Science Translations
Established 1990
PC410.COM™
PC Updater News

Who Left the Windows Open?

I know who gets into trouble, who clicks what they shouldn't, and who gets their computers infected. There is a pattern to it. From worst to best, it's over 90% preventable. Where do you fit on this scale?

- **Worst:** User runs Windows as an administrator, with no password, and has User Account Control turned off because some accounting-software support tech did it while installing an update. When absolutely forced to use a password, it's always the same one, for the past twenty years. The

antivirus software that shipped with the computer expired years ago, but is still running, partially.

- **Result:** All software requiring admin rights runs unstopped, unannounced, and is often completely unseen. There are many infections, of the worst types. Occasionally suffers from account takeovers and identity theft. Home pages change randomly, and there are constant popups.Computer cleanups required, but user just thinks the computer is slow because it's old.

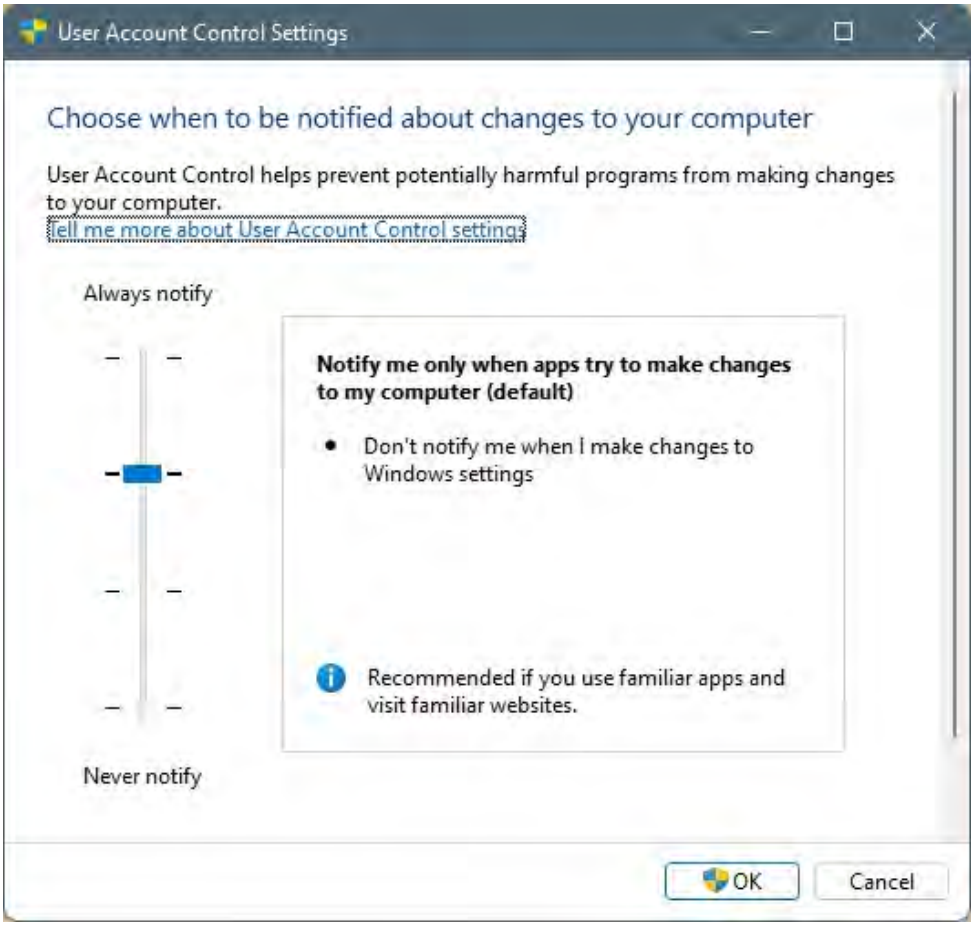
- **Bad:** User runs Windows as an administrator, with User Account Control turned on, but no password. For any permission popup, clicks the 'go away' button fast to get back to work. The antivirus software is up-to-date free software from the former Soviet Block.
- **Result:** Repeated cleanups, mostly rogue add-ons in browsers causing loads of popups and some banking password thefts.

