



Girls Who Code en casa

Detective cibernética

Descripción de la actividad

¿Sabía que el primer teléfono inteligente se creó en 1992? Si bien el teléfono Simon se consideraba en cierta forma un teléfono inteligente, sus funciones y su aspecto eran muy básicos en comparación con los teléfonos que usamos hoy en día. Mire la foto de la derecha en la que se compara el teléfono Simon con un iPhone 4S.



Fuente de la imagen: [Time](#)

El teléfono Simon tenía una pantalla táctil que solo podía usarse para la carga de notas, una libreta de direcciones, un calendario, un reloj y responder a las llamadas. Mire este [video](#) con una demostración del teléfono. La tecnología ha evolucionado exponencialmente desde el primer teléfono inteligente con casi todo tipo de dispositivos electrónicos conectados a Internet a través de [wifi](#) o [5G](#). La comodidad de tener todos nuestros dispositivos conectados conlleva posibles grandes riesgos de seguridad.

Se estará preguntando por qué es importante esto. Cuando usted compra artículos en línea, completa una solicitud para la universidad o se registra en una nueva aplicación, debe proporcionar información confidencial, como el número de su tarjeta de crédito, su nombre, su fecha de nacimiento y, a veces, su número del seguro social. En 2019, aproximadamente 1 de cada 15 personas fue víctima de un [fraude de identidad](#). El primer paso para protegerse es informarse sobre los tipos de ataques que pueden dejarnos vulnerables. Los especialistas en seguridad cibernética se encargan de implementar medidas de seguridad en cualquier computadora (es decir, cualquier dispositivo electrónico que esté conectado a Internet) y de reconocer las posibles amenazas. [La seguridad cibernética](#) es un sector de rápido crecimiento que representa entre el 32 % y el 45 % de todos los puestos de trabajo en tecnología de Estados Unidos, con un salario básico promedio de **\$83,000**. En esta actividad sin conexión, usted hará de especialista en seguridad cibernética o detective cibernética, para lo cual deberá seguir las pistas presentadas en el cuento e identificar el ataque cibernético.

Objetivos del aprendizaje

Al finalizar esta actividad, será capaz de:

- ❑ identificar distintos tipos de virus y ataques cibernéticos frecuentes.

Materiales

→ No se requiere material adicional.

Conocimientos previos

→ No se requieren conocimientos previos.

“Mujeres en tecnología” artículo destacado: Jaya Baloo



Fuente de la imagen:
[Intelligent CISO](#)

En 2017, Jaya Baloo fue nombrada entre los [100 CISO \(directores de Seguridad de la Información\) más importantes](#). Es experta en [criptografía](#) y estudia técnicas para proteger las comunicaciones. Jaya comenzó a desarrollar su interés por las computadoras a los 9 años de edad. Después de graduarse en la [Tufts University](#), Jaya trabajó en Bankers Trust como instructora de seguridad en Internet. Gracias a esta experiencia, se dio cuenta de que la seguridad cibernética era vista como un arma por Estados Unidos, lo que explicaba por qué este país ocultaba su tecnología al público. No obstante, Jaya tenía una opinión diferente: la seguridad cibernética debía hacerse pública para defender la vida de todos.

Con la evolución de la tecnología y la invención de más dispositivos inteligentes, la seguridad cibernética es más importante que nunca. Con todos los dispositivos conectados en un mismo sistema, muchas personas pueden quedar vulnerables a los ataques cibernéticos. Jaya ahora trabaja para [Avast](#) y ofrece un software antivirus gratuito para todos. Parte de su trabajo en Avast es implementar la [informática cuántica](#) y la [inteligencia artificial](#) para detectar amenazas y proteger las computadoras. Jaya considera que la seguridad cibernética es un *derecho fundamental* y debe ser de libre acceso.

Mire este [video](#) para obtener más información sobre la importancia de la seguridad cibernética y cómo se pueden vulnerar fácilmente los sistemas a través de dispositivos 5G conectados. ¿Desea obtener más información sobre Jaya? Mire su charla [TED talk](#) de 2017 sobre cómo la seguridad cibernética repercute en nuestra vida diaria y explore su [perfil](#) en la Singularity University.

Reflexión

Ser un experto informático es más que sencillamente ser bueno programando. Tómese algunos minutos para reflexionar sobre cómo Jaya y su trabajo reflejan las características que todos los verdaderos expertos informáticos deben desarrollar en sí mismos: valentía, resiliencia, creatividad y propósito.



