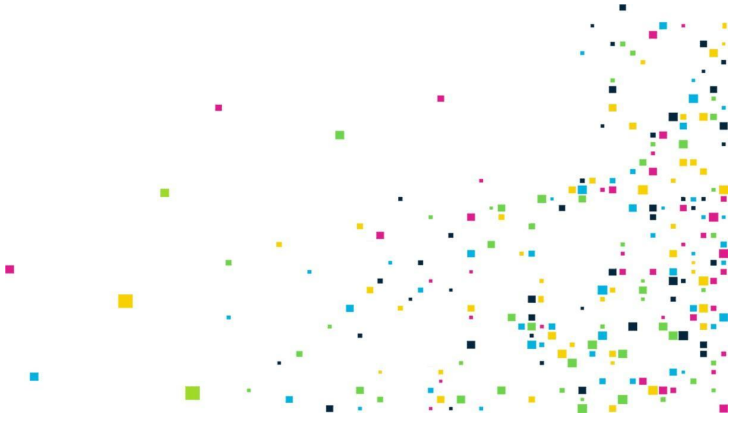
Orleans Digital Literacy Initiative

Actualizaciones y seguridad

Este módulo va a explicar como asegurar que su dispositivo esté actualizado y seguro. Hablaremos sobre ajustes de las actualizaciones, cuando uno debe de actualizar, y porque es importante tener una contraseña y programas de anti-virus y anti-malware

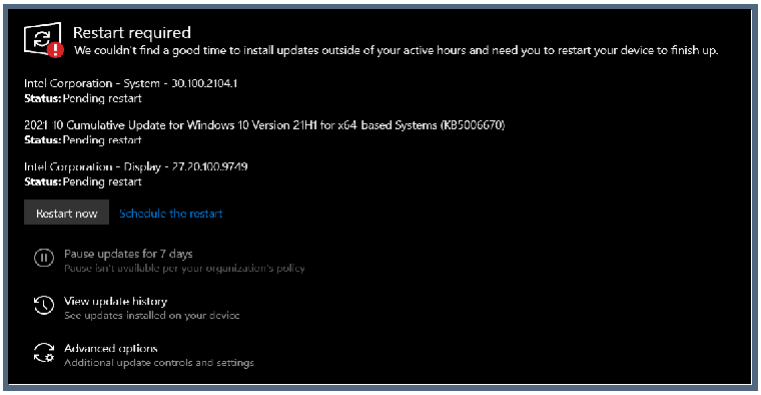


Porque actualizar?

El software está en constante evolución. Los programadores que crean el software en tu dispositivo siempre están trabajando para mejorar su software y hacerlo más fácil de usar y más seguro. Querrás poder actualizar su sistema operativo y software para mantenerlo actualizado con la última versión.

→ Un sistema operativo (OS) es un software de sistema que administra el hardware de la computadora, los recursos de software y proporciona servicios comunes para los programas de la computadora.

Ajustes de actualización



En el menú de 'Configuración de actualización,' puede ver qué actualizaciones están disponibles para su sistema operativo y si se necesita una actualización. Cuando actualice su computadora, necesitará reiniciarla. También puede optar por reiniciar su computadora ahora o programarla para reiniciar más tarde.

Imagen de las ajustes de actualización en Windows

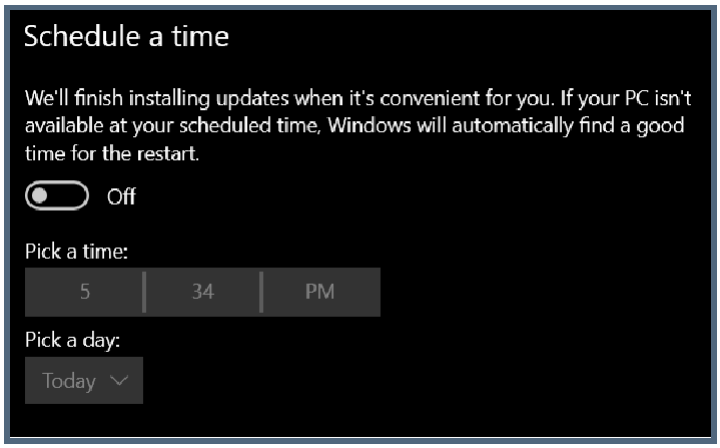
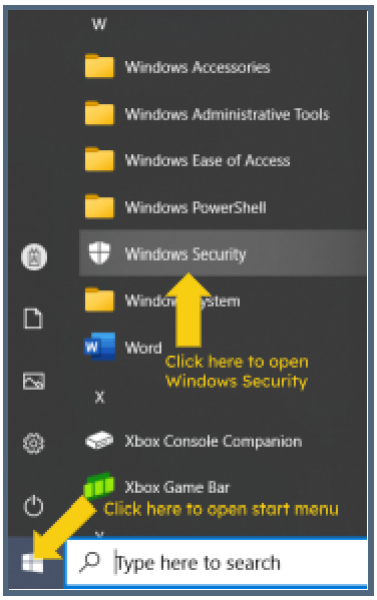


