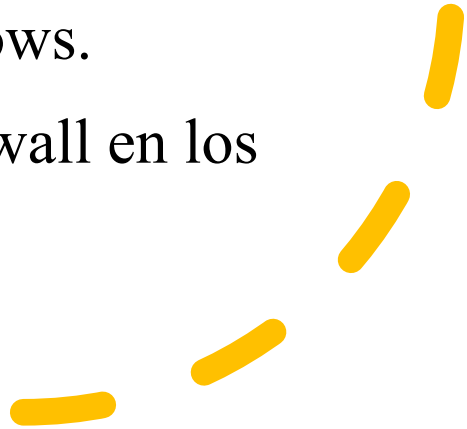


Capítulo 3: Protección de sus datos y de su seguridad

Este capítulo se centra en sus dispositivos personales y sus datos personales. Incluye sugerencias para proteger sus dispositivos, crear contraseñas seguras y usar redes inalámbricas de manera segura. También analiza el mantenimiento de sus datos protegidos. Sus datos en línea valen mucho para los delincuentes cibernéticos. Este capítulo abarca brevemente las técnicas de autenticación para ayudarlo a mantener sus datos protegidos. Además, cubre las opciones para mejorar la seguridad de sus datos en línea con sugerencias sobre qué hacer y qué no hacer en línea.

Proteja sus dispositivos informáticos

- Sus dispositivos informáticos almacenan sus datos y son el portal hacia su vida en línea. La siguiente es una breve lista de pasos a seguir para proteger sus dispositivos informáticos contra intrusiones:
 - **Mantenga el firewall encendido:**
 - Ya sea un firewall de software o un firewall de hardware en un router, el firewall debe estar activado y actualizado para evitar que los hackers accedan a sus datos personales o empresariales. Haga clic [Windows 7 y 8.1](#) o [Windows 10](#) para activar el firewall en la versión correspondiente de Windows.
 - Haga clic [aquí](#) para activar el firewall en los dispositivos Mac OS X.
- 



Proteja sus dispositivos informáticos

- **Utilice un antivirus y antispyware:**

- El software malicioso, como virus, troyanos, gusanos, ransomware y spyware, se instala en los dispositivos informáticos sin su permiso para obtener acceso a su computadora y sus datos.
- Los virus pueden destruir sus datos, ralentizar su computadora o apoderarse de ella. Una manera en que los virus pueden apoderarse de su computadora es permitiendo que los emisores de correo no deseado envíen correos electrónicos desde su cuenta.
- El spyware puede supervisar sus actividades en línea, recopilar su información personal o enviar anuncios emergentes no deseados a su navegador web mientras está en línea.
- Una buena regla es descargar software solamente de sitios web confiables para evitar obtener spyware en primer lugar.
- El software antivirus está diseñado para analizar su computadora y correo electrónico entrante para detectar virus y eliminarlos.
- A veces el software antivirus también incluye antispyware.
- Mantenga su software actualizado para proteger su computadora de software malicioso reciente.

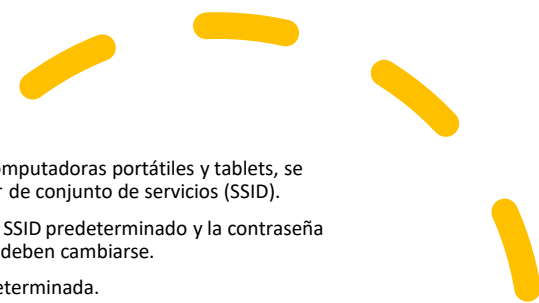


Proteja sus dispositivos informáticos

- **Administre su sistema operativo y navegador:**
 - Los hackers siempre están intentando aprovechar las vulnerabilidades en sus sistemas operativos y navegadores web.
 - Para proteger su computadora y sus datos, establezca los parámetros de seguridad en su computadora o navegador en medio o alto.
 - Actualice el sistema operativo de la computadora, incluidos los navegadores web, y descargue e instale periódicamente parches y actualizaciones de seguridad del software de los proveedores.
- **Proteja todos sus dispositivos:**
 - Sus dispositivos informáticos, ya sean PC, PC portátiles, tablets o smartphones, deben estar protegidos con contraseña para evitar el acceso no autorizado.
 - La información almacenada debe estar cifrada, especialmente en el caso de datos sensibles o confidenciales.
 - En los dispositivos móviles, almacene solo información necesaria en caso de robo o pérdida cuando está fuera de su hogar.
 - Si alguno de sus dispositivos se ve comprometido, los delincuentes pueden tener acceso a todos sus datos a través del proveedor de servicios de almacenamiento en la nube, como iCloud o Google Drive.

