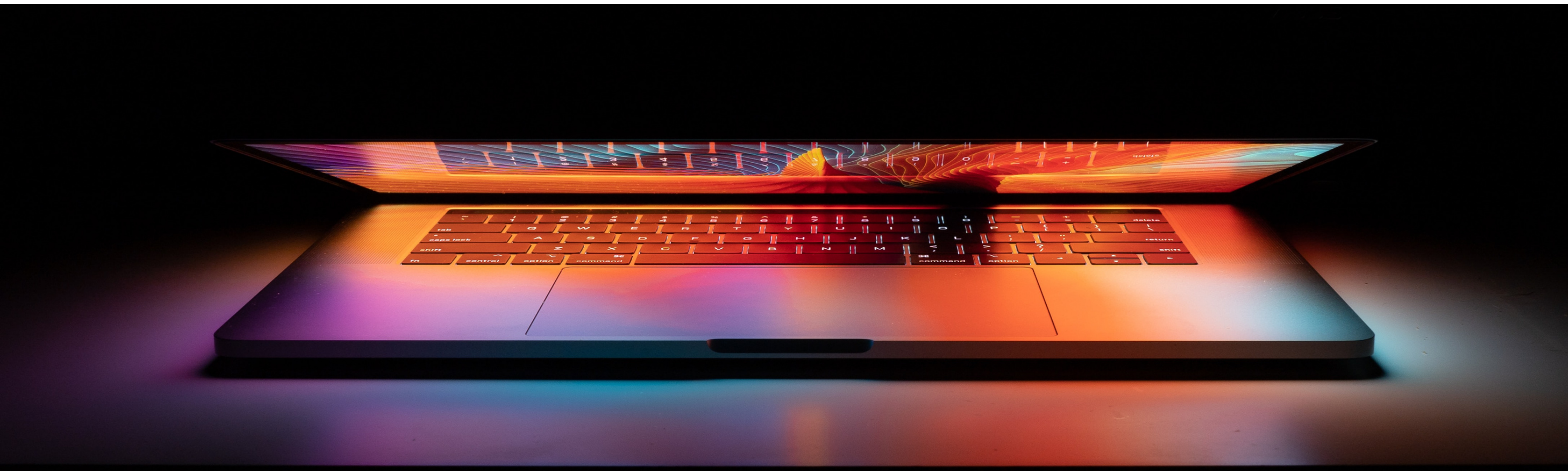
PLUMAS COUNTY TECH TIPS

WHAT YOU NEED TO KNOW ABOUT TECHNOLOGY TODAY



INSIDE THIS ISSUE:

CONTACT US:

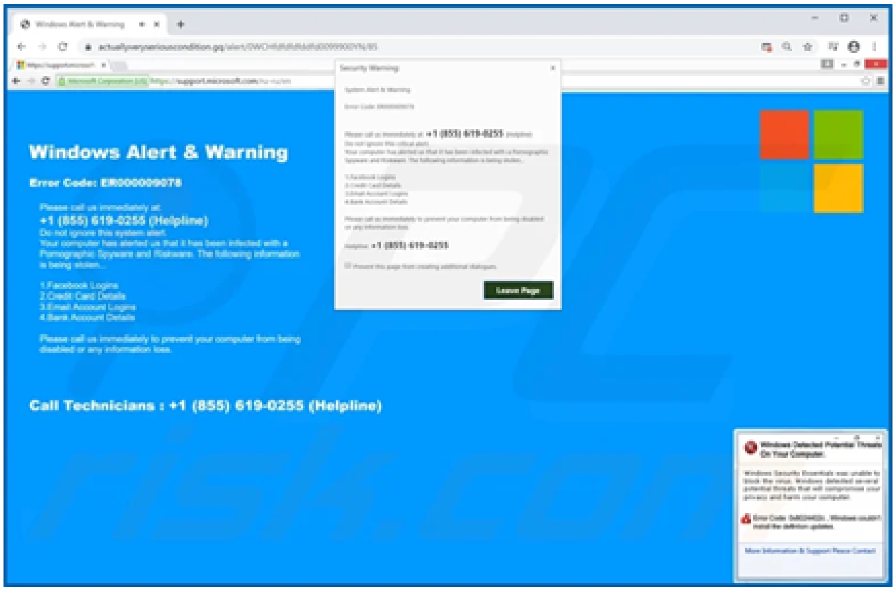
HANIF	(530) 283-**6263**
MELODIE	(530) 283-**6147**
JEREMIAH	(530) 283-**6335**
GREG	(530) 283-**6336**

Moving Offices? Call us FIRST!

