Science Translations
Established 1990
PC410.COM™
PC Updater News

Beware Trojan Horses, Bearing Invoices

First, a definition: A Trojan Horse, or just a trojan for short, is just what it was classically, in the invasion of Troy by Odysseus, where a large wooden horse was left outside the gates of Troy. The Trojan forces pulled the horse into the city as a victory trophy, but Odysseus and a small force of soldiers were hidden inside, and when they emerged at night, they opened the city gates for their forces. That ended that war.

For the modern era, it's a file sent to you, or sometimes that you searched for, that is not what it claims to be.

- It's a document that claims to be an invoice, but is ransomware or banking spyware.
- It's a download of a "driver search program" to update your computer, ALWAYS a bad idea even if it worked, but the real payload is malware that intercepts your searches and banking logins.
- It's a download that claims to be game cheat codes, but that would be just a list, a short document, and yet it somehow needs to be an installed program.
- And very popular right now, there are browser plugins that claim to provide maps, coupons, recipes, or search features, but just turn your computer into a slow machine that clicks advertisements all day long to make money for the authors.

Best Defenses

The best defense, back in Troy, would have been guards at the gate that not only didn't have the authority to look a literal wooden gift horse in the mouth and pull it into the city, but didn't actually even have the ability to open the gate. In modern times, that means that your computer user accounts should not have admin rights, and so have no ability to install software. According to Microsoft, that simple precaution blocks over 90% of malware.

Some trojans get into computers through holes in software. The news outlets report these as 'you must immediately update' some popular program, but they announce it from three days to a week too late. Software that automatically updates the most-popular software on your computer quickly blocks the security gaps that were patched by the publishers, and then announced, which is of course the signal for the trojan authors that says, "Found a way in, and most systems are unpatched, let's go!" There are several good updaters, call if you need help choosing one.

And a good up-to-date endpoint security program with heuristic filters (behavior detection) should catch what's left. What gets past those three layers of protection is usually low-level stuff that can be cleaned up very quickly, nearly always browser add-ins.

Recognizing Trojan Horses

Lately, I'm seeing an increase in emails arriving here and at clients that are fake invoices. There are multiple types:

An "invoice" attached as an html file, urgent or overdue, from some sender you don't know. You can always delete these; they are either dangerous ransomware or an attempt to steal your login for an email account or a credit card. Nobody legit, ever, will send an invoice as an attached HTML file, which is short for Hypertext Markup Language, or, more simply, a saved web page. Delete the email.

An invoice saved for you in an online shared account, frequently Google Docs or Amazon Web Services, and again, it's an unknown sender. The payload is the same dangerous junk. Delete the email.

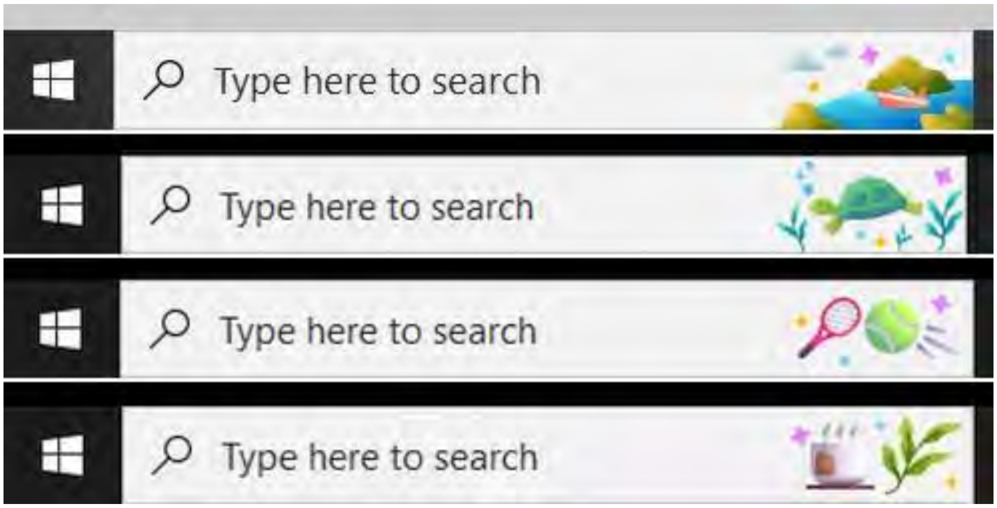
And there are still zip files arriving as invoices, with a password. Delete these. No one sends invoices in a zip file and adds password security and tells you the password, all in the same email. It would be insanely bad security for an invoice, but it does block antivirus software from scanning the zip file as it arrives.