PROPÓSITO

Jaya considera que el software de seguridad cibernética debería ser de libre acceso, en lugar de un servicio pago. Esta opinión contrasta con la forma en la que el gobierno estadounidense ve este conocimiento. ¿Cuáles son las ventajas de distribuir gratuitamente el software de seguridad cibernética? ¿Cuáles son los posibles riesgos de la distribución gratuita de software?

Comparta sus respuestas con un familiar o amigo. Anime a los demás para que lean más sobre Jaya y se unan a la charla.

Paso 1: ¿Qué es la seguridad cibernética? (de 2 a 3 minutos)

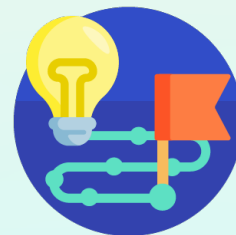


Imagine a un hacker. ¿Qué aspecto tiene? ¿Qué hace? De algunas películas, podemos imaginarnos a un hombre con una capucha negra delante de muchas computadoras. ¿Sabía que alrededor del 20 % de los hackers son mujeres? Un **hacker** es una persona que usa sus conocimientos de programación informática para exponer posibles vulnerabilidades en un sistema informático. Quizá piense que un hacker es una mala persona, pero muchos en realidad trabajan para defender las computadoras y reforzar las medidas de seguridad contra los ciberdelincuentes. A esta práctica se la denomina **seguridad cibernética**.

La seguridad cibernética hace referencia a la práctica de defender las computadoras (cualquier dispositivo electrónico que pueda almacenar y procesar datos), los servidores, las redes y los datos en general de los ataques cibernéticos. Casi todos los tipos de dispositivos electrónicos se conectan a Internet a través de **wifi** o **5G**; por lo tanto, proteger la información de ataques cibernéticos es más importante que nunca. Quizá ya esté familiarizada con algunos ataques famosos a la privacidad de las celebridades, la divulgación de información confidencial de los gobiernos y los programas de delincuencia en la televisión; o tal vez conozca personalmente a alguien que haya sufrido un ataque cibernético.

En 2019, aproximadamente 1 de cada 15 personas fue víctima de un **fraude de identidad**. El primer paso para protegerse es informarse sobre los tipos de ataques que pueden dejarla a usted y a sus datos personales vulnerables. En esta actividad, la guiaremos por algunos ejemplos de ataques frecuentes y medidas prácticas para que pueda protegerse de posibles amenazas.

Paso 2: Revisar las instrucciones de la actividad (2 minutos)



En esta actividad, usted asumirá el rol de detective especializada en ataques cibernéticos o de *detective cibernética*. En esta actividad del tipo “elige tu propia aventura”, decidirá qué medidas tomará para responder a un ataque cibernético.

En la escena inicial del cuento, obtendrá información sobre lo que ha ocurrido y algunas pistas sobre la situación. Al final de cada escena del cuento, tendrá dos opciones sobre qué hacer a continuación. Una vez que elija una opción, seguirá las instrucciones asociadas a su elección. Las instrucciones variarán según sus elecciones y repercutirán en el resultado global del cuento. Si no le agrada el resultado obtenido, vuelva e intente comenzar con el cuento de nuevo.

Ahora que ya tiene una idea general de las instrucciones de esta actividad, es hora de ponerse el sombrero de detective y las lupas virtuales y empezar.

Consejo para padres y docentes

¿Quiere que esta actividad sea más activa? Sugerimos una minibúsqueda del tesoro con las escenas y actualizar las instrucciones para su detective cibernética.

Paso 3: Leer sobre la crisis de Instagram (de 10 a 15 minutos)

Como cualquier mañana normal, usted se levanta, enciende el teléfono e inmediatamente abre Instagram. Mientras se frota los ojos, percibe algo diferente en la pantalla. Después de frotarse los ojos algunas veces más, ve el siguiente mensaje:



Aparentemente, el nombre de usuario que ha introducido no pertenece a una cuenta. Compruebe su nombre de usuario y vuelva a intentarlo.

Piensa: “Mmm, qué raro, ¿me habré equivocado de contraseña?”. Intenta iniciar sesión nuevamente, y aparece el mismo mensaje de error. Piensa: “¿Qué significa esto? Yo sé cuál es mi nombre de usuario y mi contraseña”.

¿Qué hace luego?

