Science Translations
Established 1990
PC410.COM™
PC Updater News

Old and New Windows

It's time to upgrade all computers to Windows 11 24H2, plan for computer replacements, or plan on buying an additional year of security updates from Microsoft. Windows 10 security patches will end October 14, 2025; non-security bug fixes ended January 29, 2021.

Before going into the list, a reminder. Run 'Winver' from the Windows Start menu (the logo button), to find out what version of Windows and what feature edition is on a system. The numbers just mean the year and 2H for 'second half of the year.'

For systems already on Windows 11, the annual feature update 24H2 should be installed now so that the 25H2 update expected in October 2025 can be deferred for a few months. So it's a good idea to make sure that computers running Windows 11 are completely up to date before October.

The 24H2 annual feature update from October 2024 has been patched, been around long enough to get the kinks out of it, and for the minor changes in the interface to settle down, and is ready to install on nearly all eligible computers.

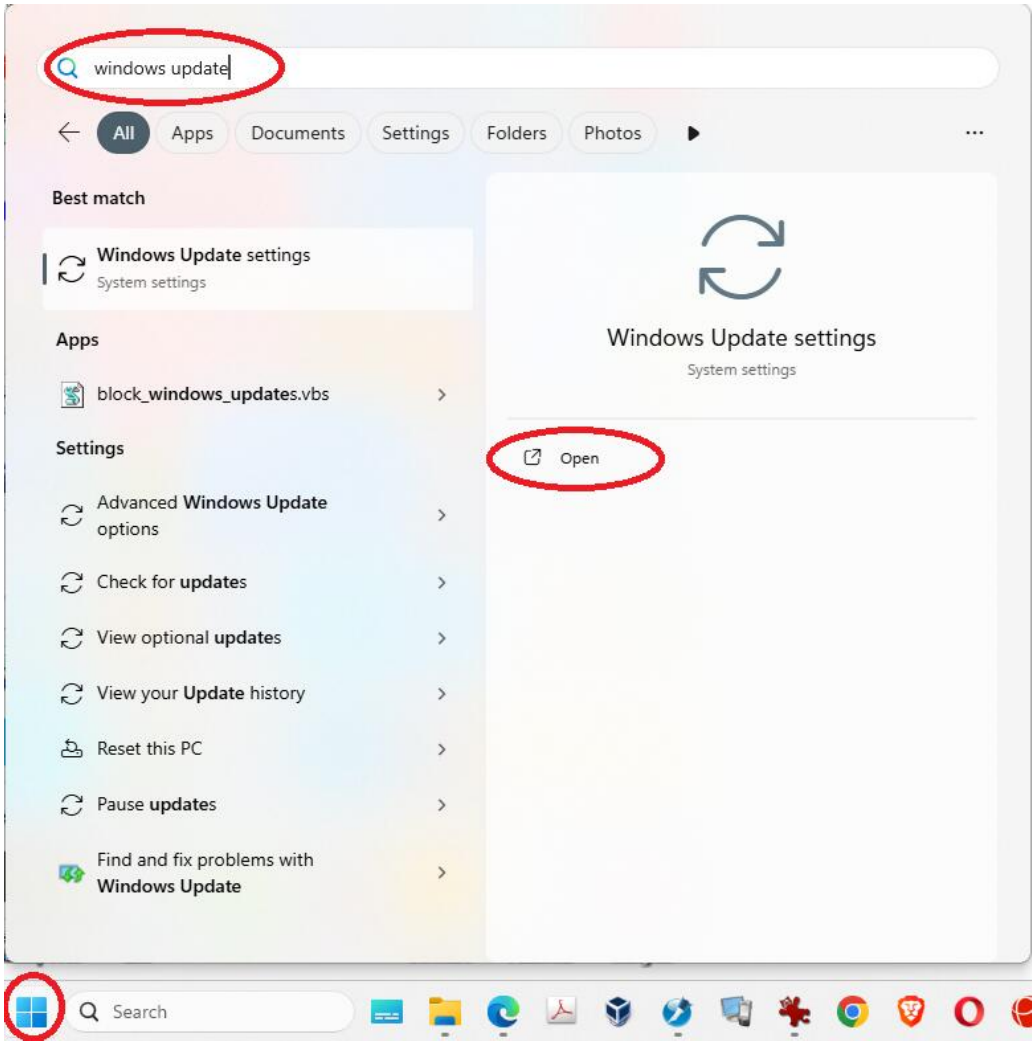
That means that any Windows 11 machine on 23H2 (patched until November 2025) or older versions (no longer patched), should be updated now.