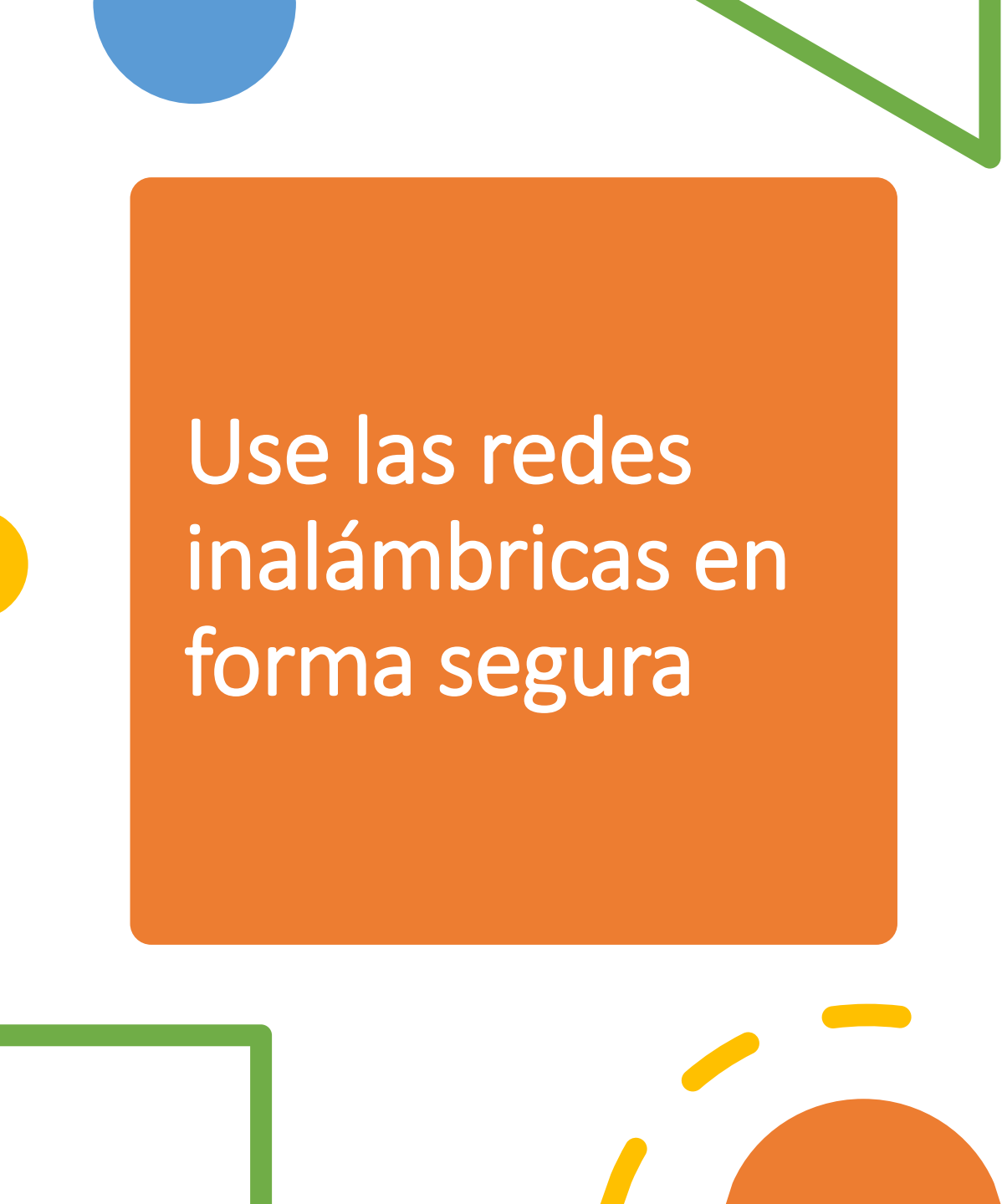
Proteja sus dispositivos informáticos

- **Los dispositivos de IoT (Internet de las cosas) representan un riesgo incluso mayor que los otros dispositivos electrónicos.**
 - Mientras que las computadoras de escritorio, portátiles y los dispositivos móviles reciben actualizaciones de software frecuentes, la mayoría de los dispositivos de IoT aún tiene su firmware original.
 - Si se encuentran vulnerabilidades en el firmware, el dispositivo de IoT es probable que se mantenga vulnerable. Para empeorar el problema, los dispositivos de IoT están diseñados para conectarse con los servidores del proveedor (call home) y solicitar acceso a Internet.
 - Para acceder a Internet, la mayoría de los fabricantes de dispositivos de IoT confían en la red local del cliente.
 - El resultado es que los dispositivos de IoT son muy propensos a verse comprometidos y, cuando lo están, permiten el acceso a la red local del cliente y sus datos.
 - La mejor manera de protegerse de esta situación es contar con dispositivos de IoT con una red aislada compartida únicamente con otros dispositivos de IoT.
- Haga clic [aquí](#) para visitar Shodan, un escáner de dispositivos de IoT basado en la web.



Use las redes inalámbricas en forma segura

- Las redes inalámbricas permiten que los dispositivos habilitados con Wi-Fi, como computadoras portátiles y tablets, se conecten a la red por medio de un identificador de red conocido como identificador de conjunto de servicios (SSID).
 - Para evitar que los intrusos ingresen en su red inalámbrica doméstica, el SSID predeterminado y la contraseña predeterminada para la interfaz de administración en el navegador web deben cambiarse.
 - Los hackers son conscientes de este tipo de información de acceso predeterminada.
 - Opcionalmente, el router inalámbrico también puede configurarse para que no difunda el SSID, lo que añade una barrera adicional para la detección de la red. Sin embargo, esto no debe considerarse una seguridad adecuada para una red inalámbrica.
 - Además, debe encriptar la comunicación inalámbrica habilitando la seguridad inalámbrica y la función de encriptado WPA2 en el router inalámbrico.
 - Incluso con el encriptado WPA2 habilitado, la red inalámbrica aún puede ser vulnerable.
- En octubre de 2017, se descubrió una falla de seguridad en el protocolo WPA2.
 - Esta falla permite a un intruso descifrar la encriptación entre el router inalámbrico y el cliente inalámbrico, lo que permite que este tenga acceso al tráfico de red y lo manipule.
 - Esta vulnerabilidad puede ser atacada utilizando el Ataque de reinstalación de clave (KRACK, Key Reinstallation Attack).
 - Afecta a todas las redes wifi protegidas, modernas.
 - Para mitigar un ataque, un usuario debe actualizar todos los productos afectados: routers inalámbricos y cualquier dispositivo inalámbrico, como computadoras portátiles y dispositivos móviles, tan pronto como las actualizaciones de seguridad estén disponibles.
 - Para las computadoras portátiles u otros dispositivos con NIC por cable, una conexión por cable podría mitigar esta vulnerabilidad.
 - Además, también puede utilizarse un servicio de VPN de confianza para prevenir el acceso no autorizado a los datos mientras se utiliza la red inalámbrica.
- Haga clic [aquí](#) para saber más acerca de KRACK.



Use las redes inalámbricas en forma segura

- Cuando está lejos de casa, los puntos públicos de acceso inalámbrico permiten tener acceso a su información en línea y navegar por Internet.
 - Sin embargo, es mejor no acceder ni enviar información personal confidencial a través de una red pública inalámbrica.
 - Verifique si su computadora está configurada para compartir archivos y medios digitales y si requiere la autenticación de usuario con encriptación.
 - Para evitar que una persona intercepte su información (lo que se conoce como “eavesdropping”) mientras utiliza una red pública inalámbrica, utilice túneles VPN y servicios encriptados.
 - El servicio VPN proporciona acceso seguro a Internet con una conexión cifrada entre la computadora y el servidor VPN del proveedor de servicios VPN.
 - Con un túnel VPN encriptado, aunque se intercepte una transmisión de datos, no podrá descifrarse.
- Haga clic [aquí](#) para obtener más información acerca de la protección al utilizar redes inalámbricas.

