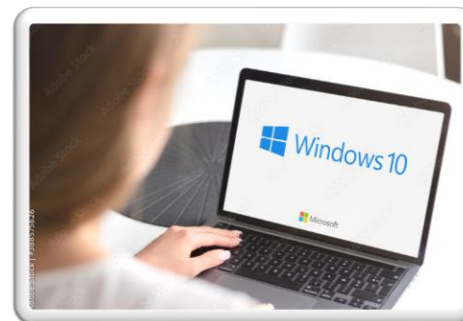




Cómo eliminar el malware de su PC con Windows

Paso 1: Ingrese al modo seguro.

- Antes de hacer algo, debe desconectar su PC de internet y no usarla hasta que esté listo para limpiar.
- Si cree que su PC puede tener una infección de *malware*, inicie su PC en el modo seguro de Microsoft.
- Para iniciar en el modo seguro de Windows, primero haga clic en el botón Inicio en Windows 10 y seleccione el botón de encendido como si fuera a reiniciar, pero no haga clic en nada.
- A continuación, mantenga presionada la tecla **Mayúscula** y haga clic en **Reiniciar**.
- Cuando aparezca el menú de pantalla completa, seleccione Solución de problemas, luego **Opciones avanzadas**, luego **Configuración de inicio**.
- En la siguiente ventana, haga clic en **Reiniciar** y espere a que aparezca la siguiente pantalla (solo quédese con nosotros aquí, sabemos que esto es largo).
- A continuación, verá un menú con opciones de inicio numeradas; seleccione el número **4**, que es **Modo seguro**.



388575626



Paso 2: Eliminar archivos temporales.

- Archivos temporales: Puede usar la utilidad de limpieza de disco integrada de Windows 10 para eliminar archivos temporales innecesarios de su sistema.
- Ahora que está en modo seguro, querrá ejecutar un análisis de virus.
- Pero antes de hacer eso, elimine sus archivos temporales.
- Hacer esto puede acelerar el análisis de virus, liberar espacio en el disco e incluso deshacerse de algunos programas maliciosos.
- Para usar la utilidad Liberador de espacio en disco incluida con Windows 10, simplemente escriba "Liberador de espacio en disco" en la barra de búsqueda o después de presionar el botón Inicio y seleccione la herramienta que aparece llamada "Liberador de espacio en disco".



519958905

Paso 3: Descargue los escáneres de *malware*.

- Ahora está listo para que un escáner de *malware* haga su trabajo y, afortunadamente, ejecutar un escáner es suficiente para eliminar la mayoría de las infecciones estándar.
- Si ya tenía un programa antivirus activo en su computadora, debe usar un escáner diferente para esta verificación de malware, ya que es posible que su *software* antivirus actual no haya detectado el *malware*.



	<ul style="list-style-type: none">➤ Recuerde, ningún programa antivirus puede detectar el 100 por ciento de los millones de tipos y variantes de <i>malware</i>.➤ Probablemente esté más familiarizado con los programas antivirus en tiempo real, que se ejecutan en segundo plano y vigilan constantemente el <i>malware</i>.➤ Otra opción es un escáner bajo demanda, que busca infecciones de <i>malware</i> cuando abre el programa manualmente y ejecuta un escaneo.➤ Solo debe tener un programa antivirus en tiempo real instalado a la vez, pero puede tener muchos escáneres bajo demanda instalado para ejecutar escaneos con múltiples programas, asegurando así que si un programa pierde algo, otro diferente podría encontrarlo.➤ Si cree que su PC está infectado, le recomendamos que primero use un escáner bajo demanda y luego haga un seguimiento completo con su programa antivirus en tiempo real.➤ Entre los escáneres bajo demanda gratuitos (y de alta calidad) disponibles se encuentran Bitdefender Free Edition, Kaspersky Virus Removal Tool, Malwarebytes, Malicious Software Removal Tool de Microsoft, Avast y Superantispyware.	
--	--	--



Paso 4: Ejecute un escaneo con Malwarebytes.