- **Pretty Good:** User has two Windows accounts, one an admin, and one that's used daily that is a standard user that can't install software. User Account Control is on. The antivirus is from the US or Western Europe. User is careful what they click.
- **Result:** Occasionally lands on misspelled web page addresses that pop up scary demands to call 'Microsoft' but knows that's a hoax, and calls me. Result: Rare minor cleanups, usually low-level stuff, or just a reboot to clear a hoax page.

- **Best, and ideal for business accounts:** The computer has two Windows accounts, one an administrator that has a password known only to the business owner, and a standard account with a password for the computer user. The antivirus is current and based in the US or Western Europe. The user doesn't have their own email password, as that's saved in Outlook or Thunderbird. User Account Control is turned on. Third-party updating software keeps browsers up-to-date. Popups asking permission to install software are closed, because user can not install software; that's left to the owner or tech officer.
- **Result:** Not much happens that shouldn't. Not having an email password prevents credential theft, and not being able to install software blocks most rogues, hoaxes, and trojan horses.

Action Points

User Account Control is part of Windows, and it detects software that's trying to change Windows settings, and pops up a warning and asks permission to continue. It requires administrator rights to get past a UAC prompt. **It should be turned on. Always.** To check, click Start, type UAC and go to the UAC Settings screen. The default setting shown below is best.



Antivirus: The free products are mostly about constant advertising for paid products. I see far more cleanups that should not be needed from AVG and Avast users than I do from users of Webroot or the paid edition of Malwarebytes.

Third-party Software patching: This is automatic patching of Adobe Reader, Chrome, Firefox, Thunderbird, and over a hundred other programs. Most users have around 5-12 of these installed. There is free patching software that you can run yourself every few months, (See patchmypc.com and click the 'home users' link.) or I can automate patching, at $20/year.

That 90% preventable number that I mentioned? If you do nothing else but separate the user and administrator passwords and automate patching, that's

the result. 90% or more of mail hoaxes and web page drive-by attacks are blocked.

Call if you need help setting up a separate administrator account and so on. All I've covered above works for both business and home users.

Expired Windows

There will be a new Windows 10 feature release, version 22H2, later this month. The 22H2 version of Windows 11, inconsistently ALSO labeled as Windows 11 2022, was released in November. My current recommendation is to NOT INSTALL these optional updates until at least mid-January. It's best to allow time for myself and other techs around the world to try these out and see what they break, and time for Microsoft to quietly place fixes in the monthly Patch Tuesday security updates. FOR NOW, all Windows 10 and 11 machines should be on version 21H2, short for 2021, second half.

The new features in the Windows 11 22H2 are not going to all arrive with the feature update; they will arrive gradually over the next few months during the regular monthly security updates, generally on or after the second Tuesday of each month.

Here's Microsoft's information on what's new:
https://blogs.windows.com/windowsexperience/2022/09/20/available-today-the-windows-11-2022-update/

Microsoft expires their software. You can use it as long as you like, but the security patches end at a date known as the end of Extended Support, and after that, there are safety issues, and for some of you, legal compliance requirements to keep systems up-to-date and patched.

Quick Version Check: Winver

To check the Windows version, click on Start, type ‘winver’, and select Winver from the search results. The Windows version is on the second line.

Old Windows

All unsupported systems below should be upgraded or replaced or disconnected from the internet. Here’s a summary of where Windows and Office versions stand right now.

- All Windows 7 and Windows 8.0 systems are past all security patching now. Windows 8.1 will join them in January of 2023.

- Windows 10 should be version 21H2 right now. Version 21H1 will leave support in December, and 21H2 next June.

- Windows 11 21H2 was the only feature release of Windows 11 until last

month. Wait until January, and then update it to the 2022 (22H2) version, before October 2023.

These dates are kept online on my web calendar, here:
https://pc410.com/calendar

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

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