Use bluetooth de forma segura

Muchos dispositivos móviles, como smartphones y tablets, incluyen el protocolo inalámbrico Bluetooth.

Esta funcionalidad permite que los dispositivos con Bluetooth habilitados se conecten entre sí y compartan información.

Desafortunadamente, Bluetooth puede ser atacado por hackers a fin de espiar algunos dispositivos, establecer controles del acceso remoto, distribuir malware y consumir baterías.

Para evitar estos problemas, mantenga Bluetooth desactivado cuando no lo utiliza.

Utilice contraseñas únicas para cada cuenta en línea

- Posiblemente tenga más que una cuenta en línea y cada cuenta debe tener una contraseña única.
- Son muchas contraseñas para recordar.
- Sin embargo, la consecuencia de no usar contraseñas seguras y únicas los deja a usted y sus datos vulnerables ante los delincuentes cibernéticos.
- Usar la misma contraseña para todas las cuentas en línea es como usar la misma llave para todas las puertas cerradas; si un atacante consiguiera su contraseña, tendría acceso a todo lo que usted posee.
- Si los delincuentes obtienen su contraseña mediante la suplantación de identidad, por ejemplo, intentarán ingresar en sus otras cuentas en línea.
- Si solo utiliza una contraseña para todas las cuentas, pueden ingresar en todas estas, robar o borrar todos sus datos, o hacerse pasar por usted.

Utilice contraseñas únicas para cada cuenta en línea

Utilizamos tantas cuentas en línea que necesitan contraseña que es demasiado para recordar.

Una solución para evitar reutilizar las contraseñas o utilizar contraseñas débiles es utilizar un administrador de contraseñas.

El administrador de contraseñas almacena y encripta todas sus contraseñas complejas y diferentes.

El administrador puede ayudarlo a iniciar sesión en sus cuentas en línea automáticamente.

Solo debe recordar la contraseña maestra para acceder al administrador de contraseñas y administrar todas sus cuentas y contraseñas.

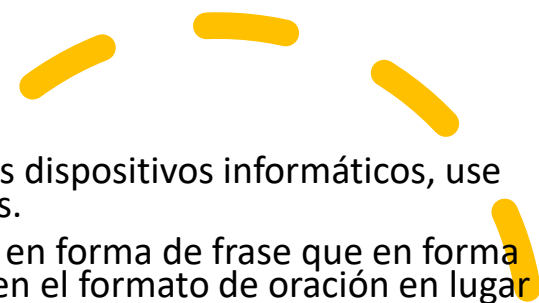
+

•

- Utilice contraseñas únicas para cada cuenta en línea

- **Consejos para elegir una buena contraseña:**

- No use palabras del diccionario o nombres en ningún idioma.
- No use errores ortográficos comunes de palabras del diccionario.
- No use nombres de equipos o cuentas.
- De ser posible, use caracteres especiales como ! @ # \$ % ^ & * ().
- Utilice una contraseña con diez o más caracteres.



Use una frase
en lugar de
una palabra
como
contraseña.

- Para evitar el acceso físico no autorizado a los dispositivos informáticos, use frases en lugar de palabras como contraseñas.
 - Es más fácil crear una contraseña larga en forma de frase que en forma de palabra porque generalmente está en el formato de oración en lugar de palabra.
 - Una longitud mayor hace que las frases sean menos vulnerables a los ataques de fuerza bruta o de diccionario.
 - Además, una frase puede ser más fácil de recordar, especialmente si debe cambiar de contraseña con frecuencia. Aquí se incluyen algunas sugerencias para elegir buenas contraseñas o frases:

Sugerencias para elegir una buena frase:

- Elija una oración que signifique algo para usted.
- Agregue caracteres especiales, como ! @ # \$ % ^ & * ().
- Mientras más larga, mejor.
- Evite oraciones comunes o famosas, por ejemplo, letras de una canción popular.
- Recientemente, el Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos publicó requisitos de contraseña mejorados. Las normas del NIST están destinadas a aplicaciones del gobierno, pero también pueden servir como normas para otras.
 - Las nuevas pautas tienen como objetivo proporcionar una mejor experiencia del usuario y poner la responsabilidad de comprobación del usuario en los proveedores.

Resumen de las nuevas pautas:

Esta debe tener una longitud mínima de 8 caracteres, pero no más de 64 caracteres.

No utilice contraseñas comunes ni que se puedan adivinar con facilidad; por ejemplo, contraseña, abc123.

No hay reglas de composición, como el tener que incluir números y letras mayúsculas y minúsculas.

Mejore la precisión de escritura permitiendo que el usuario vea la contraseña mientras la escribe.

Se permiten todos los caracteres de impresión y espacios.

Sin pistas de contraseña.

Sin fecha de caducidad periódica o arbitraria de la contraseña.

Sin autenticación basada en conocimientos, tales como información de preguntas secretas compartidas, datos de marketing, historial de transacciones.

Haga clic [aquí](#) para obtener más información sobre el requisito de contraseña mejorado del NIST.

Aunque el acceso a sus computadoras y dispositivos de red sea seguro, también es importante proteger y preservar sus datos

