Science Translations
Established 1990
PC410.COM™
PC Updater News

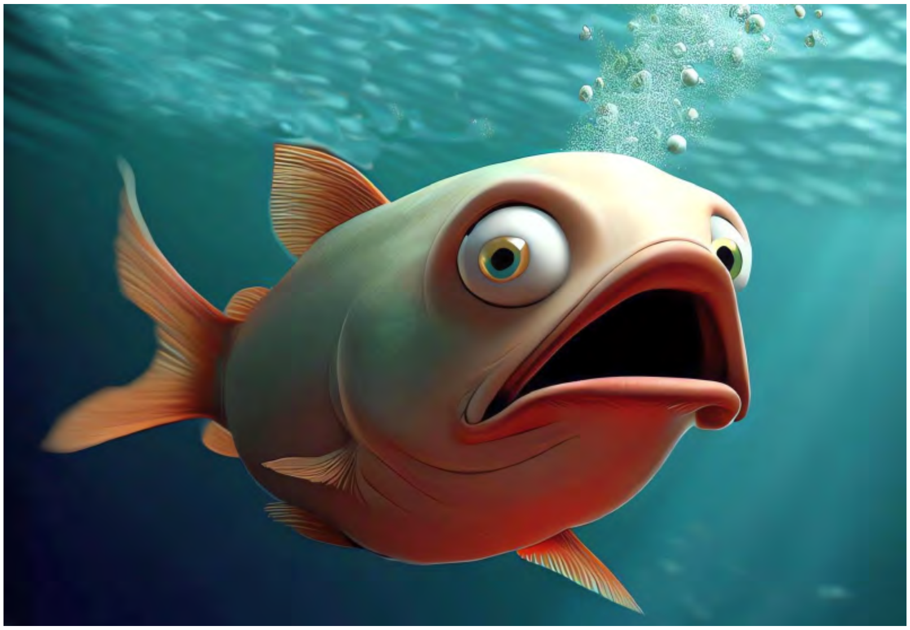
Definitions: When is a Phish a Trojan Horse?

A Phish email wants you to take some bait. A Trojan Horse wants to run around in your computer. And ClickBait is just the web page version of a Phish. There's nothing technical about bait and switch attacks; they're just criminal marketing methods. Recognizing them is important: For computer users who **never** view email or surf the web as administrators, and that should be all of you, no exceptions, nearly all malware that succeeds are attacks that rely on you to take action on something that looks safe and wanted, but is really just bait.

So the attackers are using multiple tricks. They make things look highly urgent.

Or like something you want, based on your web page visits. And they are getting better at targeting by industry, and pulling public information about you into an email. AI will make this much worse.

Phish



Phish are basically bait, something for you to click on, and fleeting. There's some urgency, to make them look important. What's behind that phish? It could be any other type of malware delivery, or sometimes, it's clickbait, which is usually trying to take you to an infinite slideshow with a dozen paid advertisements and over 20 trackers per page, or a browser hijack page. (below)

False Urgency Syndrome

False Authority Syndrome is basic applied psychology that's used in most of these email phish messages. Some company or agency you've heard of needs you to click or call urgently. That's false authority–it is **not** the IRS, and not some store that is going to autobill you for $397 today. What they want is a click, or to dial the hoax phone number to supply your credit card number, or worse, send gift cards for payments; those are **always** fraudulent.

It's also not some magical file that contains "your invoice." An invoice in any format other than PDF is dangerous, and should be deleted. And any document that has a macro embedded is basically software, and that does not belong in an invoice; if opening an "invoice" triggers a software prompt to run a macro, answer **No** and delete the file.

Trojan Horse

A trojan horse, like the wooden horse from history, appears to be one thing, maybe an invoice, but it's another, like an installation script for ransomware. It relies on a user to click on it and try to open it. It's usually in an email, but not always. Some categories of file downloads are particularly loaded with trojan horses, especially PDF instruction manuals for nearly anything, game cheat codes, and drivers.

