevas formas de pensar.

Trabajemos juntos para garantizar que cada estudiante, sin importar dónde se encuentre, tenga acceso a las herramientas necesarias para imaginar y construir un futuro en el que todos seamos protagonistas del cambio. Porque la tecnología debe ser un instrumento de justicia social, y estamos comprometidos a que las herramientas digitales ayuden a cerrar brechas sociales y económicas, garantizando oportunidades para todos.

Con estas guias, reafirmamos nuestro compromiso con la democratización de las tecnologías y el desarrollo rural, porque creemos en el potencial de cada región y en la capacidad de nuestras comunidades para liderar el cambio.

Julián Molina Gómez
Ministro de Tecnologías de la Información y las Comunicaciones
Gobierno de Colombia

Grado 5º Guía 4

TIC

Guía de íconos

Seguridad en el mundo digital

Aprendizajes de la guía

Con las actividades de esta guía se espera que puedas avanzar en:

- Reflexionar sobre la importancia de tomar medidas de ciberseguridad que protejan la información personal y la identidad.
- Familiarizarte con estrategias para proteger la identidad y los datos personales ante el *phishing*.

Resumen de la guía

Esta guía desarrolla, durante 5 sesiones, algunos conceptos importantes sobre el uso responsable de la tecnología y la información. Presenta diferentes situaciones y actividades para que la clase aprenda sobre el cuidado de sus datos, pueda reconocer enlaces sospechosos y reflexione sobre la importancia de no compartir demasiada información en internet.

Resumen de las sesiones

Sesión 1

Se presenta el concepto de *phishing* como robo de datos e información y se explica por qué puede ser peligroso.

Sesión 2

Se explica qué es la identidad en el contexto de la virtualidad y cuáles son los riesgos de compartir demasiada información o dar clic a enlaces sospechosos.

Sesión 3

Se refuerza lo aprendido en años anteriores con relación al concepto de contraseñas seguras, comparándolas con candados que cuidan la información de las personas. Se presentan recomendaciones de seguridad adicionales para identificar riesgos en internet.

Sesión 4

Se comparan mensajes seguros con mensajes sospechosos y se presentan actividades para identificarlos y decidir qué hacer en diferentes situaciones.

Sesión 5

Se hace un cierre de la sesión recordando los conceptos claves y se propone la creación de una galería para presentar más información sobre el *phishing*.

Grado 5° Guía 4

TIC

Sesión 1

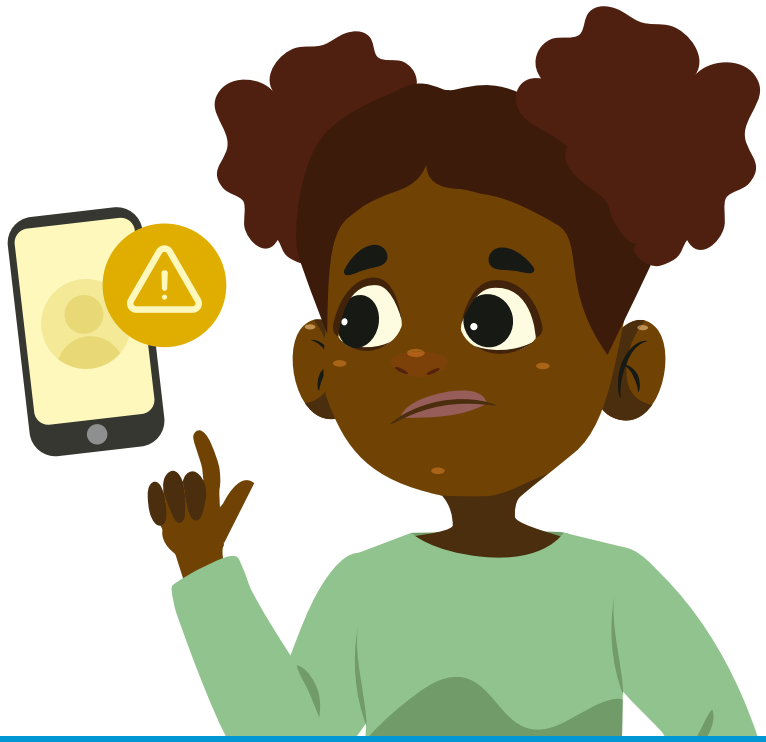
Aprendizajes esperados

Al final de esta sesión se espera que puedas:

- Identificar riesgos asociados a la navegación en internet.
- Reconocer qué es el *phishing* y por qué es peligroso.
- Enunciar algunas características de los mensajes sospechosos.

Duración sugerida

33% 34% 33%



Lo que sabemos, lo que debemos saber

Esta sección corresponde al 33% de avance de la sesión

Observa la *Figura 1.*

Figura 1. Personas sospechosas

¿En qué se coinciden las imágenes anteriores? ¿Qué puedes explicar sobre cada una de esas personas?

Quizás te han llegado a la mente palabras como persona sospechosa, ladrón(a), robar o disfrazado(a).

Enfócate en una de las palabras que necesitas tener en cuenta desde esta primera sesión de clase. La palabra **sospechoso**.

Se considera “sospechoso” a cualquier evento que parezca extraño como, por ejemplo, si una persona desconocida se te acerca y te pregunta tu nombre o información personal o cuando alguien te ofrece un trato que parece demasiado bueno para ser verdad.

¿Por qué crees que las personas de las imágenes anteriores usan antifaz?

Si pensaste que es porque no quieren que los demás se enteren de quienes son en realidad, ¡tienes razón! El antifaz les ayuda a no revelar su verdadera **identidad**.

¿?

¿Cuál o cuáles de los siguientes eventos te parecen sospechosos?

- ○ Que una persona desconocida te ofrezca un dulce o caramelo.
- ○ Que una persona que tú no reconoces te llame por tu nombre.
- ○ Recibir una carta de un desconocido o desconocida invitándote a jugar en el parque o a comer helado.

Trabaja con dos o tres compañeras o compañeros siguiendo las indicaciones de tu docente.

Discutan cuál o cuáles de las situaciones anteriores se podrían considerar sospechosas y porqué.

Figura 2. Pescando

En la *Figura 2* puedes ver a unas personas con una caña de pescar. La usan para atrapar peces. Para hacerlo, solo colocan en el anzuelo algo que atraiga la atención del pez y haga que este se dirija hacia la caña para atraparlo.

Así como se pueden encontrar eventos sospechosos en los lugares que visitas o en donde vives, también pueden ocurrir situaciones que te parezcan extrañas, es decir, sospechosas, cuando tú o personas que conozcas navegan en internet.

Por ejemplo, hay páginas que te envían mensajes con el objetivo de recopilar información que luego pueden usar para hacerte daño. Muchas veces las páginas sospechosas crean mensajes que inician presentando oportunidades que dicen **que ganaste algo, que alguien quiere jugar contigo o que algún amigo o amiga de otro país te quiere conocer, etc.**

A este tipo de prácticas se les conoce con el nombre de ***phishing***, porque lo que quieren esas páginas o personas sospechosas es "pescar" a otras para que caigan en sus trampas y lo hacen **suplantando la identidad** de otra persona o servicio, es decir, al hacerse pasar por alguien o algo más.

El ***phishing*** se ha vuelto una práctica muy común, por lo que es crucial estar alerta ante cualquier situación sospechosa que detectes. Solo de esta manera podrás evitar caer en estas trampas, las cuales seguramente pueden llevarte a enfrentar problemas difíciles de superar.

Glosario

- **Phishing:** técnica utilizada por ciberdelincuentes en internet para engañar a las personas y robar su información personal, como contraseñas o datos bancarios. Lo hacen, haciéndose pasar por otras personas o empresas reales a través de correos electrónicos, mensajes de texto o sitios web falsos.
- **Suplantar la identidad:** es hacerse pasar por otra persona o empresa, normalmente, con la intención de robar información, hacerle daño o buscar beneficios.