Windows 10 machines that can be upgraded, which are mostly from 2018 to 2021, should be moved up to Windows 11 24H2 now. Machines too old to upgrade to Windows 11, which are basically machines from 2018 and older, should either be replaced if they are low end or if they're worth keeping then consider Windows ESU Security updates when they become available this Fall. The updates are only for security patches and do not include tech support.They are suitable for computers of reasonable speed that won't support Windows 11. So if you have an Intel Core I7 computer from 2017, that would be a good candidate for the ESU program.

Windows Extended Security Updates (ESU)

Windows ESU will become available this Fall and will cost $30 for the first year, doubling in price for year 2 and doubling again for year 3. There will also be a volume license version for large networks. Announcements on how to buy the ESU plan will begin in a few months.

How to Upgrade to 24H2



The best way to upgrade Windows to 24H2 is to click the start key (that Windows logo again, on the keyboard or the task bar), type ‘windows update’, and pick it from the list. Click on Check for Updates. In general, accept the choices offered, and click to install all of them. If optional updates are offered, do NOT install anything with the word ‘Preview’ in the listing; those are for users who wish to convert their computers into free testing stations for Microsoft, or lab rats. Don’t do previews on business systems.

Help with Upgrades, and ESU

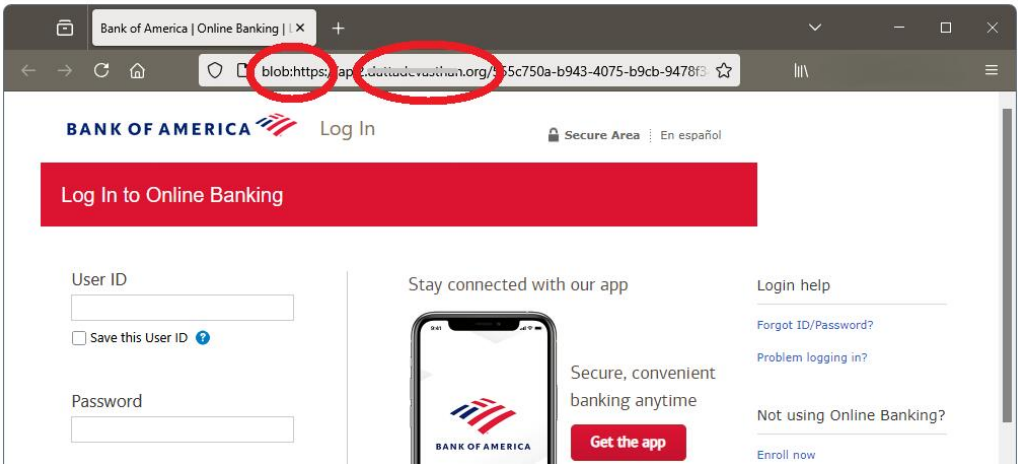
If you will want to use the ESU program, let me know; I'm starting a list for notifications. Call me f you need a free consult on 'Is this computer upgradable, replaceable, or worth the ESU program fee?'

More online:
New features in 24H2 from PC World:
https://www.pcmag.com/news/whats-new-in-the-windows-11-2024-update

Windows Calendar for the end of security updates:
https://pc410.com/calendar

Beware of the Blob!

There's a new style of dangerous emails, another species of phish, that's showing up in mailboxes. These messages use a link to a file known as a 'blob.' A blob is an archive file, which is a file that stores a group of files inside for easier sending and downloading. A blob file holds a complete web page inside. It is downloaded from from a legit server, usually hosted on Microsoft Azure or Amazon Web Services or another third-party server. That blob opens in your browser with a page address starting with 'blob:' and will probably be a copy of the login page of one of the top-30 banks, or a generic email login. Trying to login there will fail; it accepts all logins, fails them, and sends the logins back to a central server for exploitation later. These are dangerous. Here's a visual sample:



Look for ‘blob’ in the address line. The domain is clearly not at Bank of America. Don't let the 'https://' fool you. That means Hypertext Transfer Protocol Secure, so the connection to your hacker is encrypted. That does not mean that it's safe. Hackers use SSL, too..