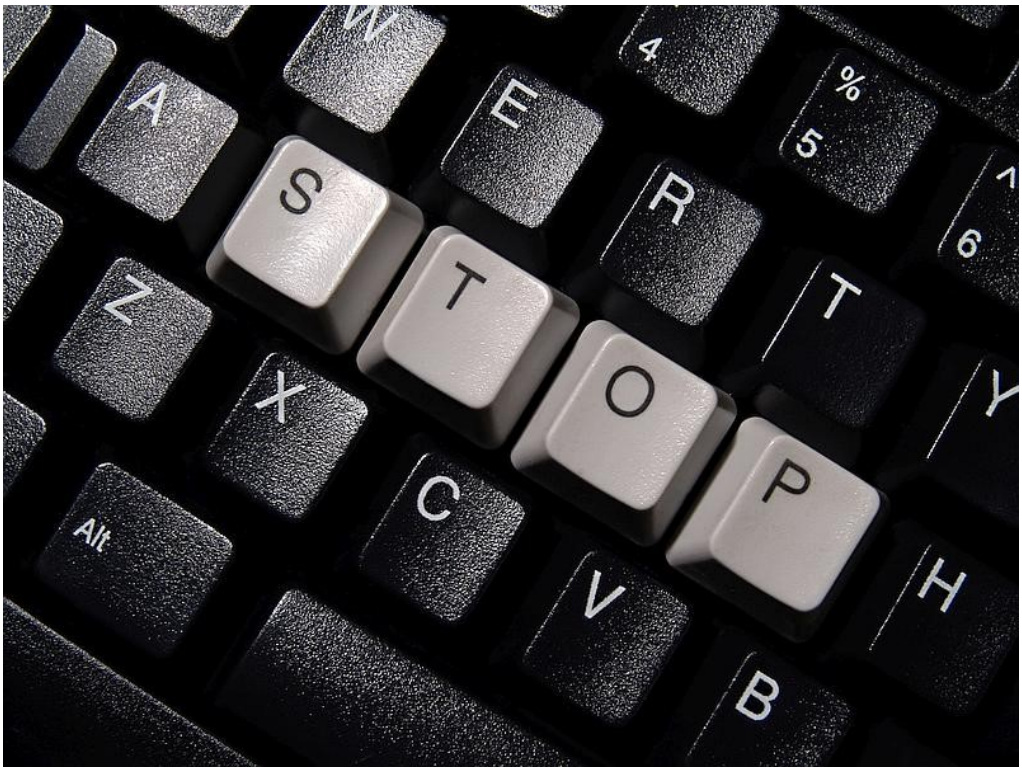
Science Translations
Established 1990
PC410.COM™
PC Updater News

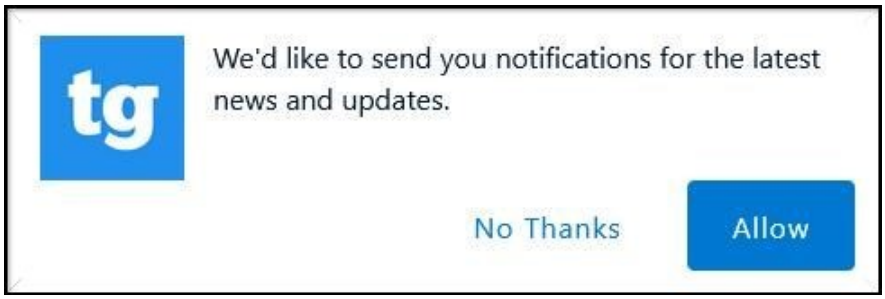
Don't Do That!



The internet is still an unregulated frontier. Clicking the wrong link, or believing that what's on-screen is real, is a good way to get into trouble. The bad guys out there want to own your computer, to send threats for ransom, or to mine cryptocurrencies, or to send you targeted non-stop advertising. But most of the software methods to do those things are blocked by the combination of good endpoint security (formerly known as antivirus software), and the use of ONLY non-administrator accounts. So the way that the bad guys use most to own your technology is encouraging you to help them. Here are some of the things not to do.

Notifications

Notifications are the bottom-right slide-in popups that happen when you are NOT visiting the site that sends them, or not even using a web browser. Notifications have some good uses, so security software isn't blocking them yet. Yes, it might be a good idea to have tornado warnings as popups. And Outlook can send its own notifications on the arrival of new mail. But web-based notifications are just popup ads in a new form, and they get into your computer as a browser option after showing a message like this, after you clicked on the 'go away' button, which is usually 'allow' or 'ok' or 'sign me up'. No, this is not an offer to show you news **while on that site**, it's permission for your browser to show you their ads at the time they choose. Always say no.



In Firefox, you can turn off Notification requests in Settings, Permissions, Notifications, Settings, and then add a check in the box 'Block new requests asking to allow notifications.' From the same page, you can see websites that have already collected permission to ad-spam you, and can change 'allow' on each listing to 'block'.

In Chrome, go to Settings, Privacy and Security, Site Settings, Permissions, Notifications, and set 'Sites can ask to send notifications' to off. On that same page, you can disable each of the currently allowed notifications.

Extensions, Add-Ons

Software that runs inside the browser is a problem in general. It runs all the time. In some cases, it runs in the background even when the browser is closed, and it slows down Windows startup. These programs are called Extensions in Edge and Google Chrome, or Add-Ons in Firefox, Thunderbird, and Outlook. Yes, they can break mail software too.