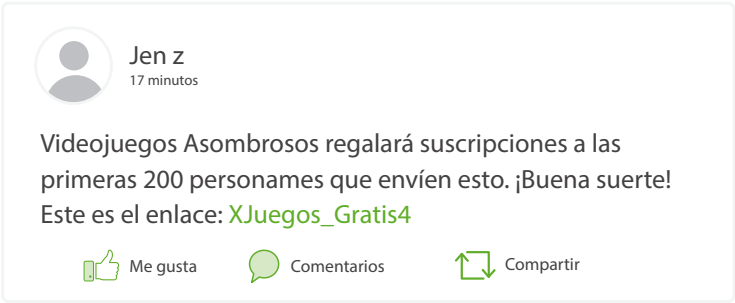
Manos a la obra
Desconectadas

Esta sección corresponde al 67% de avance de la sesión

Trabaja con una compañera o compañero según las indicaciones de tu docente. Lean y analicen la siguiente situación.

El problema

Ana es una niña de 12 años que se queda sola en casa porque su papá y mamá trabajan todo el día en una oficina. Ana tiene un horario diseñado para cuando se quede sola, por lo que siempre de 3:00 p.m. a 5:00 p.m. está conectada jugando en línea con sus amigas y amigos del colegio. Un día, Ana recibe el siguiente mensaje mientras juega por internet:



Ahora discutan sus respuestas a estas preguntas:

¿Qué información consideran del mensaje les parece atractiva y creen que podría llamar la atención de Ana? ¿Por qué?

¿Qué piensan que debería hacer Ana? ¿Por qué?

¿Quién es?

Van a aprender como identificar mensajes o personas que se pueden considerar sospechosas. Para ello van a jugar a ¿Quién es?

Su docente seleccionará en secreto a una persona de la clase. Háganle preguntas para averiguar de quién se trata. Su docente solo podrá responder diciendo sí o no. Pueden usar preguntas como las siguientes:

¿?

¿La persona que escogiste tiene el cabello negro?

¿Es de estatura baja?

¿Le gusta jugar voleibol?

Luego de identificar a la compañera o compañero secreto, respondan:

¿?

¿Cómo lograron saber quién era la persona secreta?

Mencionen algunos "datos" que les permitieron saber de quién se trataba.

Detectives

Así como los datos o pistas del juego para identificar a una persona, los mensajes sospechosos también se pueden reconocer. Por eso, antes de abrir un mensaje que reciba, cada persona debe hacerse estas preguntas:

¿?

¿Conozco a quién me escribe?

¿Algo de lo que me envían me suena extraño?

Con ayuda de tu compañera o compañero, escriban dos preguntas que podrían hacer para identificar si un mensaje es sospechoso. Escriban cada una de sus preguntas en una hoja de papel o en un octavo de cartulina.

Luego reúnanse con otro grupo y comparen sus respuestas. Deben llegar a acuerdos sobre cuáles de las preguntas deberían presentarles al resto de la clase.

Seguidamente, compartan con las demás personas de la clase su(s) pregunta(s) en el tiempo que les indique su docente.

Glosario

Contraseña: es una palabra o combinación de letras, números o símbolos, que se usa como una llave personal para entrar a algún lugar en internet (ej. redes sociales, plataformas de juego, bancos y colegios, etc.).
Una contraseña fuerte también funciona como un candado pues es muy difícil de acceder. Por eso sirve para mantener la información protegida y segura.
También se le llama clave.

Ciberdelincuente: también es llamado "hacker".
Es una persona que se hace pasar por otras o por una empresa con la única intención de conseguir su información privada, por ejemplo, su dirección, su contraseña de redes sociales, el lugar donde estudian o cualquier información privada de algún miembro de su familia.

Antes de irnos

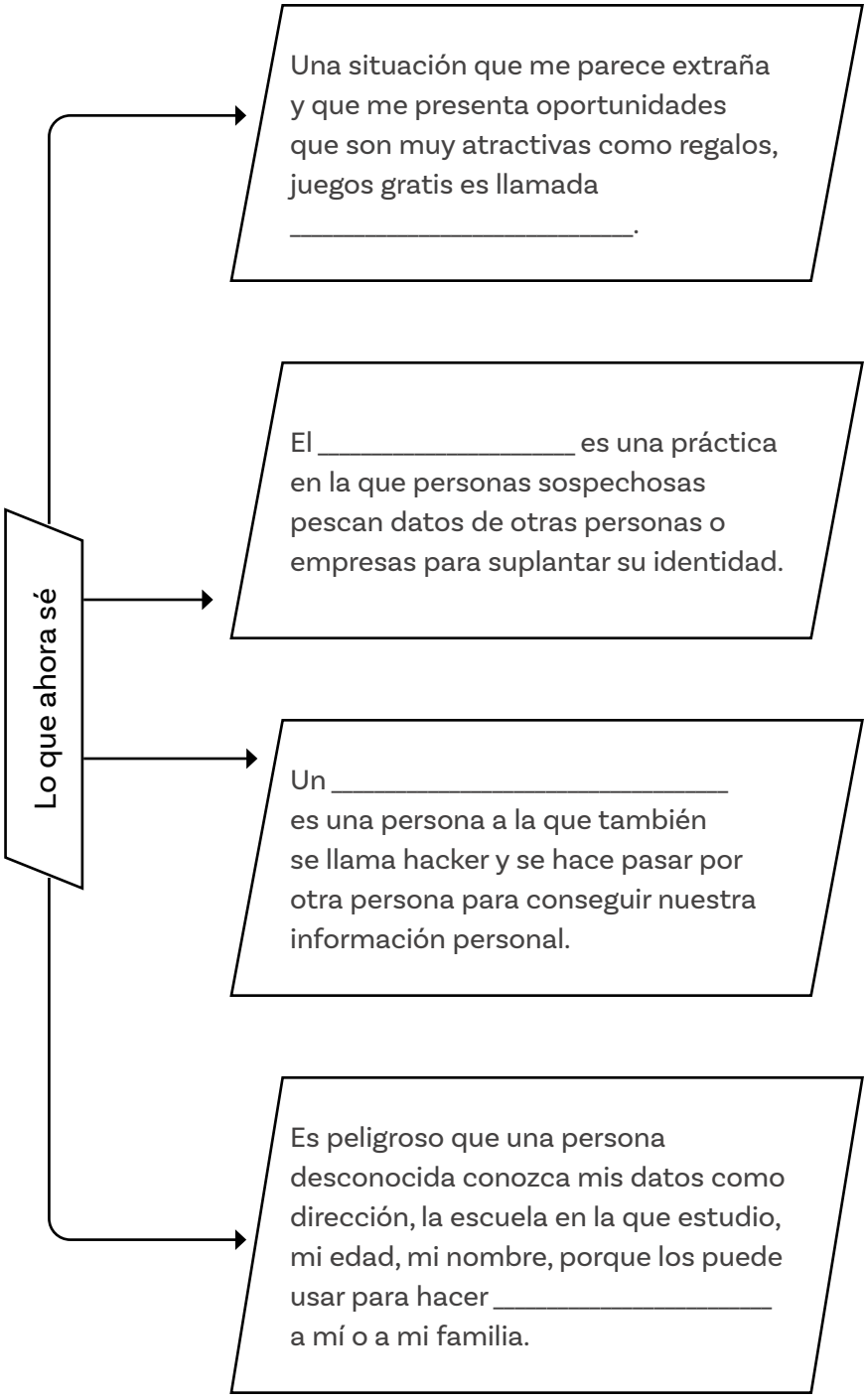
Esta sección corresponde al 100% de avance de la sesión

De forma individual, piensa en las siguientes preguntas.

¿Qué aprendiste sobre phishing y sobre las formas de identificar mensajes sospechosos?

¿Qué podrías hacer para cuidar tu información personal al navegar por internet?

Ahora, completa el recuadro con palabras que hagan falta.



Haz un dibujo que puedas usar para explicarle a tu familia lo que aprendiste en esta sesión. Puedes agregarle algunas palabras si lo consideras necesario.

Revisa los aprendizajes de la sesión. ¿Crees que lograste alcanzarlos?

1. Puedes identificar que existen riesgos asociados a la navegación en internet?

- ◯ Sí
- ◯ Parcialmente
- ◯ Aún no

2. ¿Puedes reconocer qué es el phishing y por qué es peligroso?

