Science Translations
Established 1990
PC410.COM™
PC Updater News

Windows Old and New

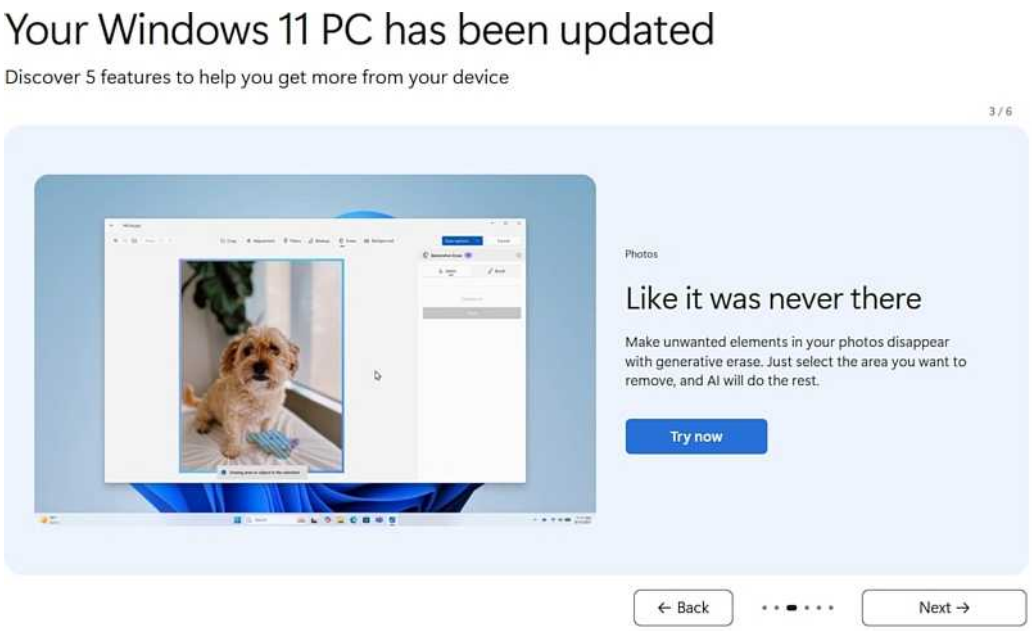
Windows 11 25H2 Arrives, Windows 10 Support Ends

The 25H2 release of Windows 11 is now available, and will start to automatically install sometime later in the Fall. For now, don't install it early, or go looking for it in Windows Update, on any business-critical computer. It's not urgent. There are also some errors in the news coverage, that there are no new features in the update. That's misleading: 25H2 turns on some new features

that were previously installed but not enabled in recent monthly updates. So the features are new to users, having previously just been sitting quietly in the background of Windows. Many of the new features are of no interest to most users, but the menu changes now allow groups of shortcuts, and will be useful to many of us. More at PC World:

https://www.pcworld.com/article/2914815/windows-11s-new-look-start-menu-is-a-huge-upgrade-lets-dive-in.html

There's a caution if you are running an older-model network-attached backup drive. 25H2 has issues with SMB version 1, which is mostly no longer used, unless you have a backup drive that's more than five years old. If in doubt, call before installing 25H2.



"Your Windows 11 PC has been updated"

This message showed up on some computers after the September Cumulative Update for Windows 11. It's a good, short, tour of new Windows features. If it did not show up, or you'd like to go back and click some of those 'Try now' buttons, here's the link; it works best in Edge.

https://www.microsoft.com/en-us/getting-started/windows/update?ep=1426&form=M1003V&es=266&cs=1552321079

Windows 10 Support Ends, Upgrade or ESU?

October 14th is the last update to Windows 10. By November 11th, the first monthly Patch Tuesday that will not deliver security updates to Windows 10,

your choices to keep running Windows safely are below, most-recommended first. Reminder: Old PCs need more repairs. All Windows 10 PCs are approaching retirement age, and most have passed it.

