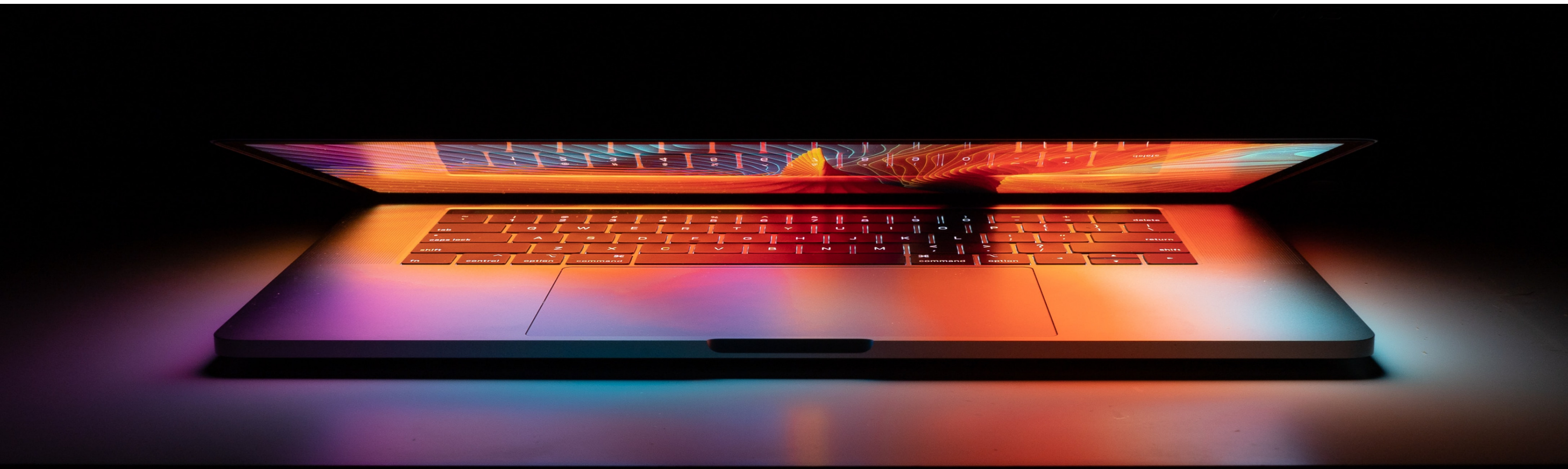
PLUMAS COUNTY TECH TIPS

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**

Cybersecurity Reminder

If it feels like you are seeing cyber security issues in the news almost every single day, it is because you almost certainly are. Research shows that cyber attacks occur at a rate of around one every 39 seconds and these attacks are indiscriminate. What this means is simple: if you have an internet-connected device, you are vulnerable.

This should be of real concern to all of us. After all, we put a huge amount of personal data out there in digital form, and businesses are entrusted with keeping our information safe and secure. Additionally, a cyber attack will jeopardize our day-to-day operations, resulting in disruption and, if successful, loss of revenue.

With this in mind, we ask you to keep remaining vigilant and participate in the monthly KnowBe4 trainings. The scale of cyber threat is continuing to grow and won't be slowing down anytime soon. Managing our cyber security is critical and it’s the only way to keep out the hackers and scammers. Let’s not let them win!

Don’t save important documents in your scan folder!

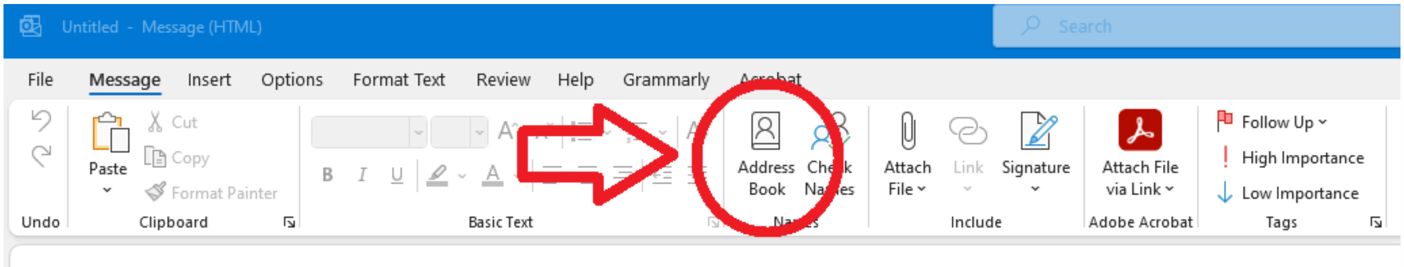
Security is a key aspect of any business, and outbound document security is no exception. There are many more reasons not to risk document security, including:

