Science Translations
Established 1990
PC410.COM™
PC Updater News

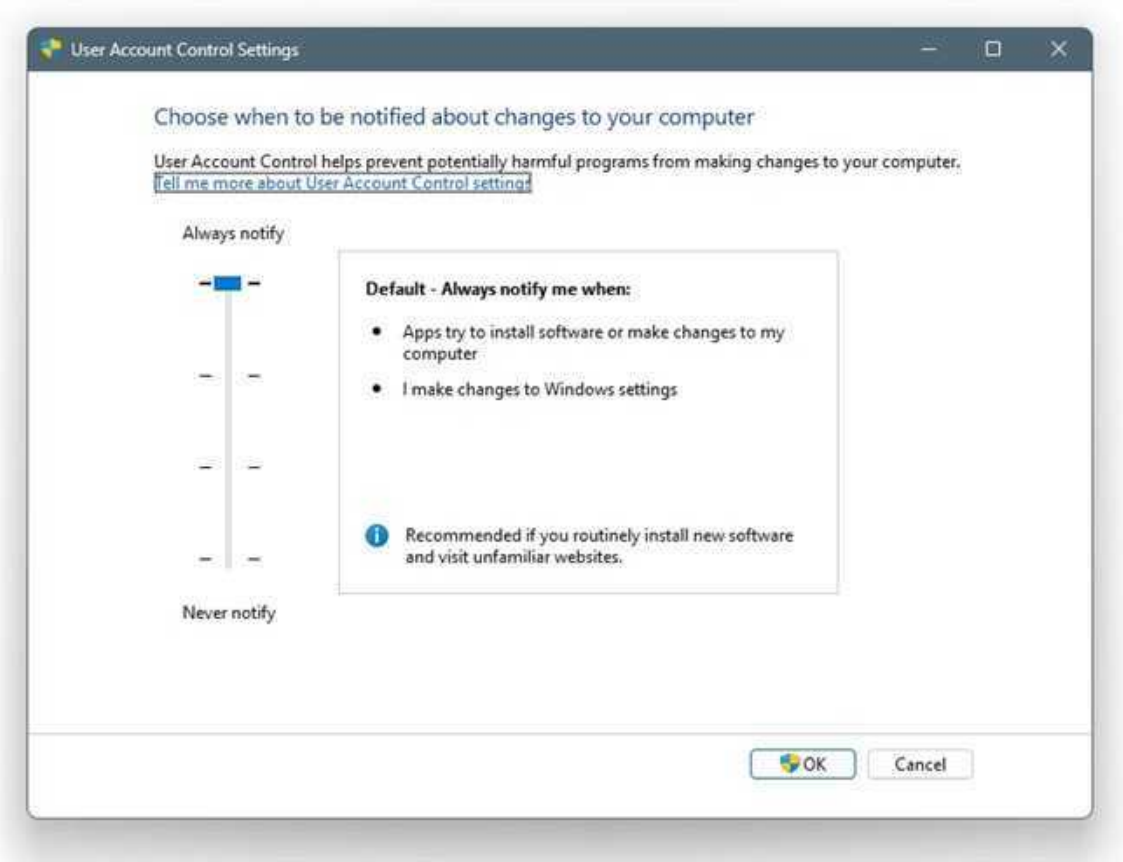
Malware: Remotes and RATs

I'm seeing a recent pattern of remote control access software hacks recently. These are mostly not 'RATs','short for 'Remote Access Trojans,' which are remote-access software that hides while providing hacking access. No, these are mostly mis-used commercial products used for tech support or remote office workers.

The message starts with a 'we have to have an urgent video chat with you, with my partner, and he can't make phone calls.' (That should be enough of a red flag already.) There's an attempt to connect a video call, sometimes with a valid service like Zoom, which won't work. The next message is a link to a new

meeting, and that's an installer for a re-named remote control application, and sometimes a bundle of several of these.

How it gets worse: Remote software for technicians can do invisible background sessions, not with the full Windows experience, but good enough to run a script to export saved passwords or to copy files.