- Con fines ilustrativos, describiremos cómo usar el escáner bajo demanda de Malwarebytes.
- Para comenzar, descárguelo.
- Si se desconectó de internet por razones de seguridad cuando sospechó por primera vez que podría estar infectado, vuelva a conectarse para poder descargar, instalar y actualizar Malwarebytes.
- Luego, desconéctese de Internet nuevamente antes de comenzar el escaneo real.
- Si no puede acceder a Internet o no puede descargar Malwarebytes en la computadora infectada, descárguelo en otra computadora, guárdelo en una unidad flash USB y lleve la unidad flash a la computadora infectada.
- Después de descargar Malwarebytes, ejecute el archivo de instalación y siga al asistente para instalar el programa.
- Una vez que se abre el programa, se activará automáticamente una versión de prueba de la versión paga que permite el escaneo en tiempo real.
- Sin embargo, no se le cobrará una vez que finalice la prueba de manera predeterminada
- El programa vuelve a la versión gratuita estándar en 14 días.
- Mientras tanto, puede desactivar el análisis en tiempo real durante esas dos semanas si lo prefiere
- Para ejecutar un escaneo, cambie de la pestaña Tablero a la pestaña **Escanear**. Mantenga seleccionada la opción de análisis predeterminada



163440459





	<p>("Análisis de amenazas") y haga clic en el botón Iniciar análisis.</p> <ul style="list-style-type: none">➤ Debería buscar actualizaciones antes de ejecutar el análisis, pero asegúrese de que eso suceda antes de continuar.➤ Aunque ofrece una opción de escaneo personalizado, Malwarebytes recomienda que primero realice el escaneo de amenazas, ya que ese escaneo generalmente encuentra todas las infecciones de todos modos.➤ Dependiendo de su computadora, el escaneo rápido puede demorar entre 5 y 20 minutos, mientras que un escaneo personalizado puede demorar entre 30 y 60 minutos o más. Mientras Malwarebytes está escaneando, puede ver cuántos archivos u objetos el software ya ha escaneado y cuántos de esos archivos ha identificado como malware o infectados por malware.➤ Si Malwarebytes desaparece automáticamente después de que comienza a escanear y no se vuelve a abrir, probablemente tenga un <i>rootkits</i> u otra infección profunda que elimine automáticamente los escáneres para evitar que lo eliminen.➤ Aunque puede probar algunos trucos para evitar esta técnica maliciosa, es mejor reinstalar Windows después de hacer una copia de seguridad de sus archivos (como se explica más adelante), en vista del tiempo y el esfuerzo que tendrá que invertir para vencer al <i>malware</i>.	
--	--	--



	<ul style="list-style-type: none">➤ Una vez que se complete el escaneo, <i>Malwarebytes</i> le mostrará los resultados.➤ Si el <i>software</i> le da a su sistema un certificado de buena salud, pero aún cree que su sistema ha adquirido algún malware, considere ejecutar un escaneo personalizado con <i>Malwarebytes</i> y pruebe los otros escáneres mencionados anteriormente.➤ Si <i>Malwarebytes</i> encuentra infecciones, le mostrará cuáles son cuando se complete el análisis.➤ Haga clic en el botón Eliminar seleccionados en la parte inferior izquierda para deshacerse de las infecciones especificadas. <i>Malwarebytes</i> también puede solicitarle que reinicie su PC para completar el proceso de eliminación, lo cual debe hacer.➤ Si sus problemas persisten después de ejecutar el análisis de amenazas y este encontró y eliminó archivos no deseados, considere ejecutar un análisis completo con <i>Malwarebytes</i> y los otros analizadores mencionados anteriormente.➤ Si parece que el malware ha desaparecido, ejecute un análisis completo con su programa antivirus en tiempo real para confirmar ese resultado.	
--	---	--