Imagen de como programar un tiempo para actualizar su computadora

Anti-virus y anti-malware

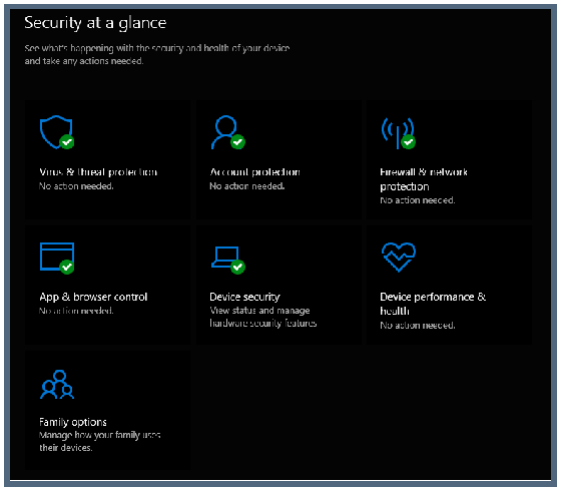
Los virus y malware son tipos de amenazas para la seguridad de su computadora.

Virus: Un tipo específico de malware informático que se autorreplica y se propaga a otras computadoras.
Antivirus: Software que escanea un dispositivo o una red para detectar amenazas de seguridad, alertarte y neutralizar código malicioso.
Malware: Software diseñado para hacer daño a un sistema informático, ya sea para tomar información, pedir rescate, deshabilitar o algo más.
Windows tiene una protección integrada contra el malware llamada Windows Security. Los sistemas operativos Mac y Chrome también tienen protecciones incorporadas. Puede encontrar Windows Security en el menú de inicio haciendo clic en el icono de Windows en la parte inferior derecha de tu pantalla de computadora.



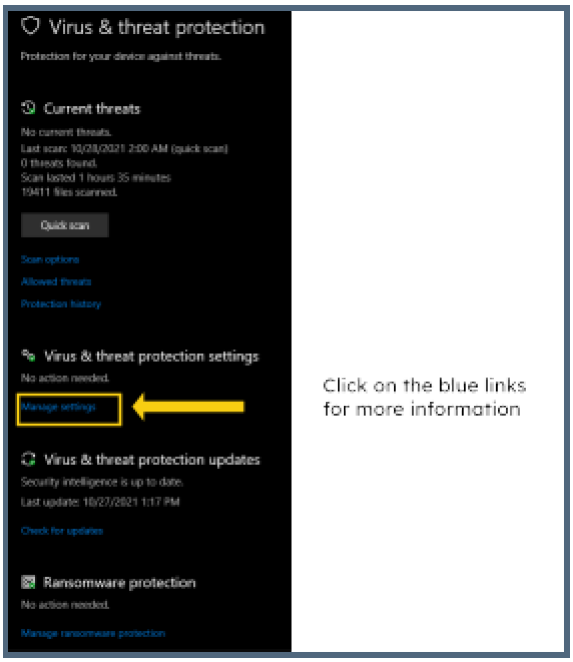
Acceder a Windows Security desde el menú de inicio

Dentro de Windows Security, tiene varias opciones para mantener su computadora segura. Desde el menú "Seguridad en un vistazo", puede obtener un rápido vistazo a la seguridad general. Puede saber si hay algún problema importante marcado con un símbolo amarillo o rojo junto al icono. Cuando todo funciona correctamente, los símbolos junto al icono serán marcas de verificación verdes, como en la imagen a continuación. Una marca roja o amarilla deberá abordarse para mantener la seguridad.



Menú de seguridad de Windows

Para Anti-Malware, lo principal es realizar controles/escaneos periódicos. La mayoría de las computadoras tienen software incorporado configurado para hacerlo automáticamente en segundo plano. También puede configurarlo en Seguridad de Windows haciendo clic en "configuración de protección contra virus y amenazas". Aquí podrá ver el estado del escaneo de protección y si se necesita alguna acción. Si necesita más información, puede hacer clic en los enlaces azules y aparecerá una página de información.



El menú de Protección contra Virus y Amenazas.

Seguridad del dispositivo

Aquí hay algunas formas en las que puede mantener seguro su dispositivo.

★ Tenga una contraseña o PIN.

★ NO deje su dispositivo en un lugar público.