- Minimizing the risk of a data breach
- The financial impact of a data breach
- Customer confidence in your products and services
- Reputational damage
- The rise of cybercrime

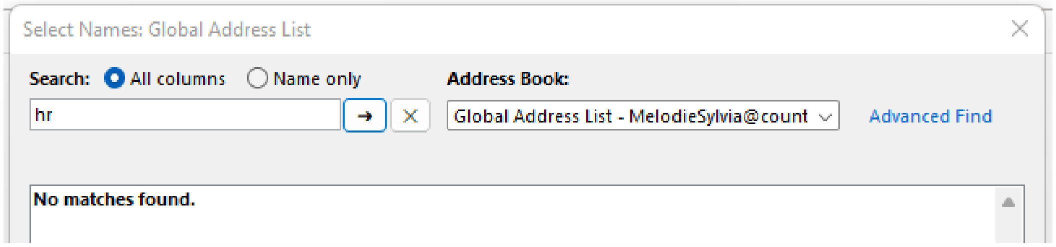
While you scan folder is handy to scan and send documents, it shouldn’t be a holding folder for documents. Once you have done what needs to be done with the document, **we highly recommend you either delete the document from your scan folder or move it to your PC**. Since you have a physical copy of the document, there is no need to keep it in your scan folder. If we continue finding personally identifiable information (PII) we will have to implement daily purges of scan folder documents. So please, make sure your scan folder is empty as soon as you’re done with the document.

How do I know if an email I get is from a legitimate @countyofplumas.com address?

A lot of the recent phishing tests spoof an @countyofplumas.com email address, so how do you tell if the address is legitimate or not? The easiest way is to check the address book in Outlook. When you create a new email, the “Address Book” is at the top of the new message ribbon:



From the “Address Book” drop-down, choose “Global Address List – your email address”. Say you got a suspicious email from hr@countyofplumas.com. Search for “hr” in the search bar and click the arrow to search. As you can see in this instance, no matches were found:



Search: ● All columns ○ Name only

hr

Address Book: Global Address List - MelodieSylvia@count

No matches found.

This means that hr@countyofplumas.com is not a real email address. Next time you get an email from an @countyofplumas.com email address that doesn’t look familiar, try searching for it before you click on any links in the email.

Cybersecurity Awareness Month Wrap Up

In 2004, the President and Congress declared October to be Cybersecurity Awareness Month and we have been celebrating this ever since. The purpose of Cybersecurity Awareness Month is to help individuals protect themselves online as threats to information technology and confidential data become more common. The Cybersecurity and Infrastructure Security Alliance (CISA) and the National Cybersecurity Alliance (NCA) lead a collaborative effort between government and industry to raise cybersecurity awareness nationally and internationally. This is particularly important with all the things that are going on around the world.

This year's theme was "See Yourself in Cyber" and CISA says that it demonstrates that while cybersecurity may seem like a complex subject, ultimately it is about all people. This October we've focused on the "people" part of cybersecurity. As we wrap up the month, here are a few friendly reminders of what we've covered:

Week 1: Cyber Secure at Work

- A reminder to "Stop! Look! Think!". Stop – resist immediate action when receiving an email or text. Look – check for anything unusual in the message. Think – if something seems "phishy", report it immediately.
- Some actions to stay safe:
  - Be careful what you post and share online.
  - Don't reuse passwords for multiple sites.
  - Follow your organization's security policies and procedures.
  - If something seems suspicious, always verify that it's legitimate.

Week 2: Watch Out for That Phish

- When in doubt, check it out!
- Ask yourself these questions before you share any information:
  - Are all the facts accurate?
  - Is the author credible?
  - Is the headline trying to cause a strong emotional reaction?
  - Is the date current?
  - Has the image been altered?
  - Is the source of the information legitimate?

Week 3: More Than Just Phishing

- Think before you click.
- Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!
- Sensitive Identifiable Information – If you handle it, protect it!

Week 4: Cyber Secure at Home

- Cybercrime happens way more than you think!
- Again, think before you click!!!
- Follow these steps when working from home:
  - Use strong, unique passwords for every account.
  - Update software and enable automatic updates where available.
  - Secure your devices when not in use.
  - Remain skeptical of all requests for sensitive information.
  - Keep your work-related data separate from your personal data.
  - Pump up your password strength.
  - Don't share your password.
  - Change your password regularly.
  - Make passwords hard to guess.
  - Use a different password for each app and website.