- Upgrade to Windows 11, if possible. Some computers will FAIL the Windows 11 upgrade test, but can still be upgraded after some changes I make to the BIOS settings and boot settings. Call if in doubt; Windows 11 upgrade checks and planning are still free.
- Replace the computer.
- Subscribe for one year to Windows ESU (Extended Security Updates). It's either $30 from the Microsoft Store (easiest), or 1,000 Experience Points for Edge, Bing, and Copilot users, or there are some more complex options for Microsoft login accounts.
- Disconnect from the internet. An offline computer has no expiration dates beyond hardware failure.

Note that the ESU option may not be appropriate for anyone subject to compliance regulations for handling government accounts, medical data, or financial data, including credit card numbers, or to use the acronyms: SOX, HIPAA, or PCI.

Instructions from Microsoft for getting the ESU service for one year are here: https://www.microsoft.com/en-us/windows/extended-security-updates

How to Spot a Phish

False Urgency, AI Phishing

Phishing attempts, offering you click-bait in puzzles and surveys that lead to information harvesting, or emails that tell you that something is urgent and scary, or include a fake payment or invoice, have all been around for years. Microsoft estimates that over 90% of malware attacks are blocked by not using Admin-level accounts, so what is a poor scammer to do? They rely on you to take that bait and fill in a form or allow a program to run.

In the time of AI, what is changing is that the bait is less sloppy, and more targeted to you. That's known as either Spear Phishing (targeted bait), or Whaling (bait for large enterprise targets).

Watch out for any emails that are not how you normally work. An email asking you to log in to a webmail server to allow or fix something is an attempt to harvest your login. Delete. An unexpected security software invoice is an attempt to have you call the convenient toll-free number so that the helpful staff can harvest your credit card, or log into your computer to plant spyware. Delete.

You should know the names of the companies you do business with, and which category they are in. It's a short list, because they are the companies you pay monthly or yearly. So when you get an invoice or receipt email from some other company, you know you can delete them. These are the fake invoices that suggest calling a toll-free number to dispute an invoice, or the renewals for products you don't use, or the credit card dispute notice that is not from your merchant account provider. They're basically out-of-pattern messages; if you don't use a service, you should not be getting an invoice from them.

AI in your Search Results

Don't ask an AI where to go for bank logins, account logins, or anything else with a login. The results can't be trusted. At best, you will get the wrong bank, not from your area. At worst, you will be shown phishing login sites. Phishers are targeting AI engines to serve up incorrect scam addresses, all looking precisely like the correct page, because the graphics are pasted from the real thing.

Again: Don't follow search or email links to banks and brokerage sites. Type the address, or use your own bookmark. It's too easy for scammers to fool an AI into serving a bad link, or fool YOU into clicking on, for example, a web site with letters that look correct, but are one character wrong, like using an international character to represent a similar letter, or an address that is far too long, has the correct address embedded in it, but ends in the wrong country code.

- Like this:

- **some-bank.com.lots-more-stuff.br/**
- instead of:
- www.**some-bank.com**/

More from KnowBe4 here:
https://blog.knowbe4.com/ai-generated-summaries-mistakenly-suggest-phishing-sites

AI in your Phish, AI on your Phone

AI is taking over scam emails and calls. It's not that you'll notice anything robotic going on; it's just that the new AI-enhanced emails will be more targeted to you, have no punctuation errors or non-English capitalization errors.

For example: An AI system is given your email address. For a business, it can look up your location, and send nearby fake bank look-alike sites to log into, instead of just the top 50 global banks at random. It can look to see if your email server has a specific login, frequently CPanel or RoundCube or Microsoft 365, and send a scary 'must fix' scam message to capture your login. Or for larger targets, look up your corporate address book, and send "personnel department" messages to change payroll direct deposit accounts to some other bank.

At this point, you need to assume that emails and voice calls and text messages that ask for information in a new way are always suspect, and must be confirmed. Your staff has to know that policy changes don't arrive without pre-announcement, won't be scary-urgent, and won't suddenly require online logins where they previously did not.

For computer help, call 410-871-2877
Missed a newsletter? Back Issues

Mailing address:
Science Translations
PO Box 1735
Westminster, MD 21158-5735