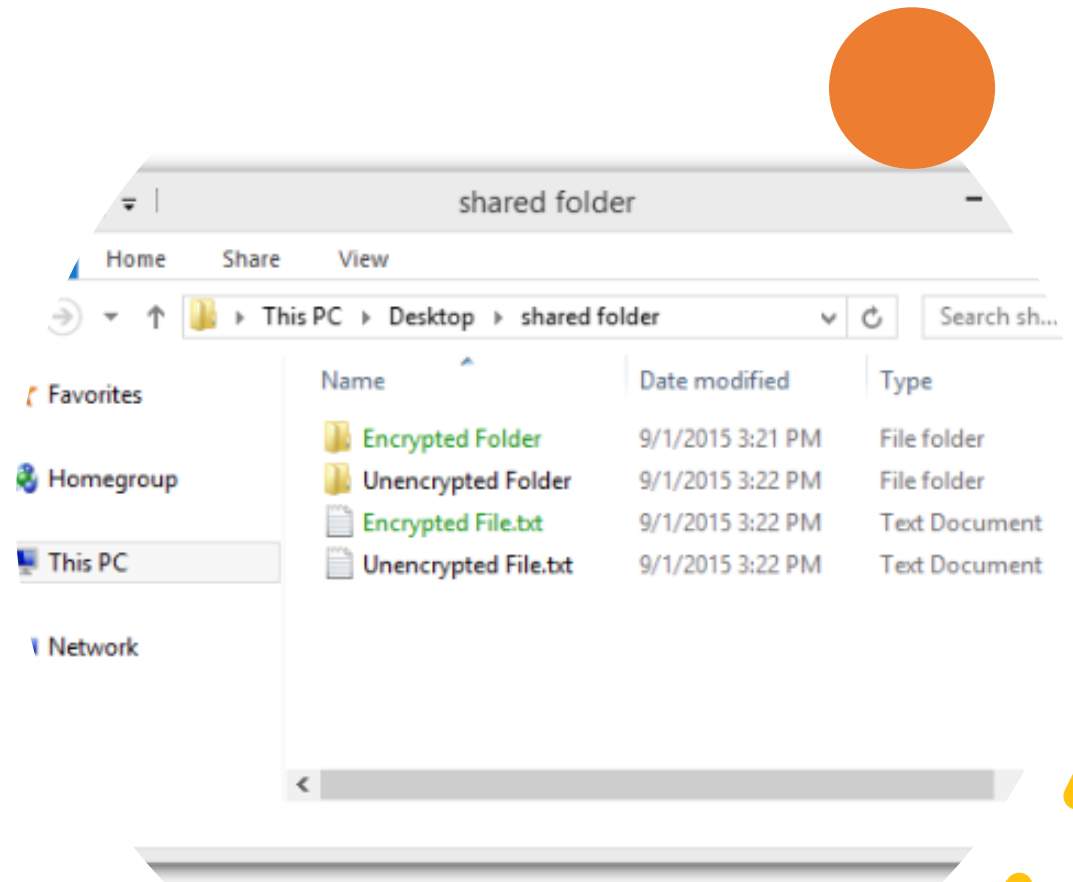
Laboratorio: crear y almacenar contraseñas seguras

En esta práctica de laboratorio, explorará los conceptos para crear contraseñas seguras y cómo guardarlas con protección.

Laboratorio: crear y almacenar
contraseñas seguras

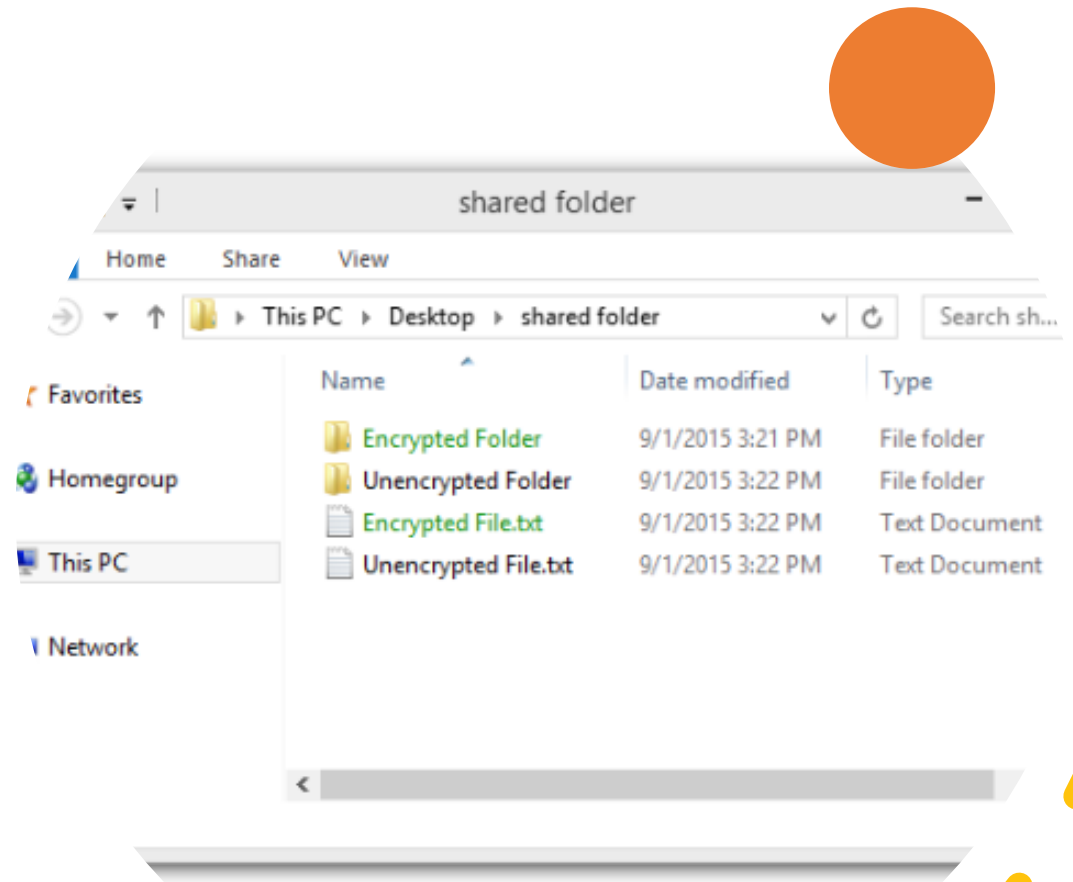
Encripte sus datos

- Sus datos siempre deben estar encriptados.
 - Es posible que piense que no tiene secretos ni nada que ocultar, ¿por qué usar la encriptación? Quizás cree que nadie desea sus datos. Muy probablemente, esto no es cierto.
- ¿Está listo para mostrar todas sus fotos y documentos a extraños?
 - ¿Está listo para compartir información financiera almacenada en su computadora con sus amigos?
 - ¿Desea divulgar sus correos electrónicos y las contraseñas de sus cuentas al público en general?
- Esto puede ser incluso más problemático si una aplicación maliciosa infecta su computadora o dispositivo móvil y le roba información potencialmente valiosa, como números de cuenta, contraseñas y otros documentos oficiales.
 - Dicho tipo de información puede generar robos de identidad, fraude o rescates.
 - Los delincuentes pueden decidir simplemente encriptar sus datos y hacer que sean inutilizables hasta que la extorsión se liquide.