<p>Paso 5: Repare su navegador web.</p>	<ul style="list-style-type: none"> ➤ Las infecciones de <i>malware</i> pueden dañar los archivos del sistema de Windows y otras configuraciones. Un rasgo común del malware es modificar la página de inicio de su navegador web para volver a infectar la PC, mostrar anuncios, evitar la navegación y, en general, molestarlo. ➤ Antes de iniciar su navegador web, verifique su página de inicio y la configuración de conexión. Simplemente vaya a la ventana de configuración de su navegador para verificar la configuración de su página de inicio. ➤ Configuración de la página de inicio de IE Asegúrese de que la configuración de su página de inicio sea correcta antes de iniciar Internet Explorer. 	 <p>38109240</p>
<p>Paso 6: Recupere archivos si Windows está dañado.</p>	<ul style="list-style-type: none"> ➤ Si parece que no puede eliminar el <i>malware</i> o si Windows no funciona correctamente, es posible que deba reinstalar Windows. ➤ Pero antes de limpiar su disco duro, copie todos sus archivos a una unidad USB o flash externa. Si revisa su correo electrónico con un programa cliente (como Outlook o Windows Mail), asegúrese de exportar sus configuraciones y mensajes para guardarlos. ➤ También debe hacer una copia de seguridad de los controladores de su dispositivo con una utilidad como Double Driver, en caso de que ya no tenga los discos de controladores o no quiera descargarlos todos 	 <p>453449609</p>



	<p>nuevamente. Recuerde, no puede guardar los programas instalados.</p> <ul style="list-style-type: none">➤ En su lugar, deberá reinstalar los programas desde los discos o volver a descargarlos.➤ Si Windows no se inicia o no funciona lo suficientemente bien como para permitirle hacer una copia de seguridad de sus archivos, puede crear y usar un Live CD, como Hiren's Boot CD (HBCD), para acceder a sus archivos.➤ Una vez que haya realizado una copia de seguridad de todo, reinstale Windows desde el disco que vino con su PC, descargando la imagen de instalación de Microsoft o usando la opción de restauración de fábrica de su PC, si tiene una.➤ Para una restauración de fábrica, normalmente debe presionar una determinada tecla en el teclado durante el proceso de arranque para que se inicie el procedimiento de restauración, y su PC debe decirle qué tecla presionar en los primeros segundos después de encenderlo.➤ Si no hay instrucciones en pantalla, consulte su manual, el fabricante o Google.➤ Siempre asegúrese de tener un programa antivirus en tiempo real ejecutándose en su PC y asegúrese de que este programa esté siempre actualizado.➤ Si no desea gastar dinero en suscripciones anuales, puede elegir uno de los muchos programas gratuitos que brindan una protección adecuada, como Avira Antivirus Free Edition y Bitdefender Antivirus Free Edition.	
--	--	--



	<ul style="list-style-type: none">➤ Si prefiere un programa AV más sólido, le recomendamos Norton Security Premium; consulte nuestro resumen de los mejores programas antivirus para obtener más información.➤ Además de instalar el software antivirus tradicional, puede considerar usar el servicio gratuito OpenDNS para ayudar a bloquear sitios peligrosos.➤ Y si frecuenta sitios sospechosos que podrían infectar su PC con malware, considere ejecutar su navegador web en modo <i>sandbox</i> para evitar que cualquier malware descargado dañe su sistema.➤ Algunos programas antivirus, como Cómodo, ofrecen funciones de <i>sandboxing</i>, o puede obtenerlas a través de un programa gratuito de terceros, como Sandboxie.➤ Cuando crea que ha eliminado las infecciones de malware de su PC, vuelva a verificar sus cuentas en línea, incluidas las de su banco, correo electrónico y sitios de redes sociales. Busque actividad sospechosa y cambie sus contraseñas, ya que algunos programas maliciosos pueden capturar sus contraseñas.➤ Si tiene un sistema de respaldo que respalda automáticamente sus archivos o sistema, considere ejecutar análisis de virus en los respaldos para confirmar que no guardaron infecciones sin darse cuenta.➤ Si los análisis de virus no son factibles, como es el caso de los sistemas en línea, ya que generalmente solo escucharán una unidad conectada a su PC o solo la unidad C, considere eliminar sus copias de seguridad antiguas y restablecer el software para comenzar a	
--	---	--



	guardar nuevas copias de seguridad que son esperemos que libre de infecciones.	
--	---	--