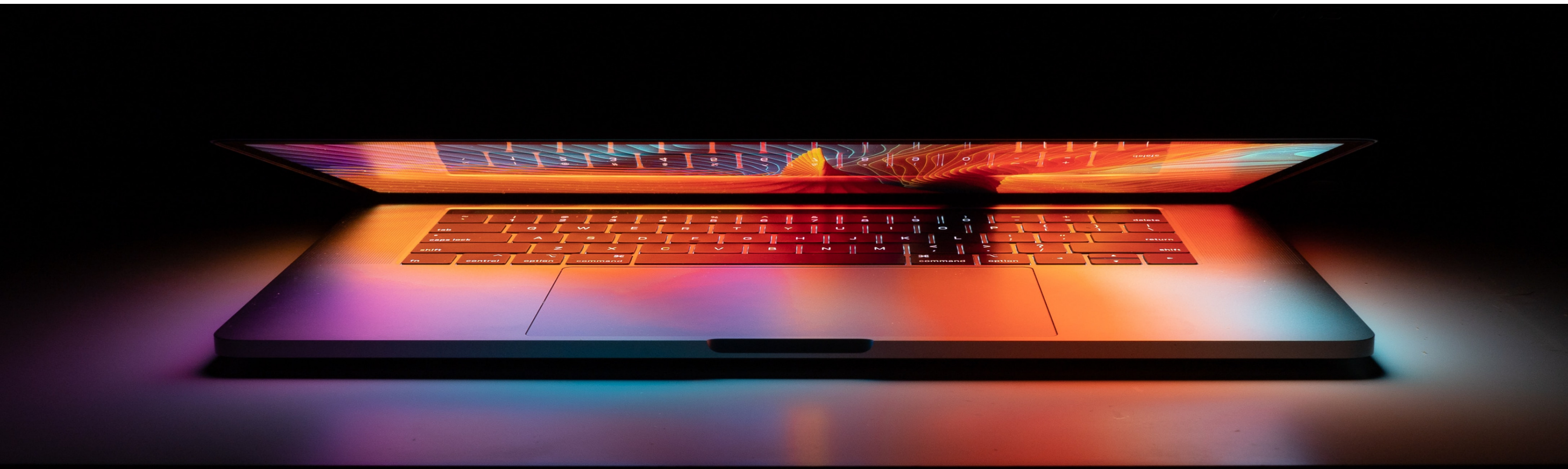
PLUMAS COUNTY TECH TIPS

WHAT YOU NEED TO KNOW ABOUT TECHNOLOGY TODAY



CONTACT US:

HANIF - (530) 283-**6263**

MELODIE - (530) 283-**6147**

JEREMIAH - (530) 283-**6335**

GREG - (530) 283-**6336**

Junk Email

Like you, I receive an inordinate amount of emails that I don’t ask for or want, but sometimes I find something of interest that I will verify before clicking on anything. However, more often than not the emails are unsolicited junk from vendors of whom I have never heard. I often use Block Sender to prevent the senders from filling my mailbox with the “Why haven’t you answered me?” emails.

If you haven’t done this, here is how:

1. Right-click on the message preview and scroll down to Junk.
2. Hover over Junk, then click Block Sender.
3. You will get a message telling you that the address has been added to your Blocked Senders List and the message has been moved to the Junk folder.

What have we been up to in IT recently?

Our backup server, Cohesity, has been installed and we are knee-deep in setting up backups for all Plumas County servers. So, what is Cohesity and what does it mean for you? Cohesity DataProtect is a modern, software-defined solution for protecting all of our data sources. With a platform built for scale and performance, Cohesity dramatically simplifies backups, reduces costs, makes instant recovery possible, and ensures business continuity. This means that we will always have an immediate backup of data and in the case of a natural disaster, ransomware attack, etc. we can get back to normal operations right away without a significant delay in services or data loss.

The Board of Supervisor's room is getting an audio/visual upgrade! We are slowly implementing pieces of audio and visual equipment as the supply chain allows. This means that any meetings held in the Board of Supervisor's room will be much easier to see and hear, especially if viewing the meetings remotely. Soon, the audio will be crystal clear and the entire room will be much more functional.

We are planning a major Office Suite upgrade for all Plumas County employees in June. All employees will be upgraded to the Office 365 Standard Business subscription which includes fully installed, and always up-to-date versions of Outlook, Word, Excel, PowerPoint, and OneNote. The upgrade also creates a hub for teamwork using Microsoft Teams, shared cloud storage accessible whenever and wherever with SharePoint, and individual cloud storage with OneDrive. You'll also be able to use one license to fully cover installed Office apps on 5 devices. We have already started implementing these changes in some departments but expect to have everyone on board by the end of July.

A Friendly Reminder...