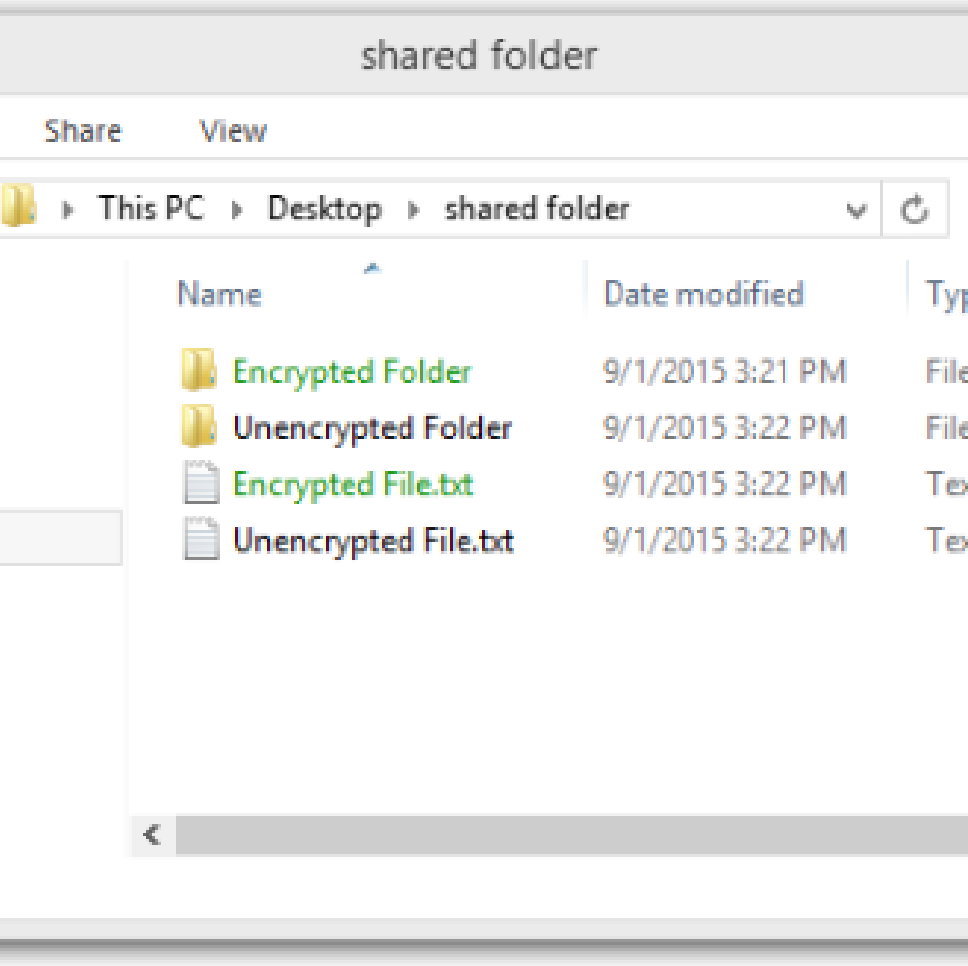


Encripte sus datos

- ¿Qué es la encriptación?
 - La encriptación es el proceso de conversión de la información a un formato que una parte no autorizada no puede leer.
 - Solo una persona de confianza autorizada con la contraseña o clave secreta puede descifrar los datos y acceder a ellos en su formato original.
 - La encriptación en sí misma no evita que una persona intercepte los datos.
 - La encriptación solo puede evitar que una persona no autorizada vea o acceda al contenido.
- Se utilizan programas de software para encriptar archivos, carpetas e incluso unidades enteras.



Encripte sus datos



- Se utilizan programas de software para encriptar archivos, carpetas e incluso unidades enteras.
- El sistema de encriptación de archivos (EFS, Encrypting File System) es una característica de Windows que permite encriptar datos. El EFS está directamente vinculado a una cuenta de usuario determinada. Solo el usuario que cifró los datos puede acceder a estos una vez encriptados con el EFS. Para encriptar datos con EFS en todas las versiones de Windows, siga estos pasos:
- **Paso 1:** Seleccione uno o más archivos o carpetas.
- **Paso 2:** Haga clic derecho en los datos seleccionados y en **>Propiedades**.
- **Paso 3:** Haga clic en **Opciones avanzadas...**
- **Paso 4:** Seleccione la casilla de verificación **Encriptar contenido para proteger datos**.
- **Paso 5:** Las carpetas y los archivos encriptados con el EFS se muestran en verde, como se muestra en la ilustración.

Realice un respaldo de sus datos

- Su disco duro puede fallar. Su computadora portátil puede perderse.
- Pueden robar su teléfono.
- Quizá borró la versión original de un documento importante.
- Tener un respaldo puede evitar la pérdida de datos irreemplazables, como fotos familiares.
- Para hacer un respaldo correcto de los datos, necesitará una ubicación de almacenamiento adicional para los datos y deberá copiar los datos en dicha ubicación periódica y automáticamente.



Realice un respaldo de sus datos

- La ubicación adicional para los archivos de copia de seguridad puede estar en su red doméstica, una ubicación secundaria o la nube.
- Si almacena los respaldos de los datos de manera local, tendrá el control total de los datos.
- Puede decidir copiar todos sus datos en un dispositivo de almacenamiento conectado a la red (NAS), un disco duro externo simple o puede seleccionar solo algunas carpetas importantes para hacer un respaldo en unidades de memoria USB, CD/DVD o incluso cintas.
- En dicho escenario, es usted el propietario y es totalmente responsable del costo y el mantenimiento de los equipos del dispositivo de almacenamiento.
- Si contrata un servicio de almacenamiento en la nube, el costo depende de la cantidad de espacio de almacenamiento que necesita.
- Con un servicio de almacenamiento en la nube, como Amazon Web Services (AWS), tendrá acceso a sus datos de respaldo siempre que tenga acceso a su cuenta.
- Cuando contrata servicios de almacenamiento en línea, es posible que deba ser más selectivo respecto de los datos que respalda debido al costo del almacenamiento y las constantes transferencias de datos en línea.
- Uno de los beneficios de guardar un respaldo en una ubicación alternativa es que es seguro en caso de incendio, robo u otro desastre, excepto que falle el dispositivo de almacenamiento.