- A. Se encoge de hombros, deja el teléfono y se prepara para ir a la escuela. Volverá a intentar iniciar sesión más tarde. **Ir a la [página 6](#).**
- B. **¡ENLOQUECE!** Busca en Google el mensaje de error para obtener más información sobre qué hacer a continuación. Ir a la [página 7](#).

Página 6

Empieza a prepararse para su rutina matutina habitual, pero tiene un nudo en el estómago que le dice que algo está mal. Ignora esta sensación por ahora; es más importante prepararse para ir a la escuela. Desayuna, se despide de la familia y se dirige a la parada del autobús para ir a la escuela.

Mientras está en el autobús, decide matar el tiempo e intenta iniciar sesión en Instagram de nuevo. Introduce las credenciales de acceso, esta vez con mucho cuidado para que no haya ningún error en el nombre de usuario o la contraseña. Sigue apareciendo el mismo error: ¿y ahora qué?

- A. Busca en Google el mensaje de error para entender qué significa. Ir a la [página 7](#).
- B. Supone que Instagram está funcionando mal y vuelve a ignorar el mensaje. Ahora, revisa el correo electrónico. Ir a la [página 9](#).

Página 7

Copia y pega el mensaje de error en la barra de búsqueda de Google y encuentra una [pregunta en Quora](#).

Pregunta: Estoy intentando iniciar sesión en Instagram, pero el sitio dice que mi nombre de usuario no pertenece a una cuenta. ¿Alguien sabe cómo arreglarlo?

Respuesta: Compruebe que haya escrito la información correctamente. Puntuación, mayúsculas, ortografía y símbolos. Todo. Copie y pegue si es necesario.

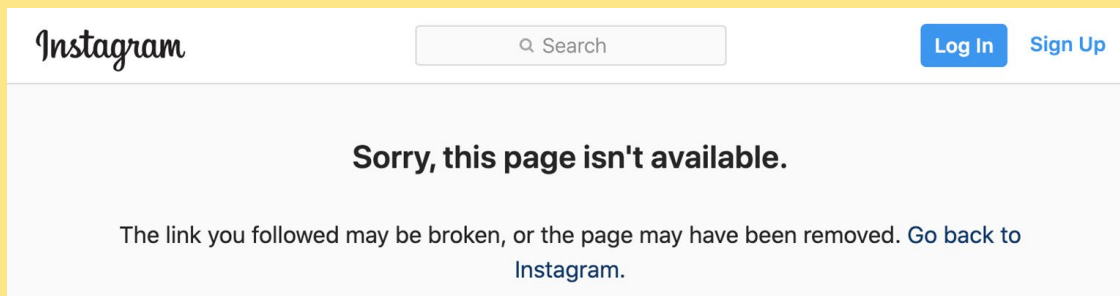
¿Sigue sin funcionar?

Intente iniciar sesión con Facebook o una cuenta de correo electrónico.

¿Sigue sin funcionar?

Es posible que su cuenta haya sido desactivada o prohibida (lo que significa que la han denunciado por infringir una o más políticas de Instagram). Para ver si esto es así, vaya a un navegador web en una computadora, escriba "http://www.instagram.com/[su perfil aquí]" y observe si aparece su cuenta. Si no aparece, es posible que se haya eliminado. Cree una nueva cuenta o comuníquese con el equipo de Instagram. Si aparece, intente con las primeras dos opciones nuevamente. ¿Sigue sin funcionar? Envíe un mensaje de correo electrónico al equipo de Instagram.

Sigue las instrucciones que ha encontrado en las respuestas de Quora anteriores. Primero, intenta iniciar sesión con sus credenciales, y comprueba una vez más que su nombre de usuario y su contraseña estén bien escritos. No hay caso. Sigue sin funcionar. Luego, intenta iniciar sesión con Facebook, pero *nada*. Su corazón palpita fuerte y se siente insegura respecto de lo que esto significa realmente. Intenta el último paso. Abre Safari en su teléfono y escribe "<http://www.instagram.com/cyberdetective101>".



"Lo lamentamos, la página no está disponible".

Pasar a la [página 8](#) para continuar con el cuento.

Página 8

El último paso... En su interior, no esperaba tener que dar el último paso. Localiza el botón de **AYUDA** y lee los temas. Selecciona **Solución de problemas de inicio de sesión** en Temas populares. A continuación, selecciona "No encuentro mi cuenta o no sé mi nombre de usuario en Instagram" y lee la respuesta.

