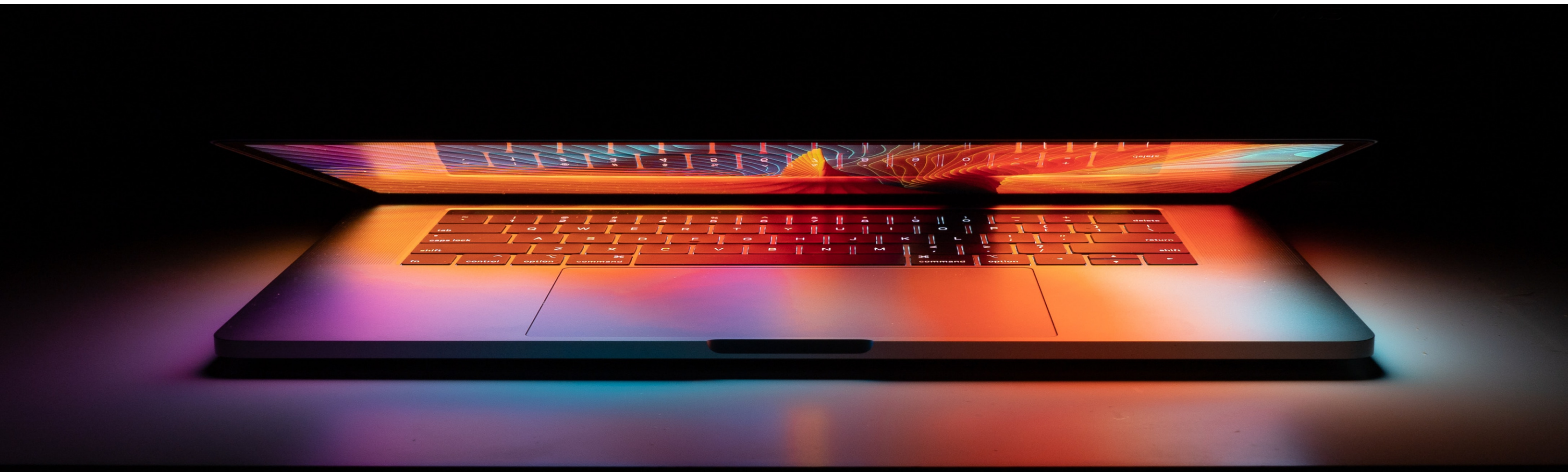
PLUMAS COUNTY TECH TIPS

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

Welcome!

Welcome to Plumas County Information Technology's monthly newsletter. In these newsletters, we will be reminding you of security best practices, technology issues you should be aware of, and general training.

Need I.T.'s help?

Don't forget to use our FreshService Ticketing system. It's not that we don't like emails or phone calls, it just helps us track projects better and helps us not forget about you! Everyone should have a red dot icon on thier desktop that will direct you to the ticketing system. You can always bookmark this link as well: https://plumascountyca.freshservice.com

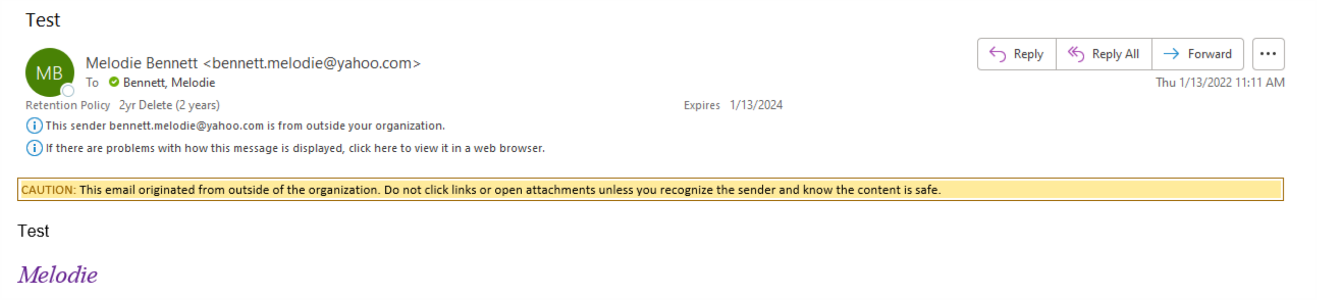
Suspicious Emails and How to Tell Where They Come From...

Have you ever received a suspicious email and wondered how to tell if it was legit or not? One of the first indicators you'll want to look at is whether the email came from inside of the organization or outside of the organization. With the new email system, we've made it easier than ever to tell the difference. If you receive an email from outside of countyofplumas.com, you'll now see a large "CAUTION" banner highlighted in yellow. (See the image below for an example of what the banner looks like). This is your first clue that the email could be spam, especially if it has the name of a co-worker but comes through with the yellow caution banner.

Other indicators of spam could include, but are not limited to:

-an unfamiliar tone or greeting
-grammar and spelling errors
-inconsistencies in email addresses
-threats or sense of urgency

The best option is to always be alert and if it looks suspicious, forward it to an I.T. team member to look at.



Test

MB Melodie Bennett <bennett.melodie@yahoo.com>
To Bennett, Melodie
Thu 1/13/2022 11:11 AM
Retention Policy 2yr Delete (2 years) Expires 1/13/2024
This sender bennett.melodie@yahoo.com is from outside your organization.
If there are problems with how this message is displayed, click here to view it in a web browser.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Test

Melodie

What is a VPN and when do you need one?

The main purpose of a Virtual Private Network or VPN is to hide your online activity. VPNs are often used to guard against hackers and snoops on public networks, but they're also useful for hiding your IP address, browsing activity, and personal data on any Wi-Fi network — even at home.

The main reason you'd want to use a VPN while working for the county is to securely access your desktop for programs hosted on the County servers such as Megabyte, HAL, etc., to access any documents you may have on your work desktop, and to access shared folder(s) on County servers.

It is not necessary to have a VPN to work remotely. Please be aware that to set up a VPN on your work laptop, you must be able to download an app on your smartphone for multi-factor authentication (for security purposes). Starting January 2022, I.T. will be charging a $4.00 per month, per user fee which will be billed to your department. For additional questions, please reach out to I.T.

Cybersecurity Awareness - Removable Media and Devices

Removable media and devices are portable hardware (such as CDs, DVDs, etc.). The most common is a USB flash drive but other forms could be an external hard drive or SD card. While useful, these devices can also be easily weaponized by an attacker and pose a significant cyber risk to an organization. Removable media can be weaponized in several different ways. These range from delivering malware to stealing data to physically destroying the computer that they are inserted into.

When it comes to cybersecurity best practices, removable media and devices must NOT be plugged into your computer unless approved by I.T. For example, if you found a USB flash drive in the grass near your office, there's a chance it wasn't dropped there by accident but planted there. A cyber attacker would try to social engineer someone into plugging the device into a computer. Whether the intention is to find out who it belongs to or keep it, the attacker wins and could successfully execute whatever malicious software might be pre-installed on the removable media or device.

Using removable media, like a flash drive, can be dangerous within an organization because the malware is able to bypass the security solution that is deployed at an organization's network perimeter. USB drives are the best ways for hackers to exfiltrate sensitive data from an organization and are more difficult to detect. Each time that a removable media device is used, there is a possibility that a computer may become infected.

We ask that you please be aware of this information and if you have any questions, we are happy to answer them.