Science Translations
Established 1990
PC410.COM™
PC Updater News

Stop. Don't Do That.

Some of you are doing stuff that costs you time. Or money, sometimes. Check which of these applies to you.

Don't overload the system. I'm talking about programs that run all the time, like antivirus (endpoint protection and security software in general). One security program is good. Two that are designed to work together might be good. (Ask me if in doubt.) Three is loading down a system with a pile of rocks. Yes, the result is a self-inflicted door stop.

Don't install software using the ‘default' options, ever. Always choose ‘custom,' and read the options.

- Watch for ‘start with Windows' and ask "Why does it need that?"
- Watch for options to install every language available and not just yours.
- Or add a load of fonts or artwork that you will never use.
- Or, worst, "Also install_____" which is generally adware.

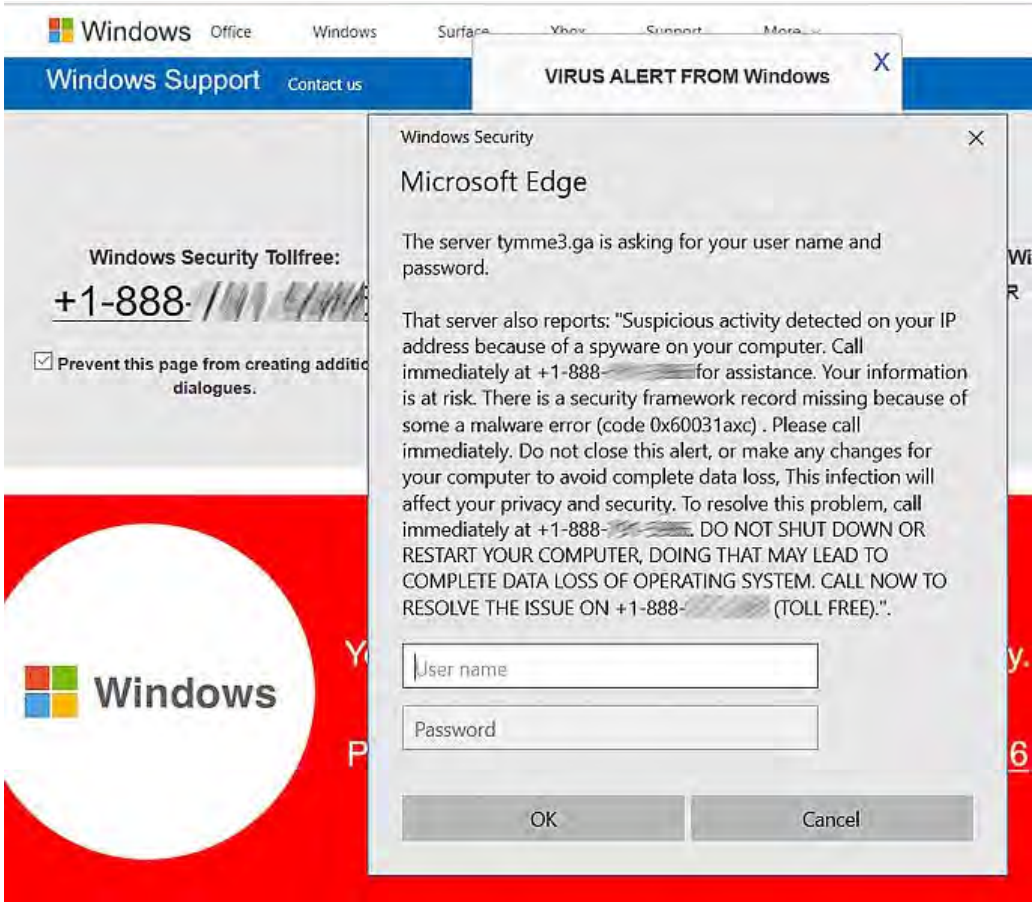
All of my computer tuneups involve looking at "What's running all the time that should run only when you need it?" and removing it. So don't trust ‘default' setups.

Don't click again. If a web page takes its own sweet time to respond, let it. Each time you click, you send an instruction that has to be handled, and the web page or program is going to process every one of your clicks one after another, and it's going to get take longer to catch up. Same thing applies to email software; the ‘get mail' button is local, but it's waiting for an online response, so multiple clicks don't help, and can cause a full-day security lockout.