- ◯ Sí
- ◯ Parcialmente
- ◯ No

3. ¿Puedes enunciar algunas características de los mensajes sospechosos?

- ◯ Sí
- ◯ Parcialmente
- ◯ No

Si tus respuestas fueron "Parcialmente" o "Aún no", revisa los dibujos hechos por algunas de tus compañeras o compañeros y trata de identificar ejemplos de situaciones o eventos sospechosos al usar internet. Si te quedan dudas sobre este tema, consulta con tu docente.

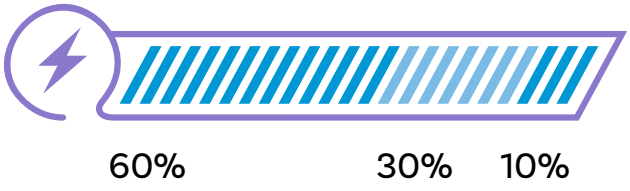
Sesión 2

Aprendizajes esperados

Al final de esta sesión se espera que puedas:

- Explicar qué es el *phishing* y por qué es peligroso.
- Analizar los riesgos de compartir demasiada información y hacer clic en enlaces sospechosos.
- Identificar estrategias para el cuidado de la información personal en internet.

Duración sugerida



Material para la clase

- Anexos 2.1 y 2.2.

Lo que sabemos, lo que debemos saber

Esta sección corresponde al 60% de avance de la sesión

La sesión anterior aprendiste sobre algunos peligros que hay en internet. Como clase, completen la siguiente frase:

Si el mensaje enviado por alguna persona o página te parece sospechoso, tú...

Tu docente irá anotando en el tablero sus respuestas y guiará la conversación para relacionarlo con los aprendizajes de la sesión anterior.

Ahora vamos a aprender más sobre la forma de detectar los mensajes que aparentemente son inocentes, pero resultan ser sospechosos.

Veamos nuevamente las imágenes de la sesión anterior.

¿? *¿Notas diferencias entre las imágenes?* Menciona una.

Seguramente has observado que en una de ellas se muestra el símbolo "$" y representa dinero. En la otra bolsa puede haber dinero, pero también puede contener algo igual de valioso.
Si observas detenidamente la imagen podrás ver que ambas personas llevan antifaz y caminan con pasos largos como si intentaran huir de algo o de alguien.

Figura 1. Tarjeta de identidad

La tarjeta de identidad es el documento de identificación para personas con edades entre los 7 y 17 años.

¿Le darías información sobre el lugar donde vives, tu nombre o cualquier otra información personal a personas que se parezcan a las que muestran las imágenes? ¿Por qué?

En cualquier lugar que estemos, es peligroso dar nuestra información personal a personas desconocidas.

Piensa en lo siguiente

¿Qué cosas materiales tienes que consideras valiosas?

¿Por qué alguien querría robarte esas cosas materiales?

Así como posees cosas materiales que consideras valiosas, también tienes algo que es igual o más valioso que las cosas: ¡Tu **identidad**!

¿Sabes qué es la identidad?
Para ayudarte a saberlo, vamos a recordarte que posees algo que tiene que ver con tu identidad. ¿Lo sabes? Sí, es tu tarjeta de identidad.

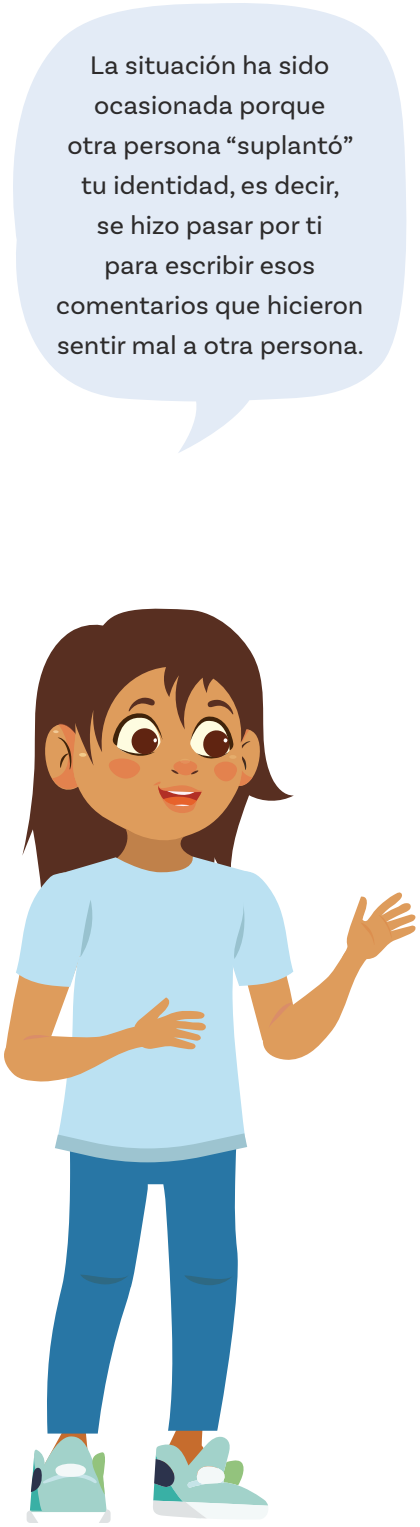
Menciona los datos que tiene tu tarjeta de identidad.

Esos datos personales definen tus características, te describen como una persona única y real. Esos datos son muy valiosos para ti porque no existe nadie más que sea exactamente como tú.

Hay personas como los ciberdelincuentes que quieren robarnos nuestros datos, lo cual pone en peligro nuestra seguridad y la de nuestra familia.

Si alguien tiene alguna información de la que hay en tu tarjeta de identidad, ¿qué haría con esa información?

Figura 2. ¿Qué pudo haber pasado?



Piensa en lo siguiente: ingresaste a un lugar de juegos cerca a tu casa y accediste a tu plataforma de juegos favorita. Resulta que tuviste que irte, se había pasado el tiempo muy rápido y olvidaste cerrar tu sesión ese día. Al día siguiente ingresas desde tu dispositivo en tu casa. Observas que tienes algunos de mensajes de tus compañeras y compañeros de juego que te acusan de hacer comentarios ofensivos a una persona jugadora de esa sala y te dicen que ese niño se sintió muy mal, tanto que decidió retirarse de ese juego y dijo que no volvería.

Pero tú sabes que no hiciste eso. Y entonces piensas, ¿cómo pasó esta situación si ayer que jugué no hablé con nadie? ¿Qué pudo haber pasado? Lee lo que pudo haber pasado en la *Figura 2*.

¿Cómo se sentirá tu compañera o compañero de juegos sobre la situación que vive? Si fueses tú al que ofendieron, ¿cómo te sentirías?

Por eso es muy importante proteger las cuentas de ingreso a cualquier plataforma, incluso en la de juegos.

Al no cerrar las sesiones a las que ingresas con tus datos, alguien puede asumir tu identidad y hacer comentarios ofensivos de alguna persona, como en este caso, y también puede enviar fotografías o videos inadecuados a otras personas.

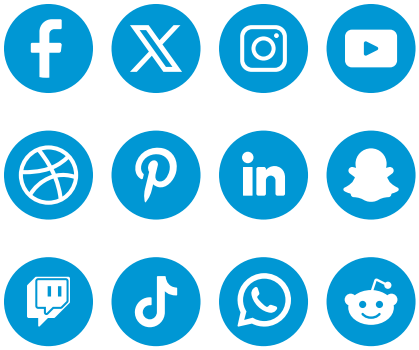
Recuerda que, como aprendiste la sesión anterior, el ***phishing*** consiste en el engaño realizado por un(a) **ciberdelincuente** a otra persona mediante **suplantar su identidad** o la de una empresa real. Esta trampa se realiza a través de métodos que parecen atractivos para que las personas no los detecten tan fácilmente. Veamos algunos ejemplos.

Primero, puede ser que recibas un mensaje que parece provenir de una plataforma que conoces, pero resulta ser de una página diferente que oculta su verdadera identidad, como si esa página tuviera un antifaz para no mostrarse tal cual es. Si no logras detectar que es un mensaje sospechoso, tus datos serán atrapados por el o la ciberdelincuente como lo sugiere la *Figura 3*.