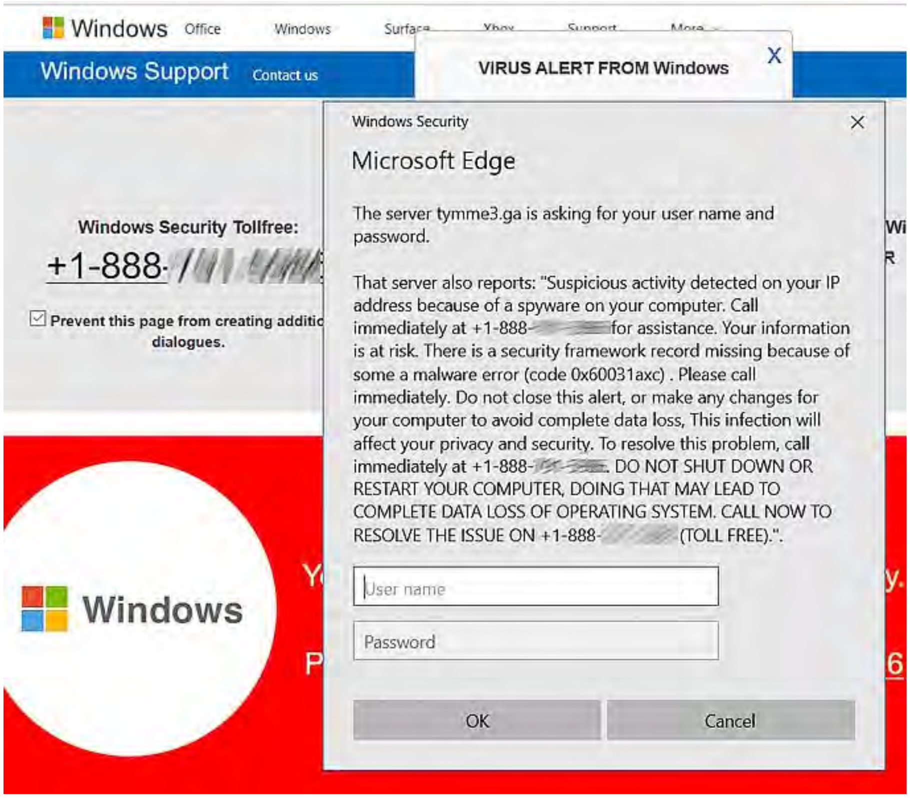
ClickBait

These are mostly web headlines that lead to garbage webpages. Many even show up tagged as an advertisement. Some are only an entry point to slideshows that go on forever without ever getting to the topic of the bait, with advertising on every page along the way. At best, these things make you into the product, not the customer, clicking to display ads forever. At worst, they setup scams that can empty accounts.

You can identify ClickBait online by variations on these headlines:

- "You can't believe what (a celebrity) looks like now."
- "This is how much (a home improvement task) should cost."
- "(your state) gets this tax break."
- "Five things we know about (a news topic)."

Browser Hijack Pages



The server tymme3.ga is asking for your user name and password.

That server also reports: "Suspicious activity detected on your IP address because of a spyware on your computer. Call immediately at +1-888-[redacted] for assistance. Your information is at risk. There is a security framework record missing because of some a malware error (code 0x60031axc) . Please call immediately. Do not close this alert, or make any changes for your computer to avoid complete data loss, This infection will affect your privacy and security. To resolve this problem, call immediately at +1-888-[redacted]. DO NOT SHUT DOWN OR RESTART YOUR COMPUTER, DOING THAT MAY LEAD TO COMPLETE DATA LOSS OF OPERATING SYSTEM. CALL NOW TO RESOLVE THE ISSUE ON +1-888-[redacted] (TOLL FREE).".

Browser Hijacks are the scary web pages that tell you to call a phone number. **Don't** do that. It's not a Microsoft phone number. Microsoft and every other big tech company makes it difficult to find their phone numbers; they don't want your phone calls, and the problems those pages warn you about are impossible to detect remotely. It's all fake.

The 'Microsoft employee' at the other end of that scam will show some scary-looking screen and call it the 'viruses in your computer' and then offer a 3-year subscription to Microsoft Defender to 'clean that up.' Hint: Microsoft Defender is totally free, already built into Windows and running ALL the time, and it's not really an antivirus product; it blocks a much shorter list of malware items that tend to spread from computer to computer, mostly known as 'worms.'

To escape the browser hijack page, just close the browser. If the red X 'close' button is missing because the page is in full screen mode, exit full-screen mode by tapping the 'F11' key. (On laptops, you may need to hold down the FN (function) key, at bottom-left, while pressing any of the top-row function keys.) If that doesn't work, try Alt-F4 to close the program. Or reboot the computer.

Sometimes these browser hijack pages come back after reboot; call if you need help. The usual fix is clearing that page from search history, and setting the browser to NOT reopen open pages after a restart.

Virus? Or Malware?

Malware is just bad software; it's the current generic term for all evil software.

A virus is a document or an image that has embedded software in it to make more copies of itself. It's nearly extinct. Nearly all malware is some other category, and not a virus. Even what used to be called Antivirus software has changed, and is now generically called 'Endpoint Protection' software.

One more time: The malware authors depend on you to open bad files and bad web links, and to click 'allow' to get past the security permissions in your devices. That's because endpoint protection software blocks everything except **you**. Stop, think before you click. Don't take the bait.

You've Got AI !

Generative AI has been available to try out by going to web pages for a few months now, but Microsoft has now added it to the Edge browser in Windows 11. If your Edge software is up-to-date, then it has a blue lower-case b icon at the top-right corner. Click that, and a side window will open for you to chat with the Bing AI.

What's it good for? So far, mostly very complex searches, because it includes links with answers. I tried this question, which would have failed completely as a normal search: "What ground cover can I grow in zone 6 that deer won't eat, stays green in Winter, and isn't over 5 inches tall?" That's 5 conditions to look for. Bing AI found Creeping Phlox, Liriope, Wintercreeper, and Bearberry, with links to more information. Finding the actual plants is more difficult than finding the information, for once.

Microsoft is going to add 'Co-Pilot' add-ins to that window, including specialized-knowledge answer sets, from real experts or specialty libraries, not just information scraped from the web. West Law will have an AI legal copilot. The expectation is that there will be dozens of these, many free, and some as paid products or as part of another package.

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

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