Don't repeat failed experiments. "It didn't work, so I tried again. Then I called you." Well, if the issue was a traffic jam on the internet, WAITING a few minutes before clicking again may work. But mostly, not. Changing nothing and just repeating what didn't work last time is still in the category of pounding on the buttons.

Don't stay logged into Windows forever. When Windows is left logged in and the computer is left on forever, or a laptop is set to sleep or hibernate when the lid is closed, nothing stops. So the result is that there's no chance for Windows to wipe the memory, restart the services, or install updates and run backups. All computers should be fully rebooted at least monthly, but weekly is better and will result in fewer interruptions while you're working.

By fully rebooted, I mean: Log out. Then reboot. Don't skip the logout. Windows 10 and 11 don't shut down services while users are logged in. Don't skip the logout.



A hoax page. It's not Microsoft.

Don't call phone numbers that show up in error messages. These are always fake. Any web page that threatens disaster and loudly tells you to call, is a hoax. It's just an advertisement for a phone "tech" that will claim they're from Microsoft and that they can fix what's wrong for $399. Microsoft doesn't actually want your phone call, and they won't call you about your computer. They don't want to talk to you. Ever. I've been a Microsoft solution partner for decades, and my **real** calls from Microsoft are **always** from the training and local events staff, and **never** about a computer.

Don't click a link in an email without first looking where it goes. Float the mouse over any link without clicking, and watch the bottom line of your screen to see where it goes, and to make sure it's going where it really should go. Is it a complex link wider than the screen? That's a tracking link. Does the domain name match what it should be, and have a slash at the end, after the domain but before the page name? If not, that's a phishing link, and it goes to a completely different place.

- **Valid link:** https://www.DOMAIN.com/... and a page title, usually.
- **Tracking link:** https://www.DOMAIN.com /**?id**=kjdlf234290co45390u34!mcucpwpnmxpcfoieurty77!fdassdfa...

- **Disguised link:** https://www.DOMA**1**N.com.**SOMEWHERE-ELSE.ru**/...

Don't change how you do business based on ONLY an email: Your boss sends an email asking for a wire transfer, but never did that before. Or worse, a 'Swift' transfer, which is international. That's a phish, or a (targeted) spear-phish. The destination is always overseas, and never reversible.

Don't open an email attachment that contains a 'payment.' There's money in that digital file, right? No, money doesn't work that way, even with new technology; it's a phish. Also don't log into websites to receive a payment; your company has established methods to accept payments, and your customers don't get to invent more.

Don't send gift cards to the IRS. There's an email or phone call from 'IRS', or any government agency, or bank, that insists you will be arrested today, or your power turned off, unless a balance is paid today by Amazon gift card or a money order sent as an ID number. No, the IRS first-contact for collection is always by paper mail, never by email or phone or text, and the first contact isn't a threat. That also applies to utility companies. This is a hoax trying to collect gift cards and money orders. Delete it, or hang up.

Don't park computers on carpet, or notebooks and laptops on blankets. The floor is where the dust bunnies live (and worse), and they like to live inside

computers. Computers work best where YOU are comfortable working. Notebooks pull air in from the bottom, so they overheat on fabric surfaces. On top of a desk is comfortable.

Don't log in as an Admin unless you're doing Admin work. Surfing the web or reading email as an Admin means that web sites can install software without asking permission. Some web pages are evil, either hacked websites of good companies or web pages that you land on by accident, from old links and spelling errors. Some of these sites use known errors in Windows and browsers to install software quietly in the background. Using a NON-admin account blocks nearly all of that. So save the Admin account for computer configuration.

Windows 11 22H2 and Windows 10 22H2

And finally, right now, if Windows offers to install 22H2, **don't do that yet**; there's usually a link to stay on the existing version, for now. These annual feature updates appear to be mostly harmless right now, but it's best to give the OTHER software companies time to test their updates with it and make any adjustments, and best to avoid helping Microsoft to test their patches. Wait for January for the 22H2 updates.

In general, when Windows gives you the option to install a new update, wait a week or three. The patches are important, but your software vendors will tell you that they don't support new Windows releases until they've had time to test them. So wait for the dust to settle and any problems to be solved, by someone else.

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

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