False Urgency Syndrome and False Authority Syndrome

False Urgency: Most trojan horses cantering into your emails will look urgent. Do something right now or else something else happens. It’s just trying to scare you and your staff into clicking on what appears to be a payment or an invoice because it’s late, or big, or scary.

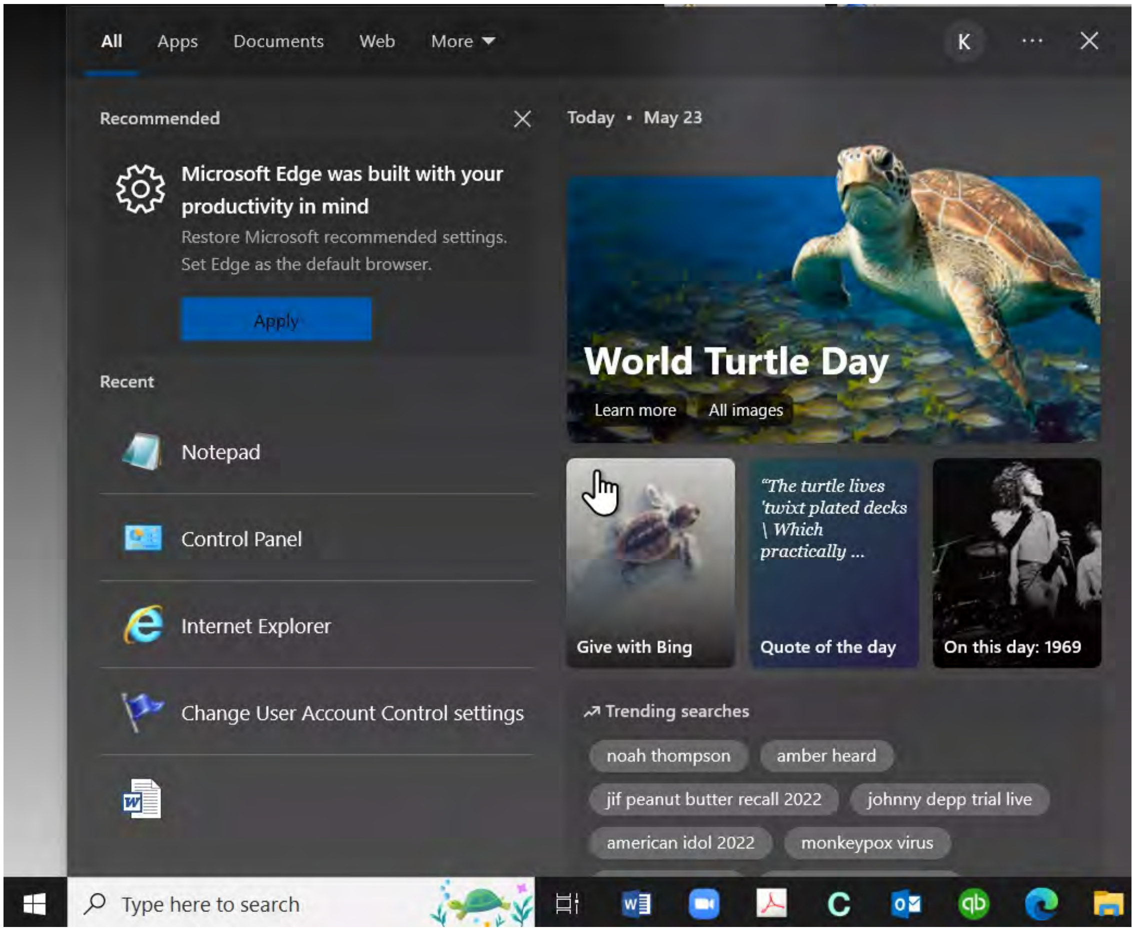
False Authority: The other approach, sometimes combined, is to make the trojan look like it’s coming from some well-known company. Maybe Norton, Appple, or Amazon. But if the email doesn’t match how those companies do business, it’s just another stray, fake, wooden pony. Don't believe an email came from a big company just because it carries their logo. Look at the sending email address, and always stop, and think: Is that a company I do business with, and is that sending email correct?

