The WizLetter

2024 SCAM ISSUE (Updated)

Call The Wizard 1st
Questions answered free
727-366-5711

1. An email thanking you for a purchase you did not make
If you receive an email thanking you for a purchase you did not make, do not panic or click on anything in the email. It **may** be for Webroot, McAfee or Norton anti-virus. It **may** be for **anything.** Notice your first and last name is not stated. Your specific payment information is not listed. It has no specific information other than your email address. If you are concerned and you happen to have an account with the company thanking you, exit email and go to that account the way you normally do. If you made the purchase, you would see it there. If you do not have an account with that company, it is even more obvious it's a scam. Either way, simply delete the email along with other **junk mail**.

2. If you get ANY pop-up with a phone number, it's a scam!
Loud noises, loud voices and very scary. Do not call the number on the screen. It's a scam to get your charge card information or to get you to send them gift cards. If you give someone control of your computer, they can get control anytime they want. You will need a professional to keep them out. Call ASAP if this happens to you.
DO NOT GIVE CONTROL OF YOUR COMPUTER TO ANYONE YOU DON'T KNOW!
Call the Wizard first for the free **20-second fix. (Tap the Windows key and Shut Down or Restart)** Do not recover the web page the next time you go online.

3. STILL HAPPENING! PEOPLE STILL PAYING THE $300+
If you think there is something wrong with your computer…
If a pop-up tells you there is something wrong with your computer…
If someone calls and tells you there is something wrong with your computer…
If you get a phone call from your own phone number…
IF YOU CALL for support and they tell you there is something else wrong with your computer…
Microsoft, Apple & the I. R. S. DO NOT MAKE OUTGOING PHONE CALLS…
All the above are scams to get your charge card information or to get you to send them Gift Cards
Call your computer guy. 727-366-5711. FREE CALL!
DO NOT GIVE CONTROL OF YOUR COMPUTER TO ANYONE YOU DON'T KNOW!

4. Any Email Stating… Please update your information.
DO NOT DO IT
Email that looks like it came from a reputable company asking you to update information may be a scam. Do not open and click on the link. It takes you to a look-alike page that will steal your login information and your identity. A few days later, you will believe you were hacked, forgetting or not knowing you were scammed.

5. Email from a friend that is out of the country asking for money
This is an oldie that keeps reappearing. Call the friend if you are concerned. But do not send money when any email asks you to.

6. Spectrum Email Scam
You receive an email from Spectrum stating your online access has been blocked or suspended. The first problem with this is you needed your online access to get the email. This email is NOT from Spectrum. It is a simple scam in an attempt to get your charge card and/or your bank account information. Anywhere you click on this email does not take you to Spectrum. Simply delete these emails. When you enter your personal information, you are sending that information to the scammers. There are several variations of this email.

7. Most hacks are voluntary
If you fall victim to any of the scams mentioned here, call me ASAP. I can fix your computer. Understand if you fall victim to a scam, you are being tricked into providing personal information. This is the information needed to steal your identity, hack into your bank account or use your charge card. A week later you may not remember providing this information and will think you were hacked. Or were you scammed? Do not provide personal information to anyone without understanding who you are actually giving it to. ESPECIALLY IF THEY CALL YOU!

8. If YOU call a company for support
Be aware companies like **DELL** and HP are selling off their out-of-warrantee and some in-warrantee support calls. If you call someone other than the Wizard for support and they do not address your problem, rather they start trying to get control of your computer, hang up. Scammers want to take control of your computer, show you **fake problems** and scare you into a $150 - $500 solution. They forget to tell you it renews next month. This is a SCAM. Be aware of this common scam that tries to sell you a support package. If you give control of your computer to someone you do not know, they will install software on your computer so they can get in any time they want. Call the Wizard first… Or ASAP after you get tricked into giving control to a stranger.
DO NOT GIVE CONTROL OF YOUR COMPUTER TO ANYONE YOU DON'T KNOW!

9. Email or phone call stating there's a problem with your Apple ID, asking you to go to your PC…
Apple does not make outgoing calls. If you suspect a problem with any online account, go to it and log in as normal. If there is a problem you will see it when you log in.
DO NOT GIVE CONTROL OF YOUR COMPUTER TO ANYONE YOU DON'T KNOW!

10. Microsoft calls and says there is a licensing Issue with your computer or software.
Microsoft does not make outgoing phone calls. Same old scam. Hang up!
DO NOT GIVE CONTROL OF YOUR COMPUTER TO ANYONE YOU DON'T KNOW!

11. Refund from an earlier scam
You receive a call from a company that scammed you in the past stating Microsoft is forcing them to issue a refund for all the money they collected from you. Then they set up a Western Union account requiring your charge card or bank information so they can complete the refund. The scam is they are sending your money to themselves instead of issuing a refund.

12. Email from your bank… *(Note: Bank of America & Wells Fargo are examples of your bank & not your bank)*
You do business with the Bank of America. You do not do business with Wells Fargo. If you receive an email from Wells Fargo asking for information or informing you of a problem with your account, you would know it was a scam and you would not comply by clicking on any link in that email. Likewise, if you receive an email that looks like it came from Bank of America asking for information or informing you of a problem with your account, you should **NOT** comply by clicking on any link in that email. If it is a scam, clicking on a link in the email will open a page that looks like your Bank of America log in page. But it's not. It's a scam login page. You enter your info and click Log in. The page changes to the same looking page. This one **is** your real Bank of America login page. You log in, all seems OK. The problem is the first page was a fake that collected your login information. A day or 2 later, your accounts are drained. You assume you were hacked because you don't remember the incident from a few days ago. You were not hacked, you were **unknowingly** scammed. Never click on links in emails from banks, charge card companies or any financial institution. Close your email and log into that site like you have in the past or call your bank of financial institution to learn the truth.

Want to be a professional computer buyer, click below
http://www.comp-wizard.com/currentspecs.htm
As always, feel free to call with questions.

As always, feel free to call with questions.
Related helpful links:
Computer SCAMS Click HERE
Then, click OK if asked.
Want to be a professional computer buyer, click below
http://www.comp-wizard.com/currentspecs.htm
Windows 10/11 New Computer Configuration Special makes your new computer easier to use than any other.
http://www.comp-wizard.com/newcomp.html

*Microsoft ended support of Windows XP on 4/8/2014, Windows Vista on 4/11/2017, Windows 7 on 1/14/2020, Windows 8.1 on 1/10/2023. **Windows 10 will be supported until 10/14/2025**. Your computer and/or printer manufacturers & Anti-virus programs may also end their support. If you are still using Windows XP, Windows Vista, Windows 7 or Windows 8, YOU ARE AT RISK TO ALL NEW WINDOWS VULNERABILITIES .