Segundo, cuando ingresas a una red social por primera vez, mucha de la información que está en tu tarjeta de identidad la necesitas para ser parte de esa red social ¿recuerdas qué información te pide para inscribirte?

Figura 3. Phishing

Figura 4. Íconos de aplicaciones



¿Cuáles de los íconos de la Figura 4 *puedes reconocer como aplicaciones que te piden algunos de los datos que aparecen en tu tarjeta de identidad?*

¿En cuál o cuáles de los que puedes reconocer necesitas ingresar tus datos personales?

La *Tabla 1* te muestra los datos que debes ingresar a algunas redes sociales. Léelos atentamente, luego escribe SÍ en caso de que tú o alguna persona de tu familia la usen, o NO en caso contrario.

Tabla 1. Datos en diferentes redes sociales

Red social	Datos que se deben ingresar	¿La usas tú o alguna persona de tu familia?
	No. de identificación_ País donde vives _ Fecha de nacimiento _ Correo electrónico _ Fotos de perfil __ Número de contacto _	
	No. de identificación_ País donde vives _ Fecha de nacimiento _ Correo electrónico _ Fotos de perfil __ Número de contacto _	
	No. de identificación_ País donde vives _ Fecha de nacimiento _ Correo electrónico _ Fotos de perfil __ Número de contacto _	

¿Qué podría hacer alguien si tiene acceso a estos datos?

Puedes pensar en que no sueles entrar a salas de juego en lugares diferentes a las que usualmente ingresas o que lo haces desde tus dispositivos móviles o el de tu madre, padre o personas cuidadoras. Lo que debes saber es que muchas veces los mensajes sospechosos de los que se ha hablado son el anzuelo que usan las y los ciberdelincuentes para atrapar tus datos. Lee con detalle lo siguiente:

En 2004, Mark Zuckerberg fundó una red social considerada "la revolución de las redes sociales": Facebook. Como puedes notar es una de las redes sociales más antigua y es muy famosa.

Si tú o alguna persona que conozcas la usan, deben estar muy alerta porque suele ser la más preferida por las y los ciberdelincuentes. Pueden recibir un correo electrónico o mensaje privado o tal vez puede aparecer una ventana emergente, es decir, otra pequeña ventana anunciando que han ganado un premio o pidiendo que accedan a su cuenta de Facebook para recibirlo. Pero cuando alguien cae en la trampa e introduce su usuario y su contraseña, quienes buscan engañarle tendrán acceso y total control de su cuenta.

Además, alguien que se encuentra en Facebook viendo lo que publican otras personas pudiera recibir un mensaje como el que se muestra en la *Figura 5*:

Figura 5. Phishing en Facebook

¿Qué muestran las flechas y cuadros?

Puedes notar que se muestra un nombre que no está relacionado con Facebook, aunque usa los mismos colores de la página, la forma en que se escribe, el tipo de letra, los logotipos y firmas. Pueden hacerte pensar que los mensajes son originales.

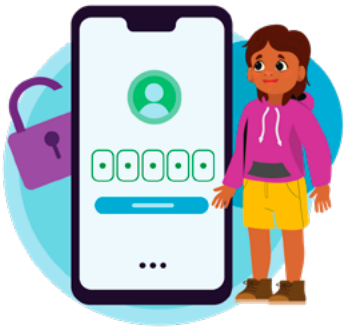
Esto no solo ocurre con Facebook, puede ocurrir en cualquier otra red social como, por ejemplo: Instagram, X, WhatsApp, Twitch y Snapchat.

Glosario

Identidad: conjunto de características, valores y creencias que definen a una persona y la distinguen de los demás. En el contexto digital, se refiere a la representación de una persona en línea, lo que puede incluir su nombre, fotos, perfiles en redes sociales y otra información personal.

Nota

Para proteger los datos personales se usan las contraseñas, por eso es clave que sean seguras. En las próximas sesiones recordarás un poco lo que ya has aprendido sobre la creación de contraseñas seguras.



Anexo

Anexo 2.1

PRIVADO	CONTRASEÑA	IDENTIDAD
CONOCIDO	AUTÉNTICO	PELIGRO
ENGAÑO	TRAMPA	SEGURIDAD

Manos a la obra

Desconectadas

Esta sección corresponde al 90% de avance de la sesión

Adivina la palabra

Recorta las tarjetas del *Anexo 2.1*. Organiza un equipo de cuatro personas según las indicaciones de tu docente.

Un integrante de tu equipo tendrá que pasar al frente cuando les corresponda su turno y describir la palabra secreta de la tarjeta sin decirla. El reto está en que debe explicar la palabra de la carta sin decirla para que su grupo obtenga el punto. Cada equipo contará con 1 minuto para identificar las palabras que se relacionan con el *phishing*. Gana el equipo que obtenga más puntos.

Detectar el phishing

Con esta actividad tú y tus compañeras y compañeros de equipo aprenderán a reconocer maneras de protegerse y evitar ser víctimas del *phishing*.

La *Figura 6* presenta afirmaciones sobre lo que estás aprendiendo. Cada afirmación corresponde a una de las dos palabras que se muestran en los recuadros superiores.

¡A jugar!

Figura 6. Juego Detectar el Phishing

Permiso **Contraseña**

Palabra secreta que ayuda a proteger nuestros datos

Desconocidas **Conocidas**

Solo podemos aceptar solicitudes de estas personas

Mensajes **Advertencia**

Tipo de “anzuelo” que usan los hackers para robar nuestros datos

Enlace

También puedes jugar a descubrir la palabra secreta ingresando en línea a:

Ahora, con tus compañeras y compañeros de grupo, escriban una pregunta similar a la que se presenta en la actividad anterior, que ustedes consideran se debe incluir para ayudar a otras personas a estar más informadas sobre el *phishing*.

¿Le creo o no le creo?
Observen la la *Figura 7*.

Figura 7. Mensaje sospechoso

Si están navegando en TikTok y les llega esta notificación, ¿le darán clic o no? ¿Por qué? ¿Qué les parece “sospechoso” en este mensaje?

Anexo

Anexo 2.2

Antes de irnos

Esta sección corresponde al 100% de avance de la sesión

Revisa de forma individual los aprendizajes de la sesión y determina el grado al que los alcanzaste.

1. ¿Puedes explicar qué es el *phishing*?

   - ◯ Sí
   - ◯ Parcialmente
   - ◯ Aún no

2. ¿Analizaste los riesgos de compartir demasiada información y hacer clic en enlaces sospechosos?

   - ◯ Sí
   - ◯ Parcialmente
   - ◯ No

3. ¿Has identificado algunas estrategias para el cuidado de la información personal en internet?

   - ◯ Sí
   - ◯ Parcialmente
   - ◯ No

> **Si tus respuestas fueron "Parcialmente" o "Aún no" o si sientes que todavía tienes alguna dificultad para comprender algo de este tema, conversa con tu docente para guiarte en la manera como puedes superarla.**

Ahora responde las preguntas del *Anexo 2.2*. Luego, recorta los boletos de salida de la clase. Debes responder cada pregunta seleccionando la opción que consideres debe realizarse según lo que has aprendido en esta sesión.

Sesión 3

Aprendizajes esperados

Al final de esta sesión se espera que puedas:

- Aplicar reglas de seguridad para la creación de contraseñas fuertes.
- Identificar actividades sospechosas en línea que pueden poner en peligro los datos personales.

Duración sugerida

15% 70% 15%

Material para la clase

- Anexo 3.1.

Lo que sabemos, lo que debemos saber

Esta sección corresponde al 15% de avance de la sesión

Empieza por recordar lo que aprendiste en la sesión anterior. ¡Vas a jugar a las adivinanzas! Trata de descubrir la palabra secreta en cada caso.

- Soy lo que te hace una persona única, tu esencia y tu ser. Todas las personas tienen una, pero solo yo te conozco bien. ¿Quién soy?

- Soy un secreto bien guardado, una combinación misteriosa. Sin mí, no puedes entrar, pero si me olvidas, ¡qué desastre! ¿Qué soy?

