

Contraseñas

Los participantes aprenderán cómo proteger mejor su información en internet mediante el uso y conservación de contraseñas seguras. Conocerán las bases para diseñar contraseñas seguras y los posibles problemas de compartirlas, así como la forma de mantener sus contraseñas seguras y qué pasos tomar para evitar el acceso no autorizado a sus cuentas.

Materiales

Guía de aprendizaje sobre las contraseñas

Aspectos básicos de las contraseñas

Primera parte

Explica a los alumnos

En general, no pensamos mucho en las contraseñas que usamos para sitios web, aplicaciones y servicios. Sin embargo, el grado de seguridad de sus contraseñas determina qué tan protegida estará su información.

Interacción grupal

Invita a los participantes a entablar un debate a partir de las siguientes preguntas. Recuérdales que es importante que no compartan sus contraseñas reales durante este y todos los ejercicios.

Pregunta a los alumnos

¿Cuántas contraseñas tienen?

¿Tienen contraseñas diferentes para cada una de las cuentas de correo electrónico y medios sociales?

¿Son muy diferentes o son variaciones de una misma contraseña?

Si tienen más de una contraseña, ¿cómo recuerdan qué contraseña pertenece a cada cuenta?

Pregunta a los alumnos

¿Con qué frecuencia olvidan una contraseña importante?

¿Qué hicieron cuando olvidaron una contraseña?

¿Cómo logran que las contraseñas sean fáciles de recordar?

¿Hay alguna contraseña que usen a diario?

¿Qué pasaría si —sin saberlo— alguien averigua su contraseña?

¿Dependería de quién fuera?

¿Qué tipo de información podría alguien obtener sobre ustedes si usara su

contraseña para entrar a su cuenta?

Segunda parte

Interacción grupal

Organiza a los participantes en parejas.

Explica a los alumnos

Analicen con su compañero qué podría pasar si alguien que quisiera causar problemas obtuviera la contraseña de la cuenta de su plataforma de medios sociales favorita.

Interacción grupal

Concede a los participantes cinco minutos para debatir y luego pide a los grupos que compartan sus ideas.

Explica a los alumnos

Ahora, conversen con su compañero sobre lo que pasaría si un hacker descubriera la contraseña de la cuenta bancaria en internet de su padre o cuidador.

Interacción grupal

Concede a los participantes cinco minutos para debatir. A continuación, pide a los grupos que compartan lo que hablaron.

Tercera parte

Explica a los alumnos

Tal vez se pregunten cómo puede un hacker obtener una contraseña privada. Hay varias formas. Una es mediante la ingeniería social, es decir, engañando a alguien para que comparta su contraseña. Para lograrlo, un hacker puede enviar un correo electrónico que parezca que realmente proviene de la plataforma o del sitio web donde la persona tiene una cuenta. En el mensaje, puede pedirle a la persona que haga clic en un enlace e inicie sesión con su nombre y contraseña. Si la persona inicia sesión, dicha información estará a disposición del hacker.

A veces, los hackers intentan adivinar sus contraseñas con frases habituales como "contraseña123", "prueba" o su nombre o apellido.

Otro recurso que usan los hackers para descubrir una contraseña privada se conoce como "ataque por fuerza bruta". Un ataque por fuerza bruta ocurre cuando un

hacker intenta iniciar sesión en su cuenta probando contraseñas diferentes repetidamente. Si bien un hacker puede llevar a cabo un ataque por fuerza bruta manualmente, este se suele llevar a cabo mediante un programa informático que prueba rápida y automáticamente cada posible combinación de contraseña que puede concebir. Por ejemplo, puede probar una lista de posibles contraseñas o un conjunto de contraseñas que consisten en combinaciones de diferentes letras y números, hasta encontrar la correcta.

Por supuesto, hay ataques por fuerza bruta que son más sofisticados. Si su contraseña está en una lista de contraseñas probables, como "rayo123" o "contraseña", entonces algunos programas podrán adivinarla más rápidamente cuando prueben dichas opciones antes que otras menos probables y otras posibilidades al azar. Cuando el hacker conoce información sobre ustedes, su ataque puede ser más preciso. Si, por ejemplo, el hacker sabe que su mascota se llama "Canela", puede probar "Canela" con diferentes combinaciones de números al final (p. ej., Canela629, Canela3020).