More on the Trojan Horse in history, here: https://en.wikipedia.org/wiki/Trojan_Horse



How to Turn off Search Highlights

Just recently, Microsoft quietly started pushing a new feature into Windows 10. I have no idea why they would add this to Windows 10 but not 11, but here it is: It's a daily cartoon-style link embedded in your search bar. At best, it's distracting, and at worst, it is yet another phone-home reduction of computer speed. If you place the mouse over the cartoon and pause there, it will pop up today's holiday link or travel link. I haven't found a fan of this yet. But you can turn it off easily.

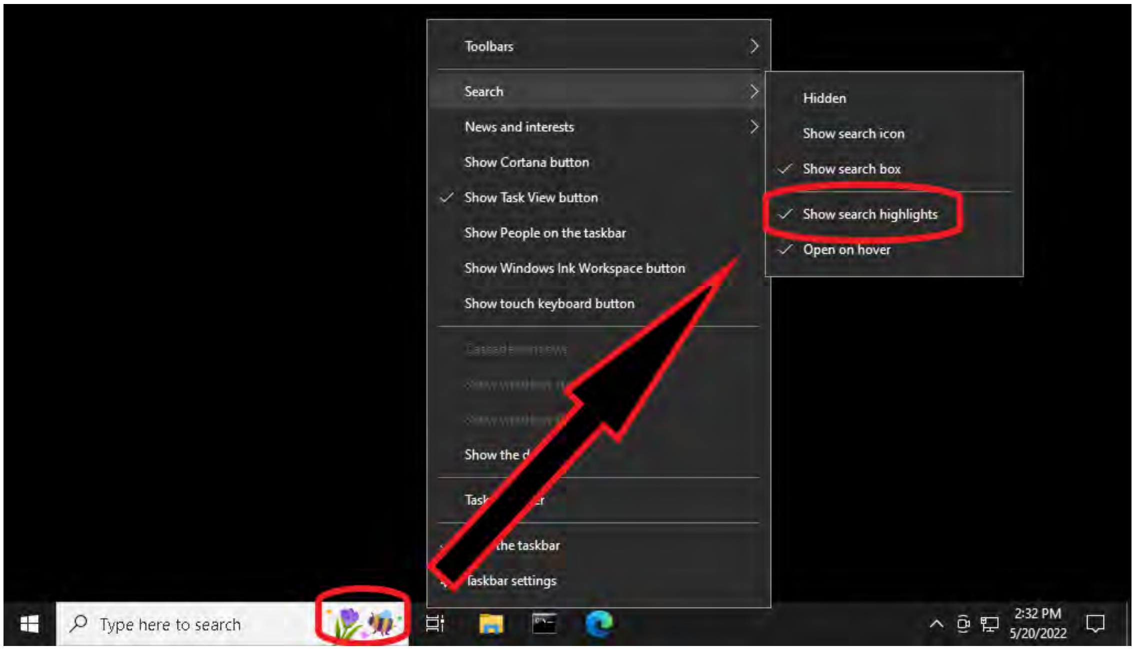


Microsoft Edge was built with your productivity in mind

Restore Microsoft recommended settings. Set Edge as the default browser.

"The turtle lives 'twixt plated decks \ Which practically ...

To turn off Search Highlights, right-click the Taskbar. That's the bottom bar, but NOT the search area. From the popup menu, choose Search, and then click to remove the checkmark next to Search Highlights. Done.



You are receiving this email because you opted in via our website or by discussion with me.

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