- Soy una sombra que se esconde. Todas las personas me miran con recelo, pero solo algunas descubren mi verdadero juego. ¿Quién soy?

Recuerda que cuidar tu información personal es igual de importante que cuidar tus pertenencias.

Tu docente puede ayudarte a verificar las respuestas.

Hasta ahora has podido reconocer algunas maneras en que las y los ciberdelincuentes envían mensajes para robar los datos privados. Recuerda que cuidar tus datos ayuda también a cuidarte, porque esos datos privados revelan quién eres, dónde estás y otra información que, en manos equivocadas, puede ser usada para hacerte daño.

Seguirás aprendiendo sobre identificación de estrategias que te ayuden a cuidar la información personal.

¿? *¿Qué se muestra en las imágenes de la* Figura 1*?*

Figura 1. Asegurar lugares y/o pertenencias

Las acciones que muestran las imágenes se relacionan con el hecho de asegurar lugares y/o pertenencias. Seguramente habrás notado que tus familiares realizan estas acciones o por lo menos una de ellas. Como quizás aprendiste en grados en anteriores, una práctica común para asegurar sitios es el uso de candados. Por eso hoy recordarás sobre candados y llaves que te ayudan a cuidar la información personal.

Como sabes, un candado es un dispositivo que se usa para proteger cosas que se consideran valiosas. También se usan para guardar información privada. Los candados ofrecen seguridad para navegar de manera que puedas acceder a tus redes y juegos. Pero recuerda que ni aun así puedes bajar la alerta sobre el *phishing*. Hay programas que reconocen esos candados y pueden engañarte para que los abras.

Al crear tus contraseñas es como si elaboraras tus propios candados para mantener protegidos tus datos. Mientras más fuerte sea un candado, mayor seguridad ofrece. En el mismo sentido, mientras más fuerte sea tu contraseña, más segura será.

Recuerda que si alguien tiene acceso a tus datos puede ingresar a tus redes o plataformas de juego. Por eso es importante crear contraseñas seguras.

Manos a la obra
Desconectadas

Esta sección corresponde al 85% de avance de la sesión

Actividad 1: ¡Vamos a crear nuestros candados!

¿Cuáles consideras que son las características que puede tener una contraseña? ¿Por qué?

Vas a crear una contraseña débil con las siguientes reglas:

- Debe tener letras o números secuenciales (ejemplo: abc, 123).
- Debe tener menos de 8 caracteres.
- Puedes usar el nombre de tu mascota, nombrar algo te gusta mucho o incluso puedes usar tu nombre.

Toma unos minutos para crear tu contraseña. Comparte con tus compañeras y compañeros tu creación y, luego, comparen sus ideas de contraseñas.

¿En qué se parecen? ¿Cuáles pistas puedes identificar en la creación de esas contraseñas?

Las contraseñas construidas con esas pistas pueden ser débiles porque alguna persona que vea tu perfil en las redes sociales puede identificar tus gustos, ver tu nombre y si tienes fotos con tu mascota y has colocado su nombre, tiene mucha información sobre ti. Si tu contraseña tiene estos datos seguramente será fácil para un(a) ciberdelincuente copiar tu contraseña y acceder a tus redes o cuentas de juego.

¿Ves lo importante que es crear una contraseña fuerte? Esta debería ser como un candado muy difícil de abrir.

A continuación recordarás las reglas para crear candados fuertes. Lee con detalle las siguientes instrucciones para crear tu contraseña:

- Debe tener entre 8 y 10 caracteres.
- De incluir una letra minúscula y una mayúscula.
- Debe incluir números que no sean consecutivos, es decir, aquellos que siguen a continuación del otro (1,2,3).
- Debe contener por lo menos un cero.
- Debe incluir uno o dos de los siguientes caracteres: *, -, ¡, +.

¡Ahora sí, crea tu contraseña!

Otra forma de hacer contraseñas seguras, pero más fáciles de recordar, es usando frases contraseña. Estas son combinaciones de palabras o frases que forman una contraseña más larga y segura. Observa los siguientes ejemplos

MiGatoEsNegro123!
Amo Leer Telenovelas?
lápiZ rosadO postE dE luZ

Instrucciones para crear tu frase contraseña:

- Piensa en una frase que te guste o que te sea fácil de recordar, como una línea de tu canción favorita o una actividad que disfrutes. O simplemente une palabras al alzar con alguna modificación.
- Combina palabras, números y caracteres especiales para hacerla más segura. Por ejemplo, puedes reemplazar letras por números (como la “o” por “0”) o agregar signos de exclamación.
- Asegúrate de que tu frase contraseña tenga al menos 12 caracteres para que sea más fuerte.

Ahora es tu turno: crea tu propia frase contraseña. Después compártela con una compañera o compañero y reflexionen juntos sobre la seguridad de sus contraseñas. ¿Cuál es más fácil de recordar? ¿Cuál es más difícil de adivinar?

Anexo

Anexo 3.1

Una vez toda la clase haya terminado, tu docente pedirá que compartan sus frases contraseña con las demás personas. Observa y escucha atentamente para que les ayudes a evaluar qué tan fuertes son sus contraseñas.

Actividad 2: Aprender a decidir

Para la siguiente actividad trabaja con otra compañera o compañero.

Lean las actividades que aparecen listadas en el *Anexo 3.1* y verifiquen qué información personal podrían estar dando si deciden dar clic en los enlaces o contestar. ¿Cuáles deberían evitar en el futuro?

En el anexo también hay una columna adicional que se titula ¿Darás clic?

Deben escribir SÍ o NO y explicar la razón.

Ahora sigan las indicaciones de su docente para compartir lo que decidieron y discutir sobre los riesgos de cada actividad.

Antes de irnos

Esta sección corresponde al 100% de avance de la sesión

Trabaja con una compañera o compañero para crear una copla (una frase de tres o cuatro versos) que destaque algo de lo que has aprendido en cuanto a la protección de los datos personales en internet. Escriban su propuesta aquí.

Sigan las instrucciones de su docente para compartir sus coplas.

Revisa los aprendizajes de la sesión. ¿Crees que lograste alcanzarlos?

1. ¿Puedes aplicar reglas de seguridad para la creación de contraseñas fuertes?