If you move your phone or computer without informing IT first, you won't have internet/domain connectivity due to port security. Port Security helps secure our network by preventing unknown devices from connecting to it. So, only recognized, and trusted devices on certain offices (ports) are allowed to send/receive traffic. Therefore, if you want to change your offices or even re-arrange and plug your devices into another port in your office space, you need to inform IT *PRIOR* to the move, otherwise your devices will not work. In another word, the ethernet plug of your office will only work for your system, not for anyone else.

Fake Virus Warnings: How to Spot and Avoid Them

Fake virus warnings are a nuisance, and if you're not careful they can lead to real malware. Hackers design scareware to trick victims into clicking on the fake virus alerts and inadvertently installing real malware. Learn the signs of fake virus threats and how to handle them — then protect yourself with antivirus software with real-time protection


Windows Alert & Warning
actuallyveryseriouscondition.gq/alert/
https://support.microsoft.com/ru-ru/en

Windows Alert & Warning

Error Code: ER000009078

Please call us immediately at:
+1 (855) 619-0255 (Helpline)
Do not ignore this system alert.
Your computer has alerted us that it has been infected with a Pornographic Spyware and Riskware. The following information is being stolen...

1.Facebook Logins
2.Credit Card Details
3.Email Account Logins
4.Bank Account Details

Please call us immediately to prevent your computer from being disabled or any information loss.

Call Technicians : +1 (855) 619-0255 (Helpline)

Security Warning

System Alert & Warning

Error Code: ER000009078

Please call us immediately at: +1 (855) 619-0255 (Helpline)
Do not ignore this critical alert.
Your computer has alerted us that it has been infected with a Pornographic Spyware and Riskware. The following information is being stolen...

1.Facebook Logins
2.Credit Card Details
3.Email Account Logins
4.Bank Account Details

Please call us immediately to prevent your computer from being disabled or any information loss.

Helpline: +1 (855) 619-0255

☐ Prevent this page from creating additional dialogues.

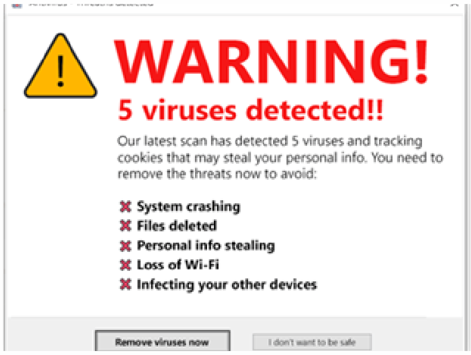
Leave Page

Windows Detected Potential Threats On Your Computer

Windows Security Essentials was unable to block the virus. Windows detected several potential threats that will compromise your privacy and harm your computer.

Error Code: 0x8024402c , Windows couldn't install the definition updates.

More Information & Support Please Contact



WARNING!

5 viruses detected!!

Our latest scan has detected 5 viruses and tracking cookies that may steal your personal info. You need to remove the threats now to avoid:

- ✖ System crashing
- ✖ Files deleted
- ✖ Personal info stealing
- ✖ Loss of Wi-Fi
- ✖ Infecting your other devices

Remove viruses now | I don't want to be safe

Phony computer virus alerts make you think your device is infected with malware then trick you into clicking a link that could cause a real malware infection.

A fake virus warning is a form of scareware that uses social engineering tricks to play on your emotions and cause panic. If you believe your device is infected with a computer virus, you might act without thinking and accidentally download harmful software.