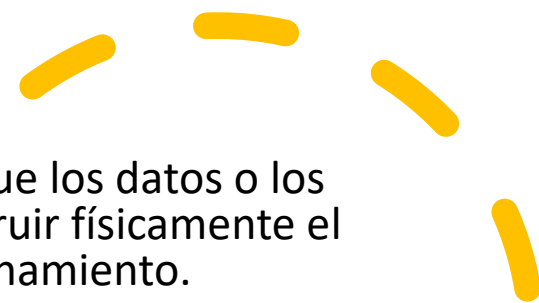
Laboratorio: crear respaldos de datos en un almacenamiento externo

En esta práctica de laboratorio, utilizará un disco externo y un disco remoto para respaldar sus datos.


Laboratorio: respaldar los
datos en un almacenamiento
externo

Eliminación de sus datos en forma permanente


- Cuando mueve un archivo a la papelera de reciclaje y lo elimina de manera permanente, no se puede acceder al archivo solo desde el sistema operativo.
 - Cualquier persona con las herramientas forenses adecuadas puede recuperar el archivo debido al rastro magnético que deja en el disco duro.
- Para borrar datos de modo que no sean recuperables, los datos deben sobrescribirse con unos y ceros varias veces.
 - Para evitar la recuperación de los archivos eliminados, es posible que deba utilizar herramientas diseñadas específicamente para hacerlo.
 - El programa SDelete de Microsoft (para Vista y versiones posteriores) reclama tener la capacidad de eliminar los archivos confidenciales por completo.
 - Shred para Linux y Secure Empty Trash para Mac OSX son algunas herramientas que aseguran proporcionar un servicio similar.




Eliminación de sus datos en forma permanente



- La única forma de estar seguros de que los datos o los archivos no son recuperables es destruir físicamente el disco duro o el dispositivo de almacenamiento.
 - Muchos delincuentes cometen la insensatez de pensar que sus archivos son impenetrables o irrecuperables.
- Además de almacenar datos en las unidades de disco duro locales, sus datos también pueden guardarse en línea en la nube.
 - Dichas copias también deberán eliminarse.
 - Tómese un momento para preguntarse:
 - ¿dónde están guardados mis datos?
 - ¿En una copia de seguridad en algún lado?
 - ¿Están encriptados?
 - Cuando deba eliminar sus datos o librarse de un disco duro o de una computadora, pregúntese:
 - ¿he protegido los datos para evitar que caigan en las manos incorrectas?



Laboratorio: ¿Quién posee sus datos?

- En este laboratorio explorará los acuerdos legales requeridos para usar diversos servicios en línea. También explorará algunas de las formas en que puede proteger sus datos.
- 

Autenticación de dos factores

Los servicios en línea más populares, como Google, Facebook, Twitter, LinkedIn, Apple y Microsoft, utilizan la autenticación de dos factores para agregar una capa adicional de seguridad para los inicios de sesión de la cuenta. Además del nombre de usuario y la contraseña, o un patrón o número de identificación personal (PIN), la autenticación de dos factores requiere un segundo token, por ejemplo:

Un objeto físico: una tarjeta de crédito, una tarjeta de cajero automático, un teléfono o un control.

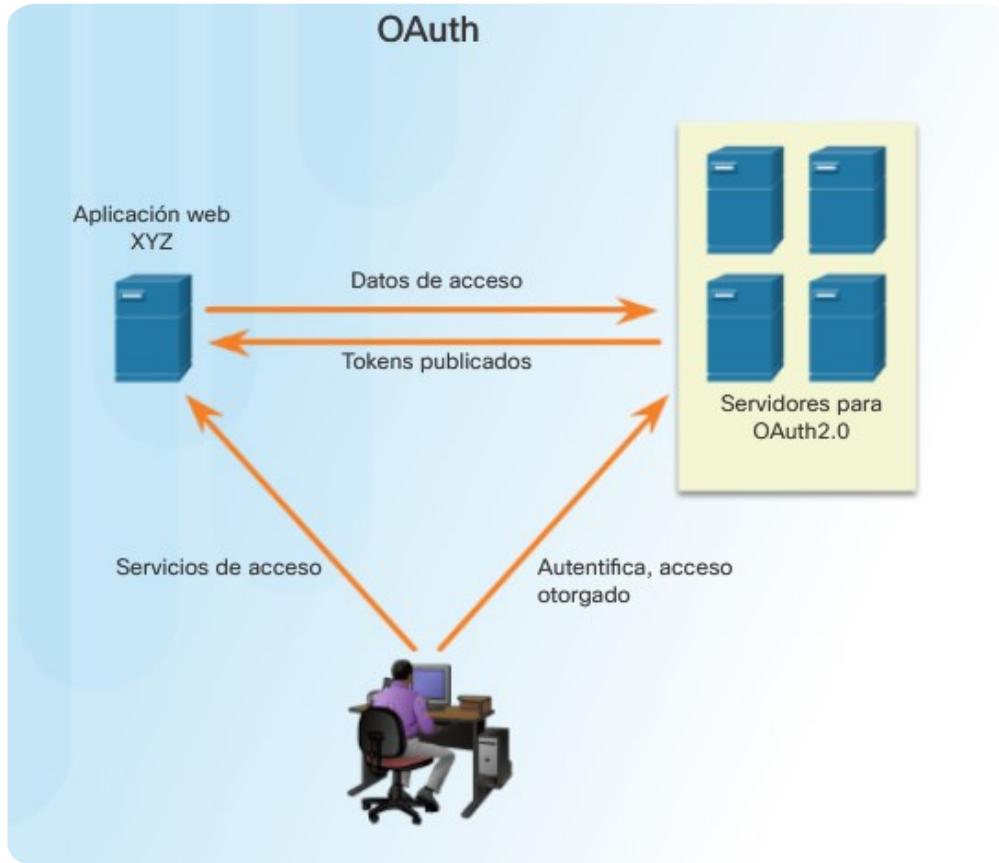
Escaneo biométrico: huellas digitales, impresión de la palma o reconocimiento de voz o de rostro.