Si no puede localizar su cuenta después de introducir su nombre de usuario:

- Asegúrese de que está introduciendo su nombre de usuario correctamente, en especial si el nombre de usuario tiene caracteres repetidos.
- No incluya el símbolo @ en su nombre de usuario.

Si cree que su nombre de usuario se ha modificado porque su cuenta se ha visto afectada:

- Compruebe si ha recibido un correo electrónico de Instagram mediante el cual se le notifica que la información de su cuenta ha cambiado.
- Pídale a un amigo que visite su perfil y haga una captura de pantalla de su nombre de usuario actual.

Obtenga más información sobre lo que puede hacer si [cree que su cuenta fue vulnerada](#).

Prueba todas estas sugerencias y mira la última oración. Piensa: "¿Mi cuenta fue vulnerada?". ¿Qué hace luego?

- A. Piensa: "¿Por qué a alguien le interesaría vulnerar mi cuenta? Ni siquiera tengo tantos seguidores, y mi cuenta es privada". Ignora la sugerencia y decide esperar hasta la tarde para volver a verificar qué sucede. Ir a la [página 9](#).
- B. Piensa: "Quizá alguien vulneró mi cuenta". Hace clic en el [enlace](#) y sigue con los demás pasos. Ir a la [página 10](#).

Página 9

Escanea su correo electrónico y su ojo capta inmediatamente un correo electrónico con el asunto “Contáctenos si quiere recuperar su cuenta de Instagram”. Hace clic para abrir el correo electrónico y leer los detalles.

Hola, @cyberdetective101:

Nos hemos apoderado de su cuenta, y hemos obtenido acceso a sus fotos, sus amigos y su información. Si no responde mediante el envío de \$2,000 a [esta cuenta](#) para hoy a la noche, eliminaremos su cuenta y venderemos su información personal.

No intente ponerse en contacto con Instagram para pedir ayuda porque hemos cambiado toda su información y seremos alertados si intenta recuperar su cuenta y la eliminaremos al instante.

¡Usted no puede creer lo que está sucediendo! ¿Qué hace luego?

- A. Envía el dinero. Todo va a estar bien, ¿no es así? Ir a la [página 11](#).
- B. ¡Han vulnerado su cuenta! Ignora el mensaje y va directamente a la página de ayuda de Instagram. Ir a la [página 10](#).

Página 10

En la página de ayuda de Instagram, encuentra el comentario [“Pienso que han vulnerado mi cuenta de Instagram”](#). Hace clic en el enlace y sigue los pasos indicados en la información de ayuda de Instagram.

Consulta su correo electrónico para ver si tiene un mensaje de Instagram. Revisa su correo electrónico en detalle e incluso la papelera. Efectivamente, hace 2 días aproximadamente, usted recibió un correo electrónico de Instagram mediante el cual se le notificaba que su dirección de correo electrónico había cambiado. Trata de revertir el cambio haciendo clic en el enlace [Proteja su cuenta aquí](#).

Para confirmar su cuenta, debe verificar su identidad; pero no reconoce ninguna de las opciones de recuperación. El correo electrónico y el número de teléfono en su cuenta han cambiado.

Lo único que queda es seguir los pasos para denunciar la cuenta y esperar lo mejor. Sigue esperando la respuesta de Instagram a su solicitud.

Ir a la [página 12](#).

Página 11

Rápidamente, toma los datos de la tarjeta de crédito de sus padres y piensa: “¡Uf, menos mal que mamá me dejó guardar los datos de su tarjeta en mi cuenta de App Store!”. Con los datos de la tarjeta en la mano, hace clic en el enlace del correo electrónico y sigue las instrucciones para enviar el dinero. Respira aliviada y espera a que le devuelvan el dinero a la cuenta. Por fin, esta pesadilla está por terminar.

Abre el navegador web en su teléfono y observa esta ventana emergente que dice:

Su teléfono ha sido vulnerado.
Todas las acciones en este dispositivo están controladas por un hacker.
¡Se requiere una acción inmediata!

Recibe un nuevo mensaje de correo electrónico. Lo abre y es otro correo electrónico del hacker que dice:

Hola, @cyberdetective101:

Nos hemos apoderado de su teléfono y hemos obtenido acceso a sus fotos, sus contactos y su información. Si no responde mediante el envío de \$10,000 a [esta cuenta](#) para hoy a la noche, venderemos toda su información personal y contactaremos a todos sus amigos.

