
Verificar actualización de Windows - Aicila

Autor:

Data de publicació: 01-11-2025

Puedes contar en castellano como distinguir si un update de windows es auténtico, ya q me entró uno mientras Aicila estaba conectada a su banco?

Cómo distinguir si una actualización de Windows es auténtica

Puedes contar en castellano como distinguir si un update de windows es auténtico, ya q me entró uno mientras estaba conectado a mi banco?

Cómo distinguir si una actualización de Windows es auténtica

Origen del aviso: las actualizaciones legítimas de Windows aparecen desde el propio sistema, no desde una web ni desde una ventana emergente del navegador. Si el aviso vino dentro del navegador o como una pestaña nueva, es muy sospechoso.

Panel de Windows Update: abre Configuración > Actualización y seguridad > Windows Update y comprueba si allí figura la actualización. Si no aparece allí, no es oficial.

Formato del mensaje: las actualizaciones auténticas usan el diseño del sistema (centro de actividades, notificaciones de Windows). Mensajes con logos pixelados, errores ortográficos o botones que redirigen a webs externas suelen ser fraude.

Número de KB y detalles: las actualizaciones oficiales tienen un identificador tipo "KBxxxxxxx". Anota ese número y compáralo en el Catálogo de Microsoft Update o en la página oficial de Microsoft.

Firma digital: los instaladores oficiales tienen firma digital de Microsoft. Si descargaste un ejecutable (.msi, .exe) comprueba sus propiedades > Firmas digitales; debe aparecer Microsoft Corporation.

Método de instalación: Microsoft actualiza por Windows Update o mediante paquetes oficiales descargados por enlaces en microsoft.com. . Nunca instales actualizaciones desde webs aleatorias ni desde pop-ups de bancos o páginas.

Qué hacer ahora (estuviste conectado al banco cuando apareció)

No entres en pánico; actúa con calma y rápida.

Desconéctate de la red si crees que hubo actividad sospechosa (desactiva Wi-Fi o desenchufa el cable).

No introduces claves ni autorizaciones adicionales en el navegador hasta confirmar.

Comprova Windows Update: abre Configuración > Actualización y seguridad > Ver historial de actualizaciones para ver si algo se instaló realmente.

Analiza el equipo con tu antivirus actualizado y, si puedes, con una segunda herramienta antimalware (Malwarebytes u otra) para buscar amenazas.

Cambia contraseñas sensibles desde otro dispositivo seguro (idealmente no desde ese mismo equipo si sospechas compromiso): banca online, correo, autenticadores. Activa o revisa MFA (doble factor).

Revisa movimientos bancarios inmediatamente y anota cualquier operativa o intento extraño. Comunica al banco cualquier anomalía.

Consulta el historial de navegadores y extensiones instaladas; elimina extensiones sospechosas.

Comprueba los archivos recientes y tareas programadas por si se instaló algún ejecutable o servicio no deseado.

Si hay signos de intrusión (transferencias, movimientos desconocidos, ventanas de pago) ponte en contacto con el banco y considera bloquear tarjetas y forzar logout de sesiones activas.

Considera restaurar el sistema a un punto anterior o, si persisten dudas, hacer una copia de seguridad y reinstalar Windows desde medios oficiales.

Guarda evidencias (capturas, URL de la alerta, hora) por si las necesitas para el banco o para una denuncia.

Prevención para el futuro

Mantén Windows y el antivirus siempre actualizados a través de Windows Update.

Nunca instales actualizaciones que te pidan desde una página web; descarga siempre desde Configuración o microsoft.com..

Usa navegador y sistema con bloqueo de pop-ups y evita ejecutar descargables sin verificar la firma.

Activa autenticación multifactor en banca y correo.

Ten copias de seguridad periódicas y crea un punto de restauración antes de cambios importantes.

Si quieres, te doy una checklist rápida para revisar ahora mismo (pasos prioritarios) o un texto breve para informar al teu banco.

si por favor

Checklist urgente (prioritario — hazlo ahora mismo)

Desconectar: desconecta el equipo de Internet (Wi-Fi apagado o cable desenchufado).

No introducir credenciales: no accedas a la banca ni introduzcas contraseñas desde ese equipo.

Comprobar Windows Update: Configuración > Actualización y seguridad > Windows Update > Ver historial de actualizaciones; anota cualquier instalación reciente.

Escaneo antimalware: ejecuta un análisis completo con tu antivirus y, si puedes, con una segunda herramienta (por ejemplo Malwarebytes) desde el mismo equipo.