Principios de diseño

Primera parte

Pregunta a los alumnos

¿Quién sabe lo que significa tener una contraseña "segura" o "más segura"? ¿Por qué esto es una buena idea?

Explica a los alumnos

Una contraseña segura ayuda a proteger la información. Aunque tener una contraseña difícil de adivinar no es garantía de que la cuenta no será hackeada, con una contraseña poco segura o débil, es mucho más fácil que alguien acceda a su información.

Ejercicio sobre contraseñas

Pregunta a los alumnos

¿Cuáles son algunos ejemplos de contraseñas débiles?

1. Estos son algunos ejemplos: "Contraseña", "12345", "¡Hola!", una fecha de nacimiento o un apodo.

¿Por qué creen que estas contraseñas son débiles?

1. Las puede adivinar fácilmente otra persona o una computadora al efectuar un "ataque por fuerza bruta".

¿De qué formas se puede aumentar la seguridad de una contraseña?

1. Algunas opciones son agregar números, letras mayúsculas y minúsculas y símbolos. También, crear contraseñas más largas y evitar usar palabras o frases comunes por sí solas.

Interacción grupal

Cuando los participantes hayan expresado sus comentarios, anota estas instrucciones en la pizarra:

Incluir al menos un número.

Incluir al menos un símbolo.

Incluir al menos una mayúscula y una minúscula.

Las contraseñas deben tener siete caracteres como mínimo.

Las contraseñas deben ser fáciles de recordar (a menos que se use un administrador de contraseñas).

Un administrador de contraseñas es un sitio web o una aplicación que ayuda a los usuarios a guardar y organizar sus contraseñas.

Las contraseñas no deben ser palabras comunes o información personal (fechas de nacimiento, nombres de los padres, etc.).

No se debe usar la misma contraseña en varios sitios web.

Explica a los alumnos

Hay dos formas de crear contraseñas seguras. La primera es seguir una "receta para una contraseña", como la de la pizarra. Dicha receta invita a incluir elementos más difíciles de adivinar en una contraseña de texto y números, y esto vuelve más ardua la tarea de descifrarla. La desventaja de este método es que resulta más difícil recordar estas contraseñas.

Contraseñas seguras

Explica a los alumnos

Otra forma de crear contraseñas seguras consiste en hacerlas más largas. Como la seguridad de una contraseña está relacionada con su longitud, cuando usamos una cadena de cuatro o más palabras no relacionadas, es mucho más difícil que la adivinen otras personas o se obtenga mediante ataques por fuerza bruta. Este método tiene la ventaja adicional de que las contraseñas son más fáciles de recordar que con la opción de la receta.

Por último, se puede usar una combinación de ambos métodos para crear una cadena de cuatro o más palabras sin relación entre sí e incluir también símbolos y números.

El objetivo de esta variedad de métodos es el mismo: crear contraseñas únicas y difíciles de adivinar para otras personas.

Explica a los alumnos

Organiza a los participantes en parejas.

En parejas, intenten crear una contraseña segura con las instrucciones anotadas en la pizarra previamente. Recuerden que una contraseña posiblemente difícil de descifrar para una computadora con un enfoque aleatorio, para un humano o una computadora que cuenten con una lista de contraseñas largas y comunes, podría no ser tan complicado. Al final de la actividad no entregarán el trozo de papel donde escriban las contraseñas. No se recomienda que usen esta contraseña en ninguna de sus cuentas, ya que la otra persona del grupo la conocerá.

Concede a los participantes cinco minutos para realizar la actividad. Después recorre la sala y pregunta a los participantes cuáles creen que son los ejemplos de contraseñas más seguras. Pregunta a los participantes si pueden recordar las contraseñas que generaron sin verlas.

Aunque algunos sitios web solicitarán que la contraseña cumpla alguna de estas condiciones, o todas, otros no tienen tales restricciones. También pueden crear contraseñas mediante una cadena de palabras comunes elegidas al azar.