★ NO deje contraseñas en su dispositivo.

★ Evite redes WiFi desconocidas.

★ Solo visite sitios web confiables.

★ Solo descargue archivos confiables.

★ NO comparta su dispositivo con alguien en quien no confíe.

Mantener sus cuentas seguras

Para mantener seguras tus cuentas, hay dos cosas principales que debes aprender: la seguridad de contraseñas y la autenticación de múltiples factores.

Seguridad de contraseñas

Tu contraseña es la primera línea de defensa para cualquiera de tus cuentas en línea o de computadora. Las contraseñas seguras son muy importantes para mantener tu seguridad en línea. Las contraseñas fáciles de adivinar o cortas facilitan el acceso de personas, especialmente aquellas con habilidades de hacking, a tus cuentas. Al practicar buenos hábitos de seguridad de contraseñas, puedes hacer que tus cuentas y la información almacenada en ellas sean más seguras.

Consejos para contraseñas:

Crea una contraseña única para cada cuenta que utilices.
Utiliza una mezcla aleatoria de números, letras y símbolos.
Usa un gestor de contraseñas para ayudarte a realizar un seguimiento de tus contraseñas únicas.
Solo proporciona tus contraseñas a sitios web apropiados (seguros).

Errores a evitar en contraseñas:

No utilices frases comunes o información personal (como el nombre de una mascota).
No escribas tus contraseñas.
No compartas tus contraseñas.
No utilices contraseñas cortas.
No utilices contraseñas que sean fáciles de adivinar.
No mantengas la misma contraseña durante mucho tiempo.
No almacenes tus contraseñas en un lugar donde puedan encontrarse fácilmente.

Ejemplos de contraseñas buenas y malas

Ejemplos de contraseñas malas	Ejemplos de contraseñas buenas
Contraseñas	@H76cxgV90$$jKTsk
Juan2021	IegtDL2021!
03-21-1990	P3aS0up4me
Wizzard22	nwso^d-scr23ap(hk3dh

Autenticación de múltiples factores

La autenticación de múltiples factores, también conocida como autenticación de dos factores, agrega una capa adicional de protección. La autenticación de múltiples factores puede proporcionar niveles de seguridad más altos cuando se combina con métodos de baja calidad (por ejemplo, una contraseña simple), ya que las personas con intenciones maliciosas no solo tendrían que conocer tu contraseña, sino también tener acceso a tu dispositivo para obtener el código de la aplicación de autenticación de múltiples factores o mensaje de texto. La autenticación de múltiples factores es ideal donde la seguridad es más importante que la facilidad de acceso. Nota: Cuando se te da la opción entre una contraseña o biometría, la biometría siempre es más segura que una contraseña muy difícil de adivinar.

La autenticación de múltiples factores es cuando se requieren varios factores para realizar una verificación exitosa de identidad. Una vez que haya ingresado correctamente tu contraseña en un sitio web, el sistema le enviará un código por mensaje de texto o pedirá que recupere un código de tu aplicación de autenticación. Luego se le pedirá que ingreses este código para finalizar el inicio de sesión en tu cuenta.

Tipos de autenticación de múltiples factores:

- ★ Código de correo electrónico
- ★ Código de texto
- ★ Código de llamada telefónica
- ★ Aplicaciones de autenticación

Si tiene la capacidad de utilizar la autenticación de múltiples factores, se recomienda encarecidamente que lo haga para agregar una capa adicional de seguridad.

Almacenamiento seguro de contraseñas con gestores de contraseñas

Un gestor de contraseñas almacena de manera segura sus contraseñas y registros, así como otra información que necesita mantener privada, pero acceder fácilmente. Algunos gestores de contraseñas populares son LastPass, 1Password o Dashlane. Los gestores de contraseñas tienen aplicaciones que puede descargar en su computadora o dispositivo móvil, y aplicaciones basadas en la web que puede acceder desde cualquier dispositivo. Tienen una variedad de planes gratuitos o de pago que puede adaptar a sus necesidades.

Es mejor evitar compartir las credenciales de inicio de sesión siempre que sea posible. Sin embargo, a veces compartir una cuenta dentro de su familia es inevitable. Ahí es donde los gestores de contraseñas pueden ser útiles. Algunos permiten poner varios usuarios en una cuenta familiar o empresarial, lo que le permite compartir de manera segura las contraseñas con una persona de confianza. Otros permiten invitar a un invitado para acceder solo a las contraseñas que desea confiarles. De cualquier manera, asegúrese de confiar en esta persona y de que no hay otra alternativa para compartir las mismas credenciales.


LastPass


1Password


Dashlane

Seguir estos consejos puede ayudar a mantenerlo a usted, sus cuentas y su información personal seguros.