Su sistema ha sido vulnerado, y ahora corre el riesgo de convertirse en víctima de fraude de identidad.

Ir a la [página 12](#).

Paso 4: Conclusión (de 10 a 15 minutos)

Dependiendo del camino que haya elegido en el transcurso del cuento, usted puede haber sido objeto de múltiples ataques cibernéticos.




Ataque n.º 1: Contraseñas poco seguras (de 5 a 8 minutos)

Si un hacker ha podido acceder a su cuenta, lo más probable es que se deba a que usted tiene una **contraseña poco segura o vulnerable**. Cuando se crea una contraseña, suele haber algunos requisitos sencillos para que la cuenta sea válida. Pueden aplicarse algunas restricciones:

- un mínimo de 6 a 8 caracteres;
- una variedad de letras mayúsculas y minúsculas;
- al menos un número;
- al menos un carácter especial.

Incluso si usted crea una contraseña que cumple los requisitos mínimos, un hacker podría tardar entre algunos segundos y un día en descifrarla. Es muy sencillo y barato para los hackers vulnerar la mayoría de las cuentas. Eche un vistazo a la tabla a continuación para comparar cómo las contraseñas pueden incidir en la vulnerabilidad de sus cuentas en línea.

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years



Cybersecurity that's approachable.
Find out more at hivesystems.io

Fuente de la imagen: [Reddit](#)

Paso 4: Conclusión (continuación)

Tómese un momento para reflexionar sobre lo que acaba de aprender sobre las contraseñas, y pruebe sola para ver si puede crear contraseñas seguras.

- ❑ **Clasifique las siguientes contraseñas del 1 al 5, donde 1 representa la contraseña más segura y 5 representa la contraseña menos segura.** Para ayudar con la clasificación de las contraseñas, incluimos algunas columnas: cantidad de caracteres y variación de caracteres.
- ❑ **Complete la columna con la cantidad de caracteres y la variación de caracteres para cada contraseña.**
- ❑ **Clasifique las siguientes contraseñas del 1 al 5.**
- ❑ **Verifique sus respuestas con [este sitio web](#) y escriba cada opción.** Complete la última columna; las horas que demorará el hacker en descifrar la contraseña para comparar sus clasificaciones.

Clasificar <i>1: más segura; 5: menos segura</i>	Contraseña	Cantidad de caracteres <i>¿Cuántos caracteres tiene la contraseña?</i>	Variación de caracteres <i>¿La contraseña incluye letras mayúsculas o letras minúsculas? ¿Números? ¿Símbolos?</i>	Horas para que el hacker descifre la contraseña <i>Según _____, ¿cuánto tiempo tardaría un hacker en descifrar la contraseña?</i>
<i>Contraseña de ejemplo</i>	ku8@}:'\$	8	Letras minúsculas, símbolos y números	4 horas
	hcVESx			
	vWESp3Tt			
	Sg3Jpezyhv			
	password1			
	jG/8ab{s			

Paso 4: Conclusión (continuación)

- ❑ Tómese **2 minutos** para idear sus propias contraseñas seguras y escríbalas en el espacio a continuación. Los hackers deberían tardar *al menos un año* en descifrar las contraseñas.

- ❑ Navegue hasta [este sitio web](#) para comprobar la seguridad de las contraseñas en los pasos anteriores.



¿Le sorprendieron los resultados? Estas son algunas pautas y recomendaciones generales para asegurar todas sus cuentas.