Interacción grupal

Con la misma pareja, indica a los participantes que creen contraseñas nuevas con cadenas de palabras. Diles que cada contraseña debe tener al menos cuatro palabras para que sea segura y fácil de recordar. Concede a los participantes cinco minutos para realizar la actividad. Después recorre la sala y pregunta a los participantes cuáles son sus ejemplos de contraseñas. Nuevamente recuérdales que no recogerás las hojas de papel al final de la actividad y que no deben usar estos ejemplos en ninguna de sus cuentas.

Explica a los alumnos

Algunos sitios web usan un sistema denominado "autenticación multifactor" (o en dos pasos) para verificar la identidad de los usuarios. A menudo, dichos sitios web usan mensajes de texto, una aplicación o un correo electrónico para enviar un código de un solo uso que se debe ingresar junto con la contraseña.

Como se integra un nivel adicional de seguridad que resulta más difícil de quebrantar, las cuentas pueden estar mucho más protegidas. Por ejemplo, para iniciar sesión en una cuenta, una persona debe tener su contraseña y acceso a la aplicación, el dispositivo o la dirección de correo electrónico asociados con la cuenta.

Protección de las contraseñas

Primera parte

Explica a los alumnos

Incluso cuando creamos una contraseña que difícilmente una persona o computadora podrían descubrir, existen otras formas en las que podría ser insegura.

Pregunta a los alumnos

¿De qué otras formas puede ser insegura una contraseña?

1. Algunos ejemplos incluyen usar una contraseña para varias cuentas, usar una contraseña que contenga información personal, usar la misma contraseña durante muchos años u olvidar la contraseña.

¿Con qué frecuencia creen que deberían cambiar sus contraseñas?

Explica a los alumnos

Hasta las mejores contraseñas son susceptibles a riesgos o robos, pero existen formas para protegerse. Si ocurre una filtración de datos en un sitio web donde tienen una cuenta, asegúrense de cambiar la contraseña de ese sitio, así como la de cualquier otro sitio web donde usen contraseñas similares.

Recordar muchas contraseñas largas y complejas puede ser difícil.

Pregunta a los alumnos

¿Creen que es buena idea escribir las contraseñas en un trozo de papel o un documento en su computadora? ¿Por qué?

Interacción grupal

Menciona las posibilidades de que alguien encuentre el trozo de papel o vea el archivo en la computadora. Explica que una opción es usar un administrador de contraseñas, una aplicación que ayuda a los usuarios a almacenar y organizar sus contraseñas.

Segunda parte

Explica a los alumnos

Todos los días usamos muchas cuentas en diferentes sitios web. Iniciar y cerrar

sesión en cada sitio web cada vez puede volverse complicado.

Pregunta a los alumnos

¿Alguna vez usan la función "Guardar contraseña" del navegador para guardar la contraseña de un sitio web? ¿Por qué?

¿Entienden cómo un sitio web recuerda quiénes son?

1. Pide a los participantes que lo expliquen y, a continuación, coméntales que los sitios web recuerdan cuando alguien inició sesión porque almacenan una cookie. Las cookies son archivos muy pequeños que se guardan en la computadora y permiten al sitio web reconocer al usuario y la computadora en futuras visitas, sin que necesite volver a iniciar sesión. Sin embargo, las cookies también se pueden usar para hacer un seguimiento de alguien a medida que navega de un sitio web a otro. Este es uno de los métodos para mostrarles determinados anuncios.

¿Está bien guardar una contraseña en una computadora propia?

Pregunta a los alumnos

¿La computadora tiene una contraseña para entrar?

¿Qué ocurre cuando se comparte la computadora con otras personas?

1. En ese caso, aunque la contraseña esté oculta mediante puntos o asteriscos en el campo de contraseña, otras personas que usen la computadora podrían descifrar cuál es. Solo porque no es posible ver la contraseña en la pantalla, no significa que no esté almacenada en alguna parte.

Pregunta a los alumnos

¿Hay ocasiones en las que está bien compartir una contraseña? ¿Cuándo? ¿Por qué?

1. Algunos ejemplos pueden ser que los padres quieren conocer sus contraseñas o que tienen una cuenta conjunta o familiar en algún servicio como Netflix.

¿Comparten sus contraseñas con alguien? En caso de hacerlo, ¿con quién y por qué?

¿Si un amigo cercano les dijera algo como "si de verdad me quieres", eso haría que compartieran su contraseña con esa persona? ¿Por qué?