   - ◯ Sí
   - ◯ Parcialmente
   - ◯ Aún no

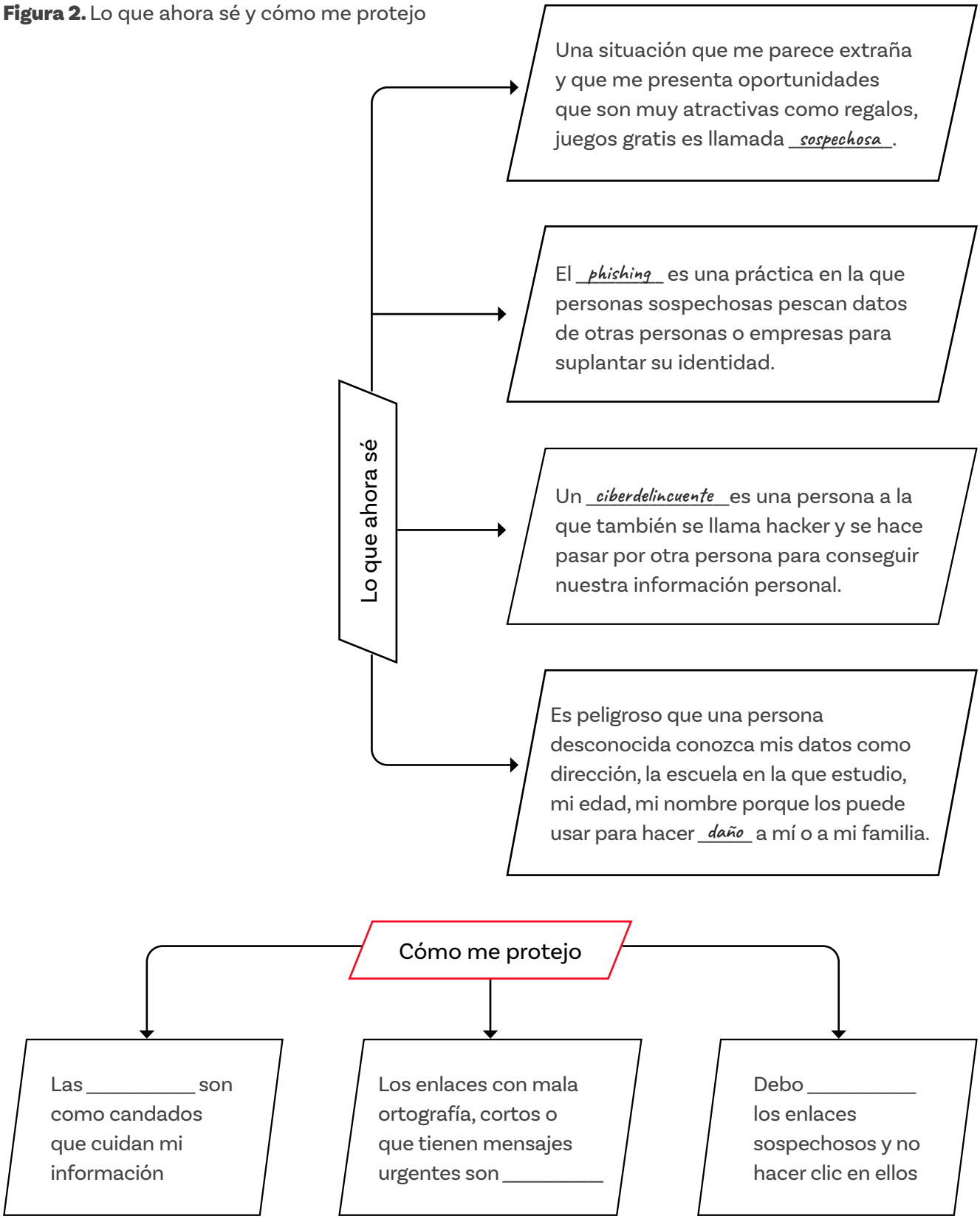
2. ¿Puedes identificar actividades sospechosas en línea que pueden poner en peligro tus datos personales?

   - ◯ Sí
   - ◯ Parcialmente
   - ◯ No

No dudes en consultar a tu docente si todavía tienes alguna inquietud sobre este tema.

Finalmente, completa el esquema en la *Figura 2* con las ideas que has aprendido en las sesiones que se han abordado hasta ahora.

Figura 2. Lo que ahora sé y cómo me protejo



Sesión 4

Aprendizajes esperados

Al final de esta sesión se espera que puedas:

- Usar claves de los mensajes para identificar ejemplos de *phishing*.
- Implementar estrategias para cuidar la información personal y la identidad.

Material para la clase

- Anexo 4.1.

Duración sugerida

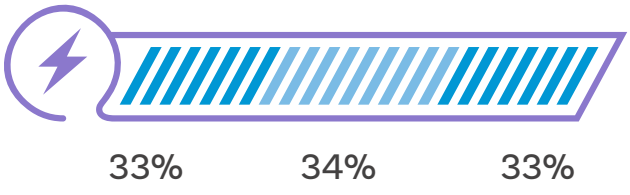


Figura 1. Mensaje de texto sospechoso

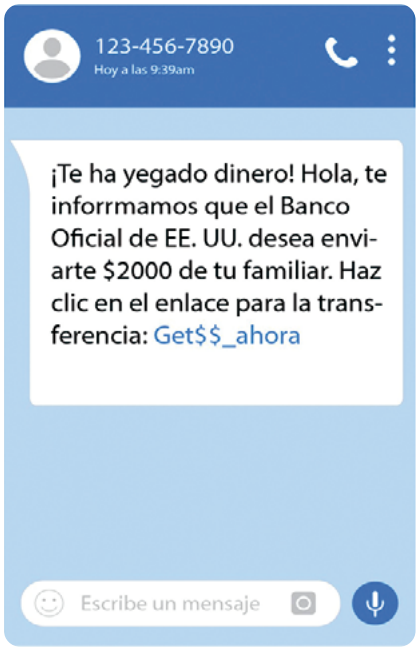


Figura 2. Pistas del phishing

Lo que sabemos, lo que debemos saber

Esta sección corresponde al 33% de avance de la sesión

Ya has avanzado en identificar maneras en las que puedes ser víctima de engaño y en reconocer mensajes que se pueden considerar sospechosos.

Ahora vas a seguir aprendiendo sobre otras maneras que usan las y los ciberdelincuentes para robar la identidad de las personas.

Observa con detalle la *Figura 1*:

¿Qué te parece sospechoso en el texto?

Algunos mensajes están diseñados para tener aspecto de confiables y legítimos, pero su objetivo es siempre el mismo: lograr extraer información personal.

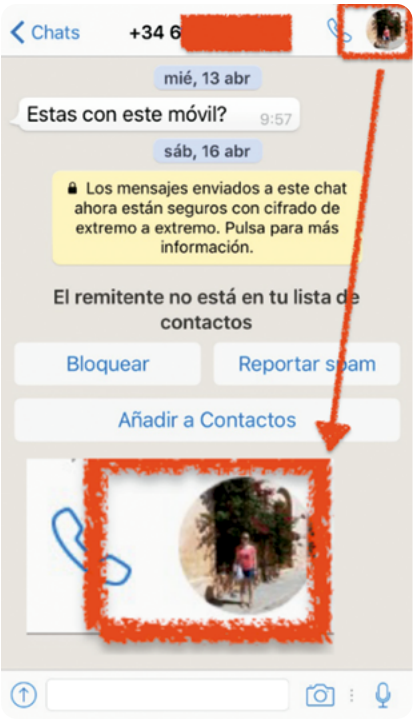
Cuando recibas algún mensaje busca señales como faltas de ortografía, lenguaje poco conocido o incorrecto o errores gramaticales muy obvios, tales como el uso incorrecto de palabras en singular y plural y el uso de figuras sobre las letras.

También pueden encontrarse páginas de internet falsas con apariencia de plataformas muy conocidas.

Para detectar las pistas del *phishing*, observa detalladamente la *Figura 2*.

- ○ Te envían un enlace abreviado.
- ○ Te ofrecen algo demasiado bueno para ser verdad.
- ○ Te piden que compartas algo.

Figura 3. Mensaje sospechoso de WhatsApp



¿Qué otras pistas puedes mencionar que te indiquen que el sitio al que te piden entrar es sospechoso? Discute lo que piensas con una compañera o compañero.

Glosario

URL: es la dirección de una página web o un recurso en internet. Su nombre viene de las siglas de las palabras en inglés Uniform Resource Locator que (localizador de recursos uniforme). La URL de páginas web normalmente inicia con las letras http.

Manos a la obra
Desconectadas

Esta sección corresponde al 67% de avance de la sesión

A continuación vas a analizar un nuevo caso. Lee detenidamente:

A tu padre, madre o cuidador(a) le ha llegado a WhatsApp, la aplicación de mensajería instantánea que utiliza, el mensaje que se muestra en la *Figura 3* y decide mostrártelo porque le pareció un poco raro. Tú miras el mensaje atentamente para encontrar posibles señales de que pueda ser falso.

¿Qué pistas te pueden indicar que este mensaje es sospechoso?

¿Qué te indican las flechas y el cuadro?

Responde las preguntas anteriores de forma individual. Luego discute tus respuestas con otras dos o tres personas, siguiendo las instrucciones de tu docente. Como grupo decidan lo que responderían. Después decidan su respuesta a la siguiente pregunta:

Anexo

Anexo 4.1

¿Qué le aconsejarían a la persona que les mostró el mensaje que había recibido?

Podrían, por ejemplo, hacerle una pregunta como esta:

¿Este mensaje te lo envió alguna persona que conoces?

En resumen

Responde Sí o No en la *Tabla 1* según corresponda.

Tabla 1. ¿Deberías abrir el mensaje?

Si el mensaje que recibes...	**¿Deberías abrirlo?**	
	SÍ	NO
Te pide actuar con urgencia		
Tiene errores de ortografía y gramática		
Contiene un enlace abreviado para acceder a otra dirección **URL**		
Le falta el saludo o es un saludo genérico		
Te pide que compartas algo		
Tiene un mensaje de ¡Alerta! ¡Alerta!		