Incluso con la autenticación de dos factores, los hackers aún pueden obtener acceso a sus cuentas en línea mediante ataques tales como suplantación de identidad, malware e ingeniería social.

Haga clic [aquí](#) para detectar si los sitios web que visita usan la autenticación de dos factores.



OAuth 2.0



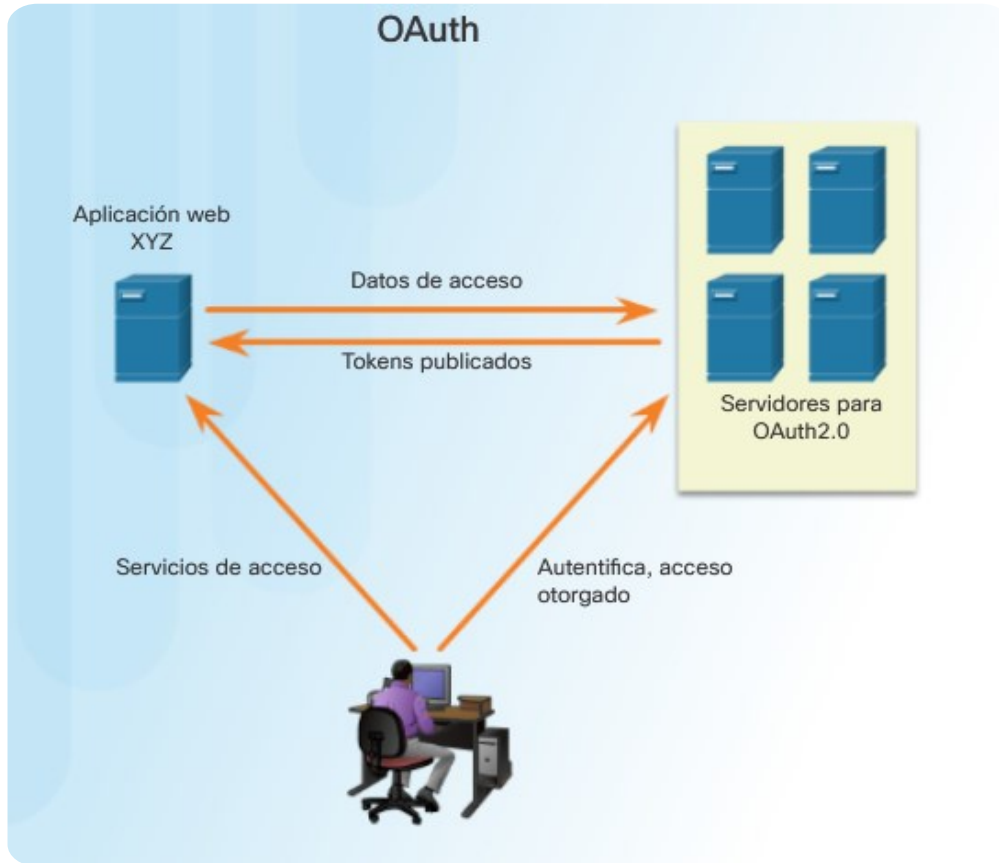
- Open Authorization (OAuth) es un protocolo de estándar abierto que permite que las credenciales de los usuarios finales tengan acceso a aplicaciones de terceros sin exponer las contraseñas de los usuarios.

- OAuth actúa como intermediario para decidir si los usuarios finales pueden acceder a aplicaciones de terceros.

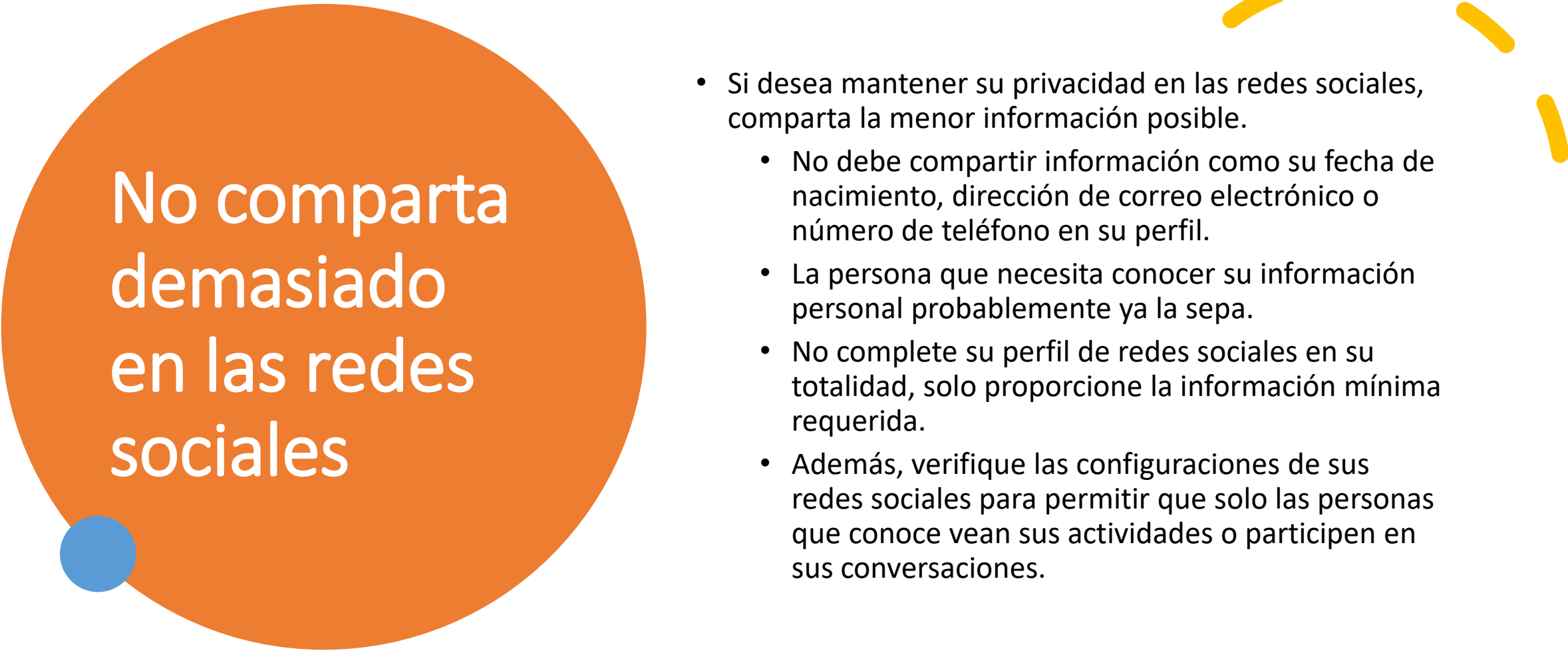
Por ejemplo, supongamos que desea acceder a la aplicación web XYZ y no tiene una cuenta de usuario para acceder a esta aplicación web.