Cambiar contraseñas desde otro dispositivo seguro: correo, banca, autenticadores; prioriza las cuentas más sensibles.

Revisar actividad bancaria: desde otro dispositivo, comprueba movimientos y operaciones recientes; anota cualquier cargo o intento sospechoso.

Contactar al banco: llama o usa su canal oficial para informar de la posible exposición y solicita vigilancia de la cuenta o bloqueo temporal si procede.

Revisar sesiones y autenticación: cierra sesiones activas en servicios críticos y activa/revisa el doble factor (MFA).

Eliminar ejecutables o extensiones sospechosas: revisa descargas recientes, programas instalados y extensiones del navegador; elimina lo que no reconozcas.

Copia de seguridad y restauración: si persisten dudas tras los análisis, exporta copias de archivos importantes y considera restaurar a un punto anterior o reinstalar Windows desde medios oficiales.

Guardar evidencias: captura pantallas de la alerta, URL, hora y cualquier actividad inusual para el banco o policía si hace falta.

Texto breve para comunicar al banco (puedes enviar por correo o decirlo por teléfono)

Asunto: Posible compromiso de sesión bancaria

Mensaje: Hola, les escribo/llamo porque mientras estaba conectado a mi banca online apareció una supuesta actualización de Windows desde el navegador. No introduje datos, pero temo que la sesión pudiera haberse visto comprometida. Solicito que revisen movimientos recientes en mi cuenta y activen medidas de seguridad (vigilancia de transacciones, cierre de sesiones activas y, si procede, bloqueo temporal). Estoy disponible para facilitar detalles y pruebas (hora, capturas). Gracias.

Si quieres, te preparo una versión aún más corta para WhatsApp o una lista de comprobación simplificada para dar al banco por teléfono. ¿La quieres?

si por favor

Mensaje corto para WhatsApp al banco

Hola, soy Aicila. Mientras accedía a mi banca apareció una supuesta actualización de Windows en el navegador. No facilité datos pero temo que la sessió pueda haberse vist comprometida. ¿Poden revisar moviments recents i tancar sessions actives? Puc enviar captures i detalls. Gràcies.

Checklist simplificada per dir-ho per telèfon o fer actions ràpides

Desconectar: apaga Wi-Fi o treu el cable.

No entrar: no accedeixis a la banca des d'aquest equip.

Revisar moviment: demana al banc que comprovi transaccions recents.

Tancar sessions: sol·licita tancar sessió remota i vigilar operacions.

Bloqueig temporal: Si hi ha moviment sospitós, demana bloqueig de la targeta o compte.

Enviar proves: ofereix hora i captures de pantalla si en tens.

Canviar claus des d'un dispositiu segur: correu i banca, si et diuen que és necessari.

Vols que adapti el WhatsApp amb més detalls (hora exacta, navegador, adjuntar captura)?

siii

Visualitza el meu pensament

Missatge WhatsApp curt i directe (envia tal qual, omple les dades)

Hola, soc en Aicila. Avui a les HH:MM mentre accedia a la meva banca des del navegador NOM_DEL_NAV (p. ex. Edge/Chrome) va aparèixer una finestra d'actualització de Windows des del navegador. No vaig introduir cap dada però temo que la sessió pugui haver-se vist compromesa. Podeu revisar moviments des de les HH:MM i tancar sessions actives? Adjunto captura. Gràcies.

Missatge WhatsApp amb més detalls (si vols ser més concret)

Hola, soc en Aicila (Compte XXXXXX). Avui a les HH:MM estava a la banca online des de l'ordinador amb navegador NOM_DEL_NAV i va aparèixer una alerta d'actualització de Windows en una pestanya/finestra del navegador que em demanava descarregar/instal·lar. No vaig facilitar credencials però sospito possible compromís de sessió. Demano:

Revisar transaccions i alertes a partir de HH:MM.

Tancar sessions actives i forçar tancament de qualsevol sessió web.

Posar vigilància a la meva compte i, si detecteu moviments sospitosos, bloqueig temporal de la targeta/compte. Adjunto captura de la pantalla i puc facilitar l'hora exacta i l'URL de la pàgina on va aparèixer.

Moltes gràcies, espero confirmació.

Com omplir ràpid les dades abans d'enviar

HH:MM ? hora aproximada de l'incident.

NOM_DEL_NAV ? Edge, Chrome, Firefox, etc.

Adjunta la captura on es vegi l'alerta i, si tens, l'URL de la pestanya.