Antes de irnos

Esta sección corresponde al 100% de avance de la sesión

Ahora, siguiendo la dirección de tu docente, van a jugar un juego de atención.

Tu docente dirá algunas afirmaciones que tú y las demás personas de tu clase deberán analizar. Si creen que son verdaderas deben ponerse de pie y si creen que son falsas deben quedarse en sus asientos. Si no están seguros de la respuesta, pueden levantar sus dos manos.

Las frases que use tu docente en el juego pueden ser las siguientes o parecerse a estas:

a. Los mensajes sospechosos podrían llegar desde números telefónicos de personas desconocidas.

b. Un mensaje que te indique que has ganado una lotería o un premio para el que no te has inscrito puede ser un mensaje de *phishing*.

c. Si alguna persona que conoces recibe un mensaje de alguien que afirma ser una amiga o un amigo que hace tiempo no ve y que necesita su ayuda urgente, deberías recomendarle que sospeche del mensaje recibido.

d. Si al navegar por internet se abre alguna pequeña ventana con un enlace que promete que podrás descargar juegos de forma gratuita, debes considerarlo sospechoso.

Es momento de hacer un último trabajo en grupo. En compañía de otras dos o tres personas, según lo que te indique tu docente, van a elaborar un friso[1] con recomendaciones para reconocer sitios que contienen enlaces o direcciones URL poco confiables. Para elaborarlo pueden recortar y utilizar las frases y ejemplos del *Anexo 4.1*. Parte de su friso podría verse como el ejemplo en la *Figura 4*:

Figura 4. Ejemplo de friso

Compartan su friso, siguiendo las instrucciones de su docente.

1. Un friso es un organizador gráfico tipo acordeón y sirve para exponer e ilustrar un tema.

Revisa los aprendizajes de la sesión. ¿Crees que lograste alcanzarlos?

1. ¿Puedes usar claves de los mensajes para identificar ejemplos de *phishing*?

- ◯ Sí
- ◯ Parcialmente
- ◯ Aún no

2. ¿Puedes implementar estrategias para cuidar tu información personal y tu identidad?

- ◯ Sí
- ◯ Parcialmente
- ◯ Aún no

Grado 5° **Guía 4**

TIC

Sesión 5

Aprendizajes esperados

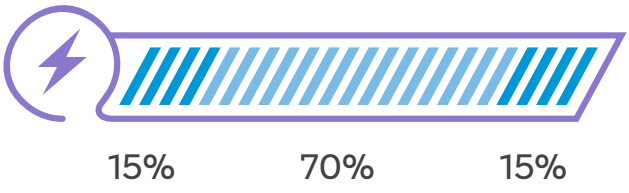
Al final de esta sesión se espera que puedas:

- Reforzar la aplicación de estrategias de seguridad digital para el autocuidado de los datos y la identidad.
- Utilizar lo aprendido sobre el *phishing* y los peligros que este representa para persuadir a otras personas a que incrementen sus medidas de seguridad digital.

Material para la clase

- Computador con acceso a internet.

Duración sugerida



15% 70% 15%

Lo que sabemos, lo que debemos saber

Esta sección corresponde al 15% de avance de la sesión

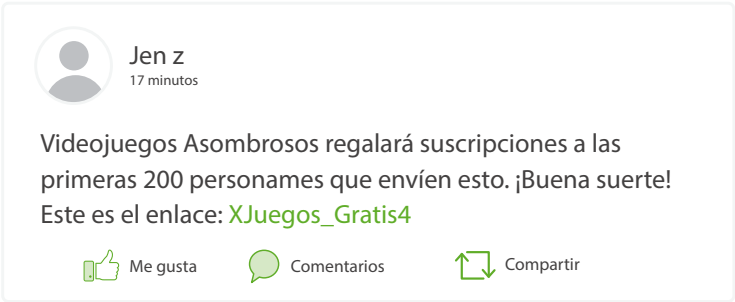
Antes de comenzar, revisemos los gráficos de anclaje o memorias colectivas que se han realizado hasta ahora. También puedes verificar tus apuntes, si los tienes. ¿Qué has aprendido hasta el momento? ¿Tienes alguna pregunta? Comenta con tus compañeras, compañeros y tu docente lo que más te ha llamado la atención de esta guía.

Hasta el momento has aprendido sobre el *phishing* y los riesgos de compartir demasiada información en internet. También has aprendido que algunos enlaces pueden ser sospechosos y has descubierto que hay personas que pueden suplantar tu identidad.

¿Recuerdas a Ana, la niña de la Sesión 1?
Reúnete con otras tres personas, siguiendo las recomendaciones de su docente y lean nuevamente su caso:

Ana es una niña de 12 años que se queda sola en casa porque su mamá y su papá trabajan todo el día en una oficina. Ana tiene un horario diseñado para cuando se queda sola, por lo que siempre de 3:00 p.m. a 5:00 p.m. está conectada jugando en línea con sus amigas y amigos del colegio. Un día, Ana recibe el mensaje que aparece en la *Figura 1* mientras juega.

Figura 1. Mensaje sospechoso



Como grupo, discutan sus respuestas a estas preguntas:

¿?

¿Qué piensan que debería hacer Ana? ¿Por qué?

¿Cómo le ayudarían a Ana a resolver la situación?

De forma individual escriban en sus cuadernos las pistas que pudieran darle a Ana para que ella aprenda a identificar los mensajes sospechosos y, de esa forma, pueda decidir si debe abrir o no mensajes como el que recibió. También escriban las pistas de alerta que han identificado en el mensaje que ella recibió.

Luego, como grupo, compartan sus opiniones y complementen sus ideas. Finalmente, preparen una breve dramatización en la que le dan sus consejos a Ana. (Si en su grupo no hay ninguna niña que pueda hacer el papel de Ana, imaginen que el personaje de la situación es un niño llamado Yeison).

Cuando su docente lo indique, cada grupo presentará sus dramatizaciones. Mientras otros grupos se presentan, vayan marcando un signo de verificación o chulo (✓) en las recomendaciones que mencionen y que ustedes tengan en sus notas. Al finalizar, su docente preguntará por los elementos comunes en las presentaciones que lograron identificar.

Manos a la obra

Desconectadas

Esta sección corresponde al 85% de avance de la sesión

De forma individual soluciona la siguiente sopa de letras encerrando en un círculo las palabras que identificas sobre el tema estudiado durante las sesiones anteriores.

R O B D E S M A R I T A N Z U E L O

A M R I D E N T I D A D A S A R M E

P R I V A C I D A D T E G R Q E W R

I N T E M C I B E R D E L I T O J N

R F U A E A D R F O C A R T U I O Y

O D A Ñ N E C V A Ñ E S A R T N O C

B A B U A X Y O P A F T U V N I R A

O T S F Z P H I S H I N G G B O L D

Z O I M A S Y T Q O H A C K E R N J

Compara tus respuestas con las de otra compañera o compañero.

¿Encontraron el mismo número de palabras?

¿Recuerdan qué significan o hay alguna palabra que todavía les cueste reconocer?

Ahora resuelvan el crucigrama que aparece en esta página. Tengan en cuenta estas pistas:

HORIZONTALES

1. Técnica de engaño utilizada por ciberdelincuentes para obtener información confidencial como contraseñas o datos personales.