Cybersecurity threats are always changing and staying on top of them is vital. Please continue to follow the general guidelines we are often sharing with you:

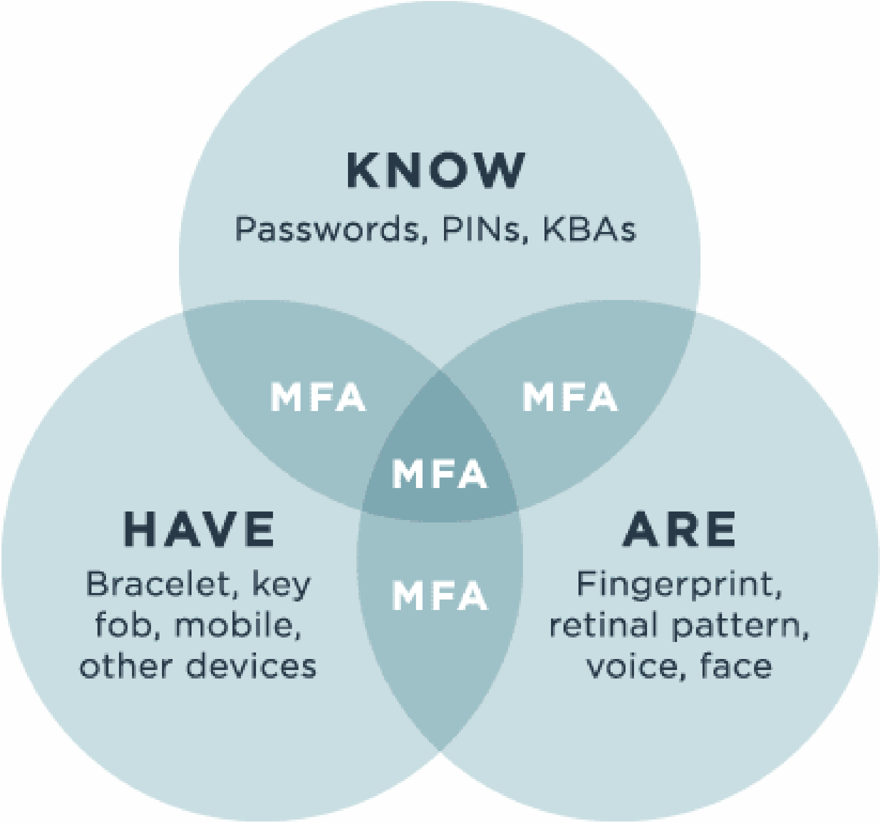
1. Do **NOT** provide your password to anyone, whether it is online, over the phone, in person, or otherwise.
   - Your bank will never ask for this.
   - Your credit card companies will never ask for this.
   - Utility companies will never ask for this.
2. Do **NOT** click on questionable links in emails you are not sure about.
3. Do **NOT** open attachments in emails from anyone at all unless you are expecting it.
4. Do **NOT** use the same passwords for multiple accounts.
   - If you think your password has been compromised for any account, change it right away.
5. Contact us at any time if you have **ANY** doubts about an email or link.
6. You can forward questionable emails to any of us in IT because we can give you advice without having to open the attachment.
7. Do not click on links within websites if you are unsure about them.
   - Spoofed sites can be made to look like the real site, so please be extra cautious.
8. Remember that phishing does not have to come from an email. Hackers use texts and phone calls, too!
9. If someone claims to be a vendor and they call asking questions about our data or business, do **NOT** give that information out.
   - If you didn't ask these people to call you, why would you share information with them?
   - Many of these "vendor" emails I get are from companies I have never heard of before and I bet the same is true for everyone else.

How does Multi-Factor Work?

A user's credentials must come from at least two of three different categories, or factors. Two-factor authentication, or 2FA, is a subset of MFA where only two credentials are required, but MFA can use any number of factors.

What you know (knowledge)
The most common example of this factor is, of course, the password, but it could also take the form of a PIN, or even a passphrase--something only you would know.

Some organizations may also set up knowledge-based authentication like security questions (e.g., "What is your mother's maiden name?"), but basic personal information can often be discovered or stolen through research, phishing and social engineering, making it less than ideal as an authentication method on its own.


KNOW
Passwords, PINs, KBAs
MFA
MFA
MFA
HAVE
Bracelet, key fob, mobile, other devices
MFA
ARE
Fingerprint, retinal pattern, voice, face

What you have (possession)
It's much less likely that a hacker has stolen your password and stolen something physical from you, so this factor confirms that you are in possession of a specific item. This category includes mobile phones, physical tokens, key fobs and smartcards.

There are a few ways that this authentication works, depending on the item, but some common methods include confirming via a mobile app or pop-up notifications from your mobile phone, typing in a unique code generated by a physical token, or inserting a card (e.g., at an ATM).

What you are (inheritance)
This factor is commonly verified by a fingerprint scan on a mobile phone, but also includes anything that would be a unique identifier of your physical person--a retinal scan, voice or facial recognition, and any other kind of biometrics.

There are a lot of possibilities spread across these three categories, and different authentication mechanisms may be better for different companies depending on their unique needs and use cases. By evaluating the relative strength, costs and benefits to both IT and users, an organization can find the combination that works best for them and their users.