Signs of Fake Viruses

Fake virus alerts can be convincing, but there are some dead giveaways. Understanding these tell-tale signs can help you avoid engaging with the phony pop-up warnings and clicking on the dangerous links. In general, trust your instincts — if something looks off, it probably is.

Here are signs of a fake virus:

- **Fake-sounding products:** Fake virus warnings usually aren't sophisticated. They often hawk products that are obviously fake.
- **High-frequency alerts:** A sudden blast of virus warnings is alarming. But this is a common adware ploy. The aim is to make you nervous enough to download their fake product.
- **Many viruses detected:** Fake virus pop-ups are not subtle. If you're getting alerts that your computer has a number of malware infections, it's likely a trick to inspire panic.
- **Vague wording:** Vague promises or product descriptions are suspect. A reputable antivirus solution will use clear language to describe its product and features.

What to do next if you encounter to this situation

The best way to keep your system safe in such a matter is not doing anything on your system and get in contact with the IT staff. However, if you are a tech savvy, you may carefully close the current tab on the browser without clicking on any part of the webpage.

URL Hijacking

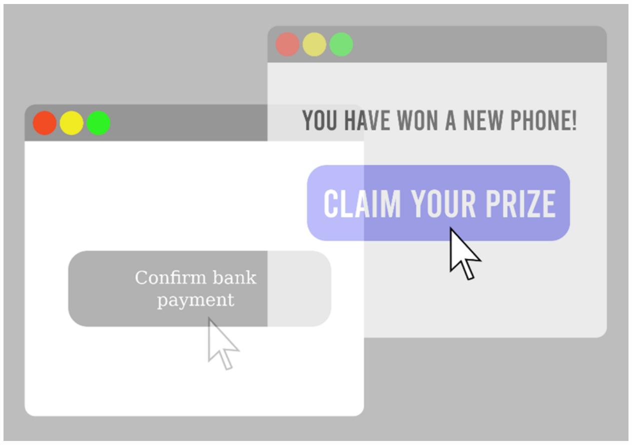
There are several tactics a cybercriminal may employ to gather URLs. This includes:

- **Typos** - It's common for a user to accidentally mistype a domain (e.g. "tiwtter.com" instead of "twitter.com") or simply not know how to spell a brand name, such as Louis Vuitton.
- **Alternative Spellings** - Different English-speaking countries, and even different regions within those countries, have alternative spellings of certain words—colors vs. colours, grey/gray, pediatric/paediatric, et al.
- **Hyphenated Domains** - Cybercriminals will also add hyphens between words within a domain (i.e., onepeloton.com vs. one-peloton.com) in an attempt to maintain the same spelling and perceived credibility.
- **Alternative Domain Extensions** - A simple swap of ".net" for ".com" allows many false websites go undetected.
- **False "www" Tags** - Most hijacked URLs won't be able to maintain a "www" tag, but they can pretend they have one. You may see some websites with "www" thrown on at the beginning of the domain name, like "wwwfacebook.com."

Click Hijacking

Clickjacking (classified as a user interface redress attack or UI redressing) is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages.

Clickjacking is an instance of the confused deputy problem, wherein a computer is tricked into misusing its authority.



Phishing Emails – Where do they go?

Do you ever wonder where the emails go when you use the Phish Alert Button (PAB)? All emails are sent to PhishER where they are sorted, scanned, and ultimately put into one of three categories – Threat, Spam, or Clean. If the email is categorized as a "Threat", our entire email server is scanned for the same sending address and/or subject and similar emails are removed before they can be opened in other email boxes. If the email is categorized as "Spam", the email stays deleted from your inbox and stays in the spam folder in PhishER. Both of these catagories are designed to remove unwanted emails from your inbox. If the email is categorized as "Clean", you'll receive an email back from me (Melodie) within 24-48 hours that the email is clean and you can proceed. PhishER also collects all of the data submitted to them and they develop simulated phishing emails that reflect real-time threats for better training experiences. If you're in doubt whether to Phish Alert an email or not, err on the side of caution and PAB it, The more emails you report through the Phish Alert Button, the more it benefits us all! Remember - all emails from @knowbe4.com are legitimate, please don't PAB them.