Good add-ons include security software from the company that runs your Endpoint Protection (anti-virus), such as Webroot or Malwarebytes. There are some good plugins for web design that help to find errors in web pages. Both those categories have good reasons to work as add-ons; they need access to the page that you're looking at.

Bad add-ons that I find in nearly every 'slow computer' tuneup generally include these badly-abused categories: maps, coupons, shopping discounts, and 'computer speed-up' add-ons, which generally scare the user into buying software to fix speed issues caused by the add-ons themselves. It's called 'creating a market for your software.'

So any offer to install a plugin, add-on, or extension into a browser, a mail program, or into other software that can use them (Adobe Photoshop and Acrobat, Autocad), should be looked at closely, and if it's not something that **must** run all the time to be useful, just say no.

To remove Firefox Add-Ons, go into the menu from the three bars icon, Add-ons, and check for software listed as either Extensions or Plugins. If it's there, and you didn't ask for it and want it, it can be disabled.

In Chrome, go into the menu from the three dots icon, More Tools, Extensions. You can turn off and keep, or turn off and remove, any extension that is not needed.

Phone Numbers on the Web

Never search for technical support phone numbers online. If you need them, first go to the company web site for the product where you need help, and then look for the support options. It's not the same as searching Google, for example, for 'Dell phone number.' Searches for phone numbers lead to ads for companies that want you to call them so that they can remote into your computer and create urgent repairs to bill you for.

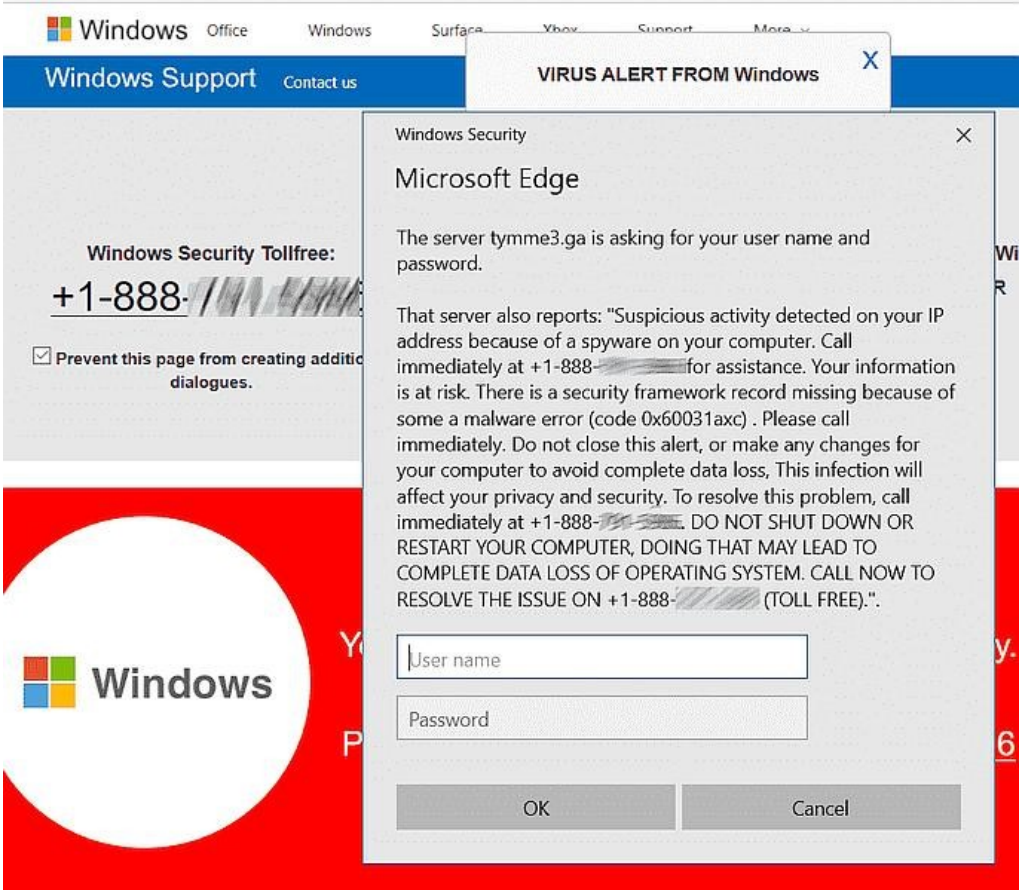
These were a very big problem a few years back, when the fake results filed the first page of searches and overwhelmed the real results. Calling those numbers usually ended in a $400 subscription to the free Microsoft Defender. Now, Google is doing a better job of filtering out the fake results, but it is still showing paid ads for third-party tech support, which should not be the first place to look for warranty claims and setup help for a product.

Phone Numbers on Error Messages

No. Just no. For the record, every phone number that shows up in an error message on your screen is a hoax, and calling it will lead to credit card fraud, at

best. Microsoft and the other big tech companies do not want you to call them on any phone number not going to their outsourced Sales line. They make their internal phone numbers hard to find, and if you really need their help, you will be guided by their web pages through a web chat as first contact.

They will also never call you to talk about problems detected in your computer; they have no way of matching up a computer to a phone number. Even I, as a dealer in Microsoft products for over 30 years, only get phone calls from Microsoft when they want me to attend a training session for some of their latest and greatest stuff. Nothing else, ever.



So this message, on your screen, and anything else like it, is always a hoax. Close the program, or call me and I will help you close it if it won't close or comes back. Never call the number.

For computer help, call 410-871-2877