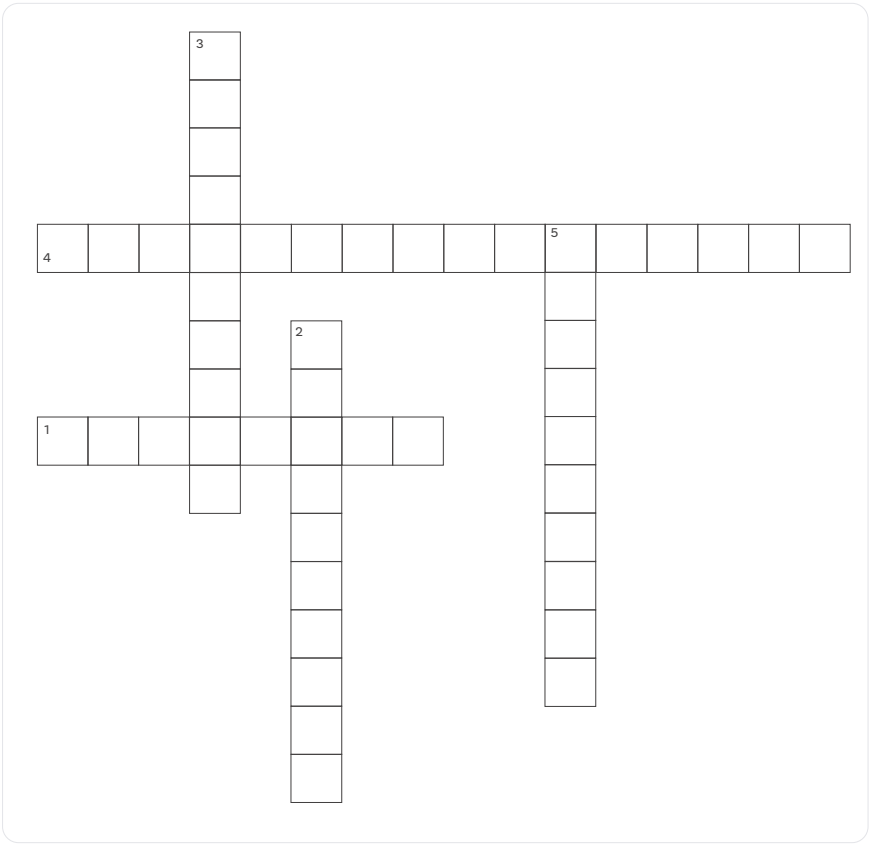
4. Persona que comete delitos en línea como el robo de identidad o el fraude.

VERTICALES

2. Derecho fundamental a controlar quién tiene acceso a nuestra información personal.

3. Algo o alguien que genera dudas.

5. Secuencia de caracteres utilizada para autenticarse en sistemas o cuentas.



Ir a Kiddle

Haz clic sobre el código QR o escanéalo para ir a Kiddle.

Escuela de Influenciadores

Haz clic sobre el código QR o escanéalo para conocer el Kit de Herramientas para el uso seguro, responsable y creativo de internet.

Manos a la obra Conectadas

Esta sección corresponde al 85% de avance de la sesión

Siguiendo las instrucciones de tu docente, tú y tus compañeras y compañeros de grupo ahora deberán preparar una exposición sobre el *phishing*. En la página web de Kiddle hay mucha información interesante que pueden consultar. Su docente le asignará a su grupo una sección de esta página para que la lean y resuman la información para presentarla al resto del salón. En la página web hay información sobre:

- Técnicas de *phishing*
- Fases del *phishing*
- Daños que causa

Si tienen alguna duda sobre palabras desconocidas que encuentren al leer el texto que les asignaron, no duden en preguntarle a su docente.

Cuando hayan terminado de leer y discutir como grupo lo que entendieron del fragmento de la página que estaban consultando, hagan un miniposter en cartulina explicando de forma gráfica y creativa lo que aprendieron. ¡Dejen volar su imaginación!

Para ir más lejos

Visita el recurso enlazado en el código QR de “Escuela de Influenciadores” para seguir aprendiendo sobre seguridad en línea.

Antes de irnos

Esta sección corresponde al 100% de avance de la sesión

Siguiendo las indicaciones de su docente, peguen sus miniposters en la pared para que los otros grupos los vean, como si fuera una galería.

Después de que hayan revisado todos los miniposters, su docente les invitará a comentar lo nuevo que hayan descubierto y también lo que les haya sorprendido sobre la información presentada.

Si, a partir de lo que aprendiste en esta guía, hay alguna acción preventiva que sientes que tienes que implementar para fortalecer aún más la seguridad de tus datos y tu identidad, anótala aquí.

La seguridad de mis datos e identidad es mi compromiso personal

Desde hoy cuidaré mejor de mis datos e información así:

- ○ _____
- ○ _____
- ○ _____
- ○ _____
- ○ _____

Revisa los aprendizajes de la sesión. ¿Crees que lograste alcanzarlos?

1. ¿Puedes explicar qué es el *phishing* y qué impacto puede tener en tu vida?

   - ◯ Sí
   - ◯ Parcialmente
   - ◯ Aún no

2. ¿Puedes identificar las características de los mensajes sospechosos?

   - ◯ Sí
   - ◯ Parcialmente
   - ◯ Aún no

3. ¿Puedes implementar algunas prácticas que te ayudan a estar seguro?

   - ◯ Sí
   - ◯ Parcialmente
   - ◯ Aún no

Anexo 2.1 Tarjetas

Privado	**Contraseña**	**Identidad**
Conocido	**Auténtico**	**Peligro**
Engaño	**Trampa**	**Seguridad**

Anexo 2.2 Boletos de salida

Dana ve un concurso en línea. ¡Podría ganarse $10.000! Ella escribe su nombre y correo electrónico en la solicitud. También le piden su apodo, los nombres de sus mascotas y el apellido de soltera de su madre. ¿Debe Dana dar esa información?

A Sí, debe hacerlo. Las preguntas son tontas, ¡pero vale la pena hacerlo para ganar $10.000!

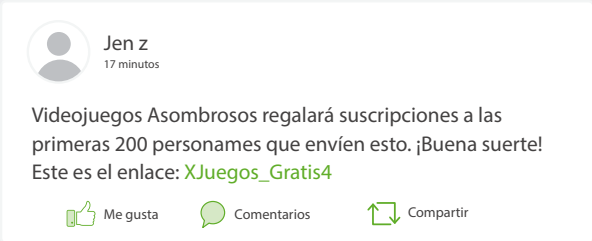
B ¡No debe hacerlo! Los que roban identidades usan esas "pistas" para descubrir contraseñas.

Tu amigo Luis recibe una alerta de Facebook. Debido a las nuevas medidas de seguridad, debe enviar su número de identidad de inmediato o se borrarán todas sus fotos. Él sabe dónde guarda su madre la tarjeta de identidad. ¿Debe hacerlo?

A Sí, debe hacerlo. Es una alerta oficial de una empresa y si espera podría perderlo todo.

B ¡No debe hacerlo! Las empresas serias no hacen eso. Los ladrones usan esa información para crear identidades falsas.

Te ha llegado este mensaje mientras estás en la red social Snapchat.



¿Debes dar clic en el enlace?

A Sí, porque no me están pidiendo ningún dato personal. Solo me piden que entre al enlace.

B No, porque al ingresar a un enlace desconocido también pueden robar mis datos, hasta mis contraseñas.

Anexo 3.1 ¿Cuáles de estas actividades deberías evitar en el futuro?

ACTIVIDADES	EJEMPLO	¿Le darás clic?
Rellenar encuestas en línea que ofrecen regalos	¡Responda algunas preguntas para obtener una tarjeta de regalo de $250!	
Completar un cuestionario de personalidad en línea	"¡Completa este breve cuestionario para averiguar en qué casa de Hogwarts estarías!"	
Mensajería por Snapchat		
Hacer clic en un enlace por correo electrónico de una empresa (o algo que parece venir de una empresa)	"Su cuenta ha sido hackeada". **¡Haga clic aquí para ingresar su contraseña!**	
Mensajería en el chat de la sala de juegos	¡Hola! Quiero ser tu nueva amiga. Tengo un juego que te va a encantar. Ven y juega conmigo en sta.Ves.mariana.ev@es.	
Me escribe una persona de la clase por messenger	Hola, amigo ¿Me puedes prestar tu tarea? Hoy no estuve en la escuela.	

Anexo 4.1 Material para elaborar el friso o plegable

https://www.googlee.cam

https://snip.li/EMOTIC0N

https://www.fäcëböök.com

https://sede.inap.gob.es

Página segura porque...

Página NO segura porque...

TIC

Apoya:

Educación

BRITISH COUNCIL

Colombia Programa
{EL CÓDIGO A TU FUTURO}