- Sin embargo, XYZ tiene la opción de permitirle iniciar sesión con las credenciales de la red social ABC.
- Por lo que puede acceder al sitio web XYZ con el inicio de sesión de la red social ABC.

OAuth 2.0



- Para que esto funcione, la aplicación 'XYZ' se registra con 'ABC' y es una aplicación aprobada.
- Cuando accede a XYZ, utiliza sus credenciales de usuario para ABC. Luego XYZ solicita un token de acceso a ABC en su nombre.
- Ahora tiene acceso a XYZ. XYZ no tiene ninguna información sobre usted y sus credenciales de usuario; esta interacción es completamente transparente para el usuario.
- El uso de tokens secretos impide que una aplicación maliciosa obtenga su información y sus datos.



No comparta demasiado en las redes sociales


- Si desea mantener su privacidad en las redes sociales, comparta la menor información posible.
 - No debe compartir información como su fecha de nacimiento, dirección de correo electrónico o número de teléfono en su perfil.
 - La persona que necesita conocer su información personal probablemente ya la sepa.
 - No complete su perfil de redes sociales en su totalidad, solo proporcione la información mínima requerida.
 - Además, verifique las configuraciones de sus redes sociales para permitir que solo las personas que conoce vean sus actividades o participen en sus conversaciones.

No comparta demasiado en las redes sociales

Mientras más información personal comparta en línea, más fácil será para alguien crear un perfil sobre usted y aprovecharse de usted fuera de línea.


¿Alguna vez ha olvidado el nombre de usuario y la contraseña de una cuenta en línea?

- Las preguntas de seguridad tales como “¿Cuál es el nombre de su madre?” o “¿En qué ciudad nació?” supuestamente deben ayudar a mantener su cuenta protegida de intrusiones.
- Sin embargo, cualquier persona que desee acceder a sus cuentas puede buscar las respuestas en Internet.
- Puede responder estas preguntas con información falsa, siempre que recuerde las respuestas falsas.
- Si tiene un problema para recordarlas, puede usar el administrador de contraseñas para que las administre.





Privacidad del correo electrónico y el navegador web

- Cada día, millones de mensajes de correo electrónico se utilizan para comunicarse con amigos y realizar negocios.
- El correo electrónico es una manera conveniente de comunicarse rápidamente.
- Cuando envía un correo electrónico, es similar a enviar un mensaje mediante una tarjeta postal.
- El mensaje de la tarjeta postal se transmite a plena vista de cualquier persona que pueda observarlo; el mensaje de correo electrónico se transmite en texto sin formato y es legible para cualquier persona que tenga acceso.
- Estas comunicaciones además pasan por diferentes servidores en la ruta hacia su destino.
- Incluso si borra los mensajes de correo electrónico, los mensajes pueden archivarse en los servidores de correo durante algún tiempo.




Privacidad del correo electrónico y el navegador web

- Cualquier persona con acceso físico a su computadora o a su router puede ver qué sitios web ha visitado con el historial del navegador web, el caché y posiblemente los archivos de registro.
 - Este problema puede minimizarse habilitando el modo de navegación privada en el navegador web.
 - La mayoría de los exploradores web populares tienen un nombre propio para el modo de navegación privada:
 - **Microsoft Internet Explorer:** InPrivate
 - **Google Chrome:** Incognito
 - **Mozilla Firefox:** ventana privada/pestaña privada
 - **Safari:** navegación privada
 - Al utilizar el modo privado, se deshabilitan las cookies y los archivos temporales de Internet y el historial de exploración se eliminan después de cerrar la ventana o el programa.
- 



Privacidad del correo electrónico y el navegador web

- Mantener su historial de exploración de Internet privado puede impedir que otros recopilen información sobre sus actividades en línea y lo tiente para comprar algo con publicidad dirigida.
 - Incluso con la navegación privada habilitada y las cookies desactivadas, las empresas desarrollan diferentes maneras de identificar usuarios para recopilar información y seguir el comportamiento de los usuarios.
 - Por ejemplo, los dispositivos intermediarios, como los routers, pueden tener información sobre el historial de navegación web del usuario.
 - En última instancia, es su responsabilidad proteger sus datos, su identidad y sus dispositivos informáticos.
 - Cuando envía un correo electrónico, ¿debe incluir su historial médico?
 - La próxima vez que busque en Internet, ¿será segura su transmisión?
 - Simplemente algunas precauciones pueden ahorrarle problemas en el futuro.
- 



Laboratorio: descubra su propio comportamiento riesgoso en línea

- En esta práctica de laboratorio, identificará comportamientos riesgosos en línea y explorará algunas sugerencias sobre cómo aumentar la seguridad en línea.
- [Laboratorio: descubrir su propio comportamiento riesgoso en línea](#)

Capítulo 3: Protección de sus datos y de su seguridad

Este capítulo se centró en sus dispositivos y sus datos personales. Incluyó sugerencias para proteger sus dispositivos, crear contraseñas seguras y usar redes inalámbricas de manera segura. Cubrió los respaldos de datos, el almacenamiento de datos y la eliminación de datos de manera permanente.

Se analizaron técnicas de autenticación para ayudarlo a mantener sus datos seguros. Cubrió brevemente cuán fácil es compartir demasiada información en las redes sociales y cómo evitar este riesgo de seguridad.

Si desea explorar más a fondo los conceptos de este capítulo, consulte la página [Actividades y recursos adicionales](#) en Recursos para los estudiantes.