- **Nunca use las mismas contraseñas para varias cuentas distintas.** Algunos sitios web son más seguros que otros; y si un hacker consigue acceder a una cuenta, usted no querrá facilitarle el acceso a sus otras cuentas. Recordar todas las contraseñas puede ser difícil, por lo que sugerimos usar un administrador de contraseñas, como [BitWarden](#), [KeePassXC](#) o [LastPass](#).
- **Nunca guarde su contraseña en el navegador.** Cada vez que inicie sesión en un sitio web, el navegador le preguntará si quiere guardar su contraseña. ¡**Selecione “Nunca”!** Aunque sea difícil recordar las contraseñas, guardarlas en los navegadores les facilita a los hackers el acceso a la información. Use administradores de contraseñas que le ayuden a recordar las contraseñas complejas.
- **Use una variedad de caracteres para su contraseña.** En general, se recomienda que las contraseñas contengan una variedad de letras mayúsculas y minúsculas, números y caracteres especiales y que tengan una longitud mínima de 11 caracteres. Evite palabras típicas como “contraseña”, nombres, fechas típicas (como la fecha de nacimiento) o números como “111” o “1234”.
- **Establezca una autenticación de dos factores.** Para asegurar aún más sus cuentas, active la configuración de 2FA (autenticación de dos factores), lo cual le obliga a iniciar sesión en las cuentas mediante una contraseña **y** una verificación a través de un dispositivo de confianza, un correo electrónico o preguntas de seguridad. Este paso adicional contribuye mucho a la seguridad de las cuentas. Lea este [artículo](#) para averiguar cómo activar 2FA para una variedad de cuentas, como [Instagram](#), [Amazon](#), [Facebook](#), [Google](#) y [Twitter](#).
- **Cambie las contraseñas con cierta frecuencia.** Lo ideal es cambiarlas cada tres meses.

Ataque n.º 2: Phishing o suplantación de identidad (de 5 a 8 minutos)



El **phishing** a menudo es un correo electrónico, un mensaje de texto o un mensaje emergente que parece provenir de una fuente conocida y que les pide a los usuarios que hagan clic en un enlace o proporcionen información confidencial. Estos correos electrónicos parecen provenir de un banco, credenciales de la universidad, varias cuentas en línea, etc. Estos enlaces suelen llevar a los usuarios a sitios web inseguros en los que los atacantes pueden acceder a su computadora y continuar con otras actividades maliciosas.

A veces, los sitios web replican sitios conocidos y roban la información cuando usted inicia sesión en sus sitios.

En nuestro cuento, usted quizá haya elegido un camino en el que recibió un correo electrónico malicioso. Este correo electrónico es particularmente diferente de los típicos correos electrónicos de phishing y contiene instrucciones e información más dirigidas. A este ataque se lo denomina **phishing selectivo**, ya que el correo electrónico estaba dirigido específicamente a un solo usuario con instrucciones específicas. Al hacer clic en el enlace del correo electrónico, se expuso a la computadora a un **malware** o software malicioso que la infecta.

Aquí tiene un ejemplo de correo electrónico de phishing:



Fuente de la imagen: **Norton**

Este correo electrónico en particular podría parecer creíble, ya que el logotipo es correcto y el estilo del texto coincide con otras comunicaciones de Instagram. Al configurar 2FA, es decir, la autenticación de dos factores, su código debe enviarse en un correo electrónico aparte antes de que usted inicie sesión con éxito. También puede notar la falta de espacio entre la última oración. Estos son indicadores muy pequeños pero detallados de que este correo electrónico es falso.

- ❑ Tómese de **5 a 10 minutos** para analizar algunos ejemplos de correo electrónico de phishing en este **sitio web** y ver si puede identificar los detalles clave que lo convierten en un ataque de phishing.

Paso 4: Conclusión (continuación)



Los correos electrónicos de phishing pueden ser difíciles de detectar. A continuación, se incluyen algunas pautas para determinar si un correo electrónico es una estafa.

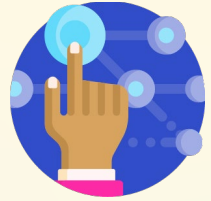
- **Errores de gramática u ortografía:** ¿Hay errores gramaticales en el mensaje? ¿Hay palabras mal escritas o el formato es ligeramente incorrecto?
- **Errores de logotipo o imagen:** ¿Las imágenes son incorrectas? ¿Es posible que el remitente esté usando un logotipo que no es oficial? ¿La resolución o la calidad de la imagen es baja? (Hay píxeles borrosos).
- **Errores de URL:** ¿El enlace es diferente del sitio web original/creíble? Quizá la URL termina en .org en lugar de en .com.

Si ha identificado un correo electrónico de phishing, aquí tiene algunos pasos que puede seguir para protegerse de posibles ataques maliciosos.