Explica a los alumnos

Pueden compartir su contraseña con alguien a quien quieran, pero querer a alguien no necesariamente significa que deben tener acceso total a sus cuentas en internet.

Antes de compartir su contraseña, reflexionen detenidamente sobre su relación con esa persona, incluso cómo podría cambiar con el tiempo. Por ejemplo, compartir su contraseña con sus padres o cuidadores es una decisión muy diferente a compartirla con su mejor amigo.

Pregunta a los alumnos

¿Qué podría pasar cuando se comparte una contraseña?

1. Alguien podría hackear sus cuentas bancarias, hacerse pasar por ustedes en internet o descubrir algunos de sus secretos.

Si compartieron la contraseña de una cuenta, ¿usarían dicha cuenta de un modo diferente?

Pregunta a los alumnos

¿Hay cosas que no verían en Netflix o no escribirían en un correo electrónico si alguien más pudiera ver lo que hacen?

Interacción grupal

Los participantes deben reflexionar sobre su propio comportamiento al usar una cuenta compartida. Deben considerar que su actividad en internet puede ser vista por los demás usuarios de la cuenta.

Pregunta a los alumnos

Si su cuenta es una representación virtual de su persona, como el caso de un perfil de medios sociales, ¿está bien permitir que otras personas la usen?

Interacción grupal

Conversen sobre la posibilidad de que alguien se haga pasar por ustedes y envíe mensajes a sus amigos.

Pregunta a los alumnos

¿Permiten que alguno de los dispositivos que usan almacenen sus contraseñas?
¿Por qué? ¿Eso significa que es seguro guardar sus contraseñas en su teléfono o computadora personal? ¿Qué pasa cuando prestan su teléfono o computadora a

algún amigo?

¿Comparten algún dispositivo con otras personas, sean amigos o familiares?

¿Comparten una cuenta en dicho dispositivo o cada persona tiene su propia cuenta?

¿Alguna vez usan dispositivos "públicos", como en la biblioteca, la escuela o algún otro lugar? ¿Hacen en ese dispositivo lo mismo que harían en cualquier otro?

Tercera parte

Interacción grupal

Organiza a los participantes en parejas.

Explica a los alumnos

Conversen con su compañero sobre si alguna vez llegaron a una computadora en la escuela, la biblioteca o algún otro espacio comunitario y vieron que otra persona había dejado abierta la sesión de su cuenta de medios sociales o correo electrónico. Reflexionen sobre si echarían un vistazo en la cuenta o harían otra cosa.

Interacción grupal

Concede a los participantes cinco minutos para debatir y pide que compartan sus reflexiones. Involucra al grupo en un debate sobre dicho uso no autorizado.

Acceso a cuentas no autorizado

Primera parte

Interacción grupal

Nota: Parte del contenido de esta actividad se aborda en la actividad n.º 1: "Aspectos básicos de las contraseñas". Dejamos a tu criterio si quieres repasar este material u omitirlo.

Explica a los alumnos

Existe la posibilidad de que otras personas accedan a sus cuentas. Incluso, sin conocer la contraseña previamente, puede ser que la adivinen. Si alguien conoce suficiente información personal sobre ustedes, puede hacer conjeturas fundamentadas de su contraseña. También puede ocurrir que esta información se obtenga tras convencer a alguien de una empresa para que la proporcione. Como no se usa tecnología para irrumpir en la cuenta, este tipo de ataque se conoce como hackeo social o ingeniería social.

Pregunta a los alumnos

Levante la mano a quién se le olvidó alguna vez su contraseña para entrar a un sitio web.

¿Qué pasa al hacer clic en "Olvidé mi contraseña"?

1. En general, el sitio web solicitará que se respondan preguntas de seguridad o propondrá contactarlos a través de un número de teléfono o correo electrónico.

¿Cuáles son algunas de las preguntas de seguridad de los sitios web?

1. Explica cómo algunas de estas son preguntas que amigos o conocidos podrían responder o adivinar. Ejemplos de datos que suelen preguntarse incluyen el nombre de la mascota, el lugar donde nacieron, el apellido de soltera de la mamá, el nombre del profesor favorito, el nombre del mejor amigo o el equipo deportivo favorito.