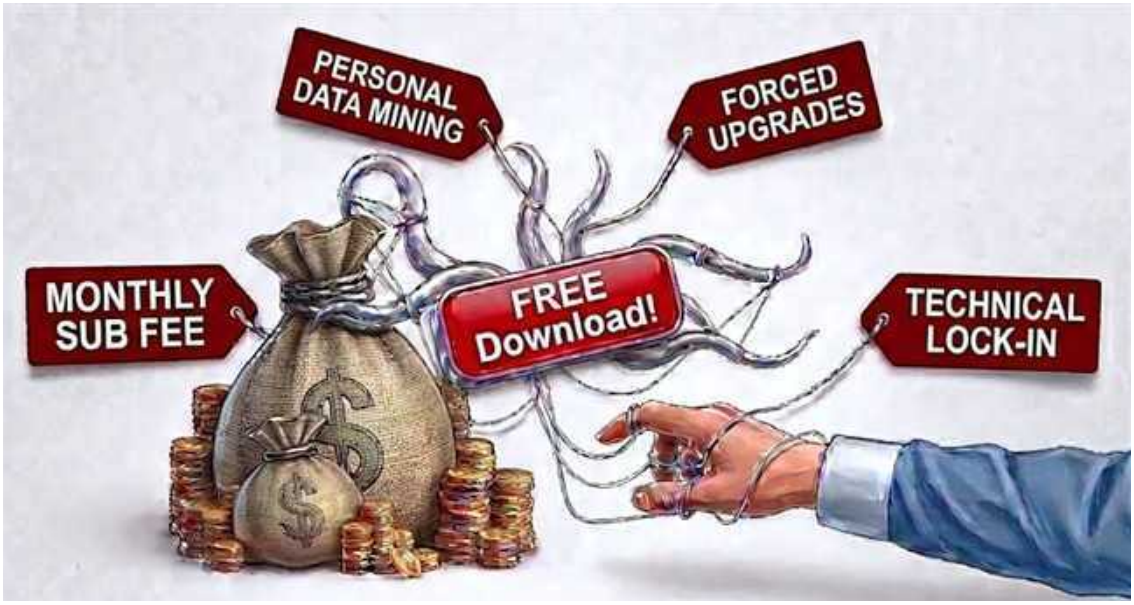


The way to keep this stuff out are the usual precautions:

- Leave 'UAC' or User Account Control, at the default 'Notify Me' setting, as above.
- Don't add software to chat with a first-time contact who has no phone number, a free email account, and stresses urgency and large sums.
- Use a 'standard' account for your daily work, NEVER an 'admin' account.
- Use different passwords and user names at all online sites.
- Don't allow browsers to 'remember' your logins for banks and the like.
- Watch out for new icons, new software, and changes in what the desktop looks like–most remote desktop software turns off the on-screen wallpaper.

The on-PC cleanup is routine on these. The banking cleanup is a mess. One

last note: If you have remote desktop software on your computer that was installed for a one-time tech support session, remove it when finished. Don't leave these doors open.



When Software is Free

Free software comes in a bunch of different categories. The basic rule is that free software and services make you into the product; your data is harvested to sell you subscriptions and add-ons or sell your shopping and searches elsewhere. This works in many different ways and can change over the lifetime of a free program.

Why is Software Free?

- Free 'light' version of a bigger product. Easeus ToDo Backup Free is a light version, with advertising for the paid product that adds more backup types, scheduled backups, and email alerts.
- Open Source. These are generally developed by a community of software developers working together. Linux is the biggest example. Firefox and Thunderbird are open source from the non-profit Mozilla Foundation.
- Bait. That's the best word I have for it. A free coupon searcher, or recipe finder, or traffic advisor, or search app. Trivial apps with zero value that sit in the browser and turn your web surfing activity into money. Or worse, that steal passwords and anything that crosses your clipboard.

- There are more types, not all in wide use right now: We've had postcardware, free games with two paid sequels, and odd marketing models that worked for a while, but not lately.

Adobe Reader is free. Back in the late 90s, it was free because Adobe had this new thing called portable documents. They wanted to establish their PDF, for portable document format, as an industry standard and they had good competition, at that time, from Corel Envoy. They won; the other portable document products are gone.

Now, Adobe continues to have a free reader program. But what it does most loudly in the newest version is push hard for subscriptions to Adobe's subscription products. So it is no longer free in order to create a standard. It is now free for marketing of a subscription, $12.99/month and up, and it is far too loud in how it does that.

Recommended substitutes: NAPS2 for PDF scanning, combining, and page rotations or deletions. And PDFGear for PDF viewing, printing, and light editing. Both are free and have no advertisements.

Before you Download, Identify WHY it's Free

Before downloading anything that's free, look to see what the publisher's web site is selling. If there's a free product and a pro product, OK. If it is open source and there's a call for volunteers, OK. But if there's nothing there but the big free claim and some marketing that says how scary and urgent not using it would be, no, that's bad.

When working with any new product, type the name into Google followed by 'complaints' and check what comes up. Not 'reviews' because those are mostly fake. Any review that links to the product with a long link that includes a code to identify the source is not a review; it's a commission payment.

When downloading any software, get it directly from the publisher's site. Nowhere else. No exceptions. The software catalog sites have altered bundled versions, and a lot of old versions.

Finally, for any program, you can check if it's known to be dangerous at VirusTotal.com. Either a download or a link is testable, and it will show the antivirus scan report for a file over (currently) 68 AV programs. It's also great for

scanning email attachments that come from unknown senders. (I.E., all of them.)

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

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