- **No haga clic en ningún enlace.** Los correos electrónicos de phishing pueden pedirle que haga clic en enlaces que instalan malware en su computadora. Asegúrese de no hacer *nunca* clic en los enlaces que haya en el correo electrónico.
- **Denuncie el correo electrónico.** En muchos casos, usted debe acceder al sitio web creíble en un nuevo navegador y denunciar el correo electrónico sospechoso ante la empresa para que puedan proteger sus sitios web. También debe denunciar el correo electrónico ante la Comisión Federal de Comercio en [ftc.gov/complaint](https://www.ftc.gov/complaint).
- **Nunca brinde información personal.** Los correos electrónicos de phishing pretenden obtener información adicional de los usuarios para hacer que sus sistemas sean más vulnerables. En muchos casos, el hacker aún no cuenta con ninguna otra información más que su correo electrónico.
- **Cambie la contraseña.** Después de un ataque, lo mejor es que cambie las contraseñas para proteger sus cuentas por si acaso.

Paso 5: Proteger su huella digital (de 5 a 10 minutos)



Ahora que tiene una idea de algunos de los ataques cibernéticos más frecuentes, ¿qué sigue?

- **Asegúrese de que sus contraseñas sean fuertes y seguras.** Use un administrador de contraseñas, como [BitWarden](#), [KeePassXC](#) o [LastPass](#), para llevar un control de sus contraseñas y cambiarlas al menos cada 3 meses.
- **Descargue antivirus/software antimalware.** Quizá tenga malware en su computadora y no lo sepa. Entre algunos de los software antivirus/antimalware gratuitos que sugerimos, se incluyen [Kaspersky](#), [Avast](#) y [Malwarebytes](#). Asegúrese de que este software se ejecute automáticamente para que compruebe a menudo la presencia de malware en su computadora.
- **Descargue siempre las últimas actualizaciones del sistema.** Las empresas como Windows y Apple siempre intentan garantizar la seguridad de las computadoras que usted usa. Aunque actualizar la computadora puede llevar tiempo, vale la pena, ya que las actualizaciones suelen incluir medidas preventivas para proteger la información.
- **Nunca comparta información personal.** Se recomienda ser selectiva a la hora de compartir información personal, como su nombre, su fecha de nacimiento, la ubicación, su número de teléfono, etc. Puede que no parezca gran cosa, pero para un hacker conseguir esta información puede conducirle a obtener información aún más confidencial, como su número del seguro social.
- **Eduque a los demás.** Aunque mucha gente es consciente de las diferentes amenazas relacionadas con la seguridad cibernética, la mayoría toma pocas precauciones para proteger sus computadoras. Comparta con amigos y familiares sus conocimientos sobre la importancia de la seguridad cibernética y sobre cómo proteger computadoras y cuentas.

Paso 6: Extensiones (de 5 a 30 minutos)

Extensión 1: Datos sobre seguridad cibernética de 2020 (de 5 a 10 minutos)

Mientras pensamos cómo Internet conecta a gente de todo el mundo, analice brevemente cómo los hackers explotan esta vulnerabilidad en 2020. Lea este [artículo](#) de CSO sobre los distintos ataques que se suscitaron este año. Tenga en cuenta también que este artículo se publicó por última vez en marzo de 2020 y que las estadísticas pueden haber cambiado desde entonces.

Extensión 2: Cuento de hacker de Instagram (de 5 a 10 minutos)

El cuento de esta actividad está basado en una experiencia real. Consulte el cuento original [aquí](#). Lamentablemente, esta situación ocurre con demasiada frecuencia y en muchas plataformas de redes sociales. También puede leer una experiencia similar en este [artículo](#) de Forbes.

Extensión 3: Más información sobre otros ataques cibernéticos (de 10 a 30 minutos)

En esta actividad, veremos dos tipos de ataques cibernéticos: las contraseñas poco seguras y los ataques de phishing. A continuación, se ofrecen algunos recursos para informarse más sobre otros ataques cibernéticos que afectan a las personas y a las empresas.

- [Scenario Based Student Guide \(Guía del alumno basada en situaciones\)](#), de CDSE
- [Cybersecurity 101: Intro to the Top 10 Common Types of Cyber Security Attacks \(Aspectos básicos de la seguridad cibernética: introducción a los 10 tipos de ataques a la seguridad cibernética más frecuentes\)](#), de Infocyt

Paso 7: Comparta su proyecto de Girls Who Code en casa (5 minutos)



Nos encantaría ver su trabajo y sabemos que a otros también les gustaría. Agregue su nombre en el [certificado de detective cibernética](#), imprímalo y tómese una selfi. 📷

Cargue su foto en cualquier sitio en las redes sociales. No olvide etiquetar [@girlswhocode](#) [#codefromhome](#), ¡y quizá la destaquemos en nuestra cuenta!

¡Espere más proyectos de Girls Who Code en casa!