¿Quién más podría conocer este tipo de información sobre ustedes?

¿Cómo los contacta un sitio web cuando olvidan su contraseña?

¿Quién más podría tener acceso a estos puntos de contacto?

Pregunta a los alumnos

¿Cómo podría un desconocido obtener la información personal asociada con sus respuestas para las preguntas de seguridad?

1. Podrían hacerlo a través de publicaciones en medios sociales, mediante búsquedas en internet de información pública, con intentos repetidos de adivinar la información, al ponerse en contacto con amigos suyos, etc.

¿Cuáles son algunos ejemplos de publicaciones en medios sociales con información personal?

1. Por ejemplo, una foto de Instagram de su gato con su nombre en el texto, una foto con una ubicación etiquetada o publicaciones de cumpleaños públicas.

¿Cómo se puede usar Google para buscar información sobre alguien y hackear su contraseña?

1. Si un motor de búsqueda muestra una foto durante la época escolar de una persona en un periódico en internet de la escuela, podrían averiguar el nombre de su profesor.

Segunda parte

Explica a los alumnos

Publicar información que contenga las respuestas a sus preguntas de seguridad puede ser una práctica muy poco segura. Deben asegurarse de elegir preguntas de seguridad cuya respuesta solo ustedes conozcan. También pueden inventar respuestas para dichas preguntas, siempre que las guarden en un administrador de contraseñas o que sean fáciles de recordar.

Los sitios web pueden ponerse en contacto con los usuarios a través del número de teléfono o correo electrónico asociado a su cuenta. Cuando un usuario olvida su contraseña, los sitios web suelen proporcionarle una temporal o un hipervínculo al que puede acceder para restablecerla.

Pregunta a los alumnos

¿Es este un modo seguro de garantizar que la persona que solicita la nueva contraseña es el usuario?

¿Qué pasa cuando se comparte la dirección de correo electrónico asociada a la cuenta?

1. El método del enlace para restablecer la contraseña es seguro la mayor parte del tiempo, pero involucra un riesgo cuando se comparte una cuenta o contraseña con alguien más.

Explica a los alumnos

Una forma del hackeo social consiste en contactar directamente a las personas e intentar engañarlas para que proporcionen su información. En ocasiones, alguien podría enviarles un correo electrónico haciéndose pasar por otra persona (un amigo, un familiar o un empleado del banco) y pedirles que compartan información importante con ellos (como su fecha de nacimiento) con el pretexto de verificar su identidad. También hay casos más sutiles, como cuando alguien hackea la cuenta de medios sociales de un amigo y les escribe (a ustedes y probablemente a muchos otros) para preguntarles su fecha de cumpleaños o el lugar donde crecieron. Si reciben mensajes extraños de sus amigos, lo primero que deben hacer es ponerse en contacto con ellos (fuera de la plataforma de medios sociales) para confirmar que efectivamente ellos les enviaron el contenido.

Los ataques donde se usan sitios web o direcciones de correo electrónico que parecen reales se conocen como phishing y pueden derivar en el robo de identidades. Por ejemplo, un ladrón de identidades puede obtener tarjetas de crédito a nombre de ustedes y usarlas, lo que podría ocasionarles problemas cuando sean mayores y quieran obtener una tarjeta de crédito.

Mediante el phishing, el ladrón puede hacerse pasar por ustedes y acceder a más información, de modo que podría husmear en sus correos electrónicos, enviar mensajes a sus amigos o robarse su dinero. En el proceso, el ladrón también podría crear una nueva contraseña para la cuenta y bloquearles el acceso.

Tarea

Guía

Tarea

Pide a los participantes que contesten las siguientes preguntas y agreguen sus respuestas en forma de texto o imágenes a la guía de aprendizaje sobre las contraseñas.

1. ¿Cuáles son tres recomendaciones principales de esta sesión que aplicarás la próxima vez que crees una contraseña?
2. ¿En qué caso consideras que está bien compartir tu contraseña con alguien más? Menciona uno.
3. ¿Cuáles son las tres estrategias que puedes aplicar para compartir tu contraseña de forma segura?
4. ¿Cuáles son tres ejemplos de lo que puede salir mal cuando una contraseña llega a las manos equivocadas?