



Methownet.com – Connecting the Methow Valley since 1995

Newsletter, January 2023

From our office to your warm hearth, Happy New Year! We thought we'd start off the year addressing recent concerns and commonly asked questions. As always, we are here to help - call our office at 509-996-2022 at anytime to chat with our helpful team. We appreciate you!

Those Rascally Scammers

How to recognize a scam and avoid the hassle

It is not your imagination. Scam messages are more frequent and personal than ever before. Scammers spoof names and numbers that at first glance appear to come from a familiar source. Here are the three most common methods scammers use to try to connect with you, and what to do when it happens.

! PC frozen with alert warning and a message to call a phone number

These messages are as annoying as a dead battery alert in a fire alarm in the wee hours of the morning, but the alert itself will not hurt your computer. The messages may appear to come from a utility or computer company. These messages are intended to create a sense of urgency to call the number listed in the pop up screen and give the scammer an opportunity to gain remote access to the computer with your help.

How to stop the scam:

- 1) Do not call the number on the pop up screen.
- 2) Make note of the website address where the popup message appeared. Do not visit the website again.
- 3) Restart computer in safe mode – instructions [here](#)
- 4) Download a free, powerful cleaner from www.ccleaner.com to remove malware

! Email message

The message may sound urgent, contain an invoice you do not recognize, and request a return phone call or click on a link. These email messages are intended to create a sense of urgency for you to call the number or visit the link. Do neither. If you receive a suspicious email, verify the return address and domain name. These emails can be safely deleted and will not hurt your computer.

For example:

From: Geek Squad Tech Support <hoachilebinh04@gmail.com>

To: joanna@methownet.com

Notice that the return email address does not contain the company name.

Read more from the SysAdmin, Audit, Network and Security newsletter [here](#)

! Text Messages

It is illegal to spoof numbers, but scammers have no scruples. A common crime is to make a call or text look like a local number. Some common scams are to start a conversation before asking for money or personal information. A "Package Delivery" scam looks like a text from a delivery service about a package. More information from the FCC [here](#).