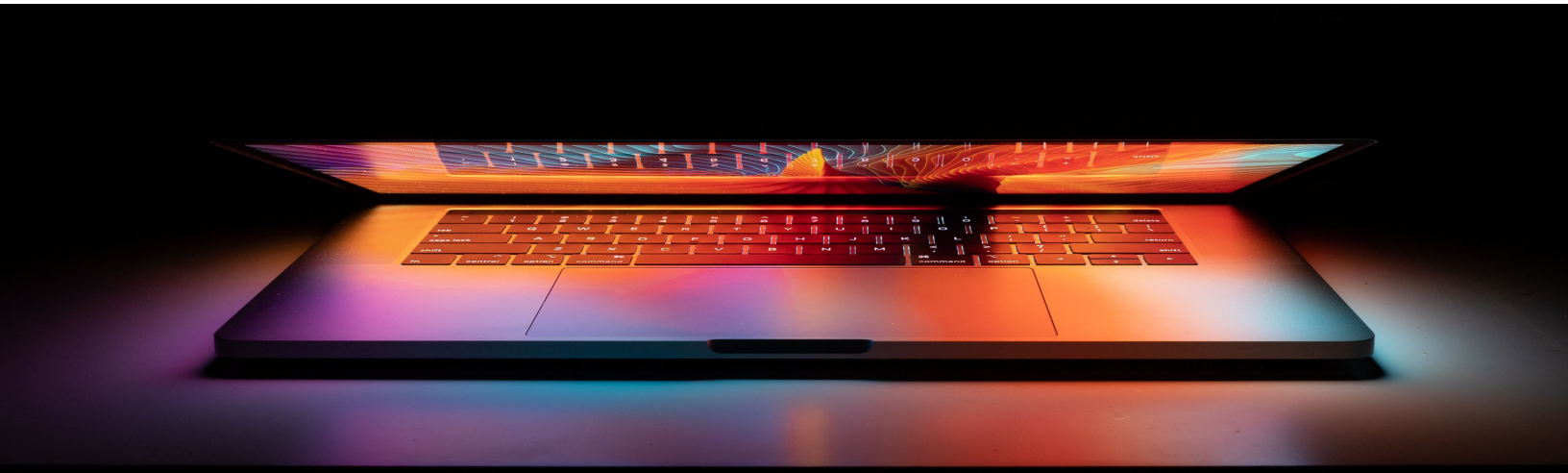
PLUMAS COUNTY TECH TIPS

WHAT YOU NEED TO KNOW ABOUT TECHNOLOGY TODAY



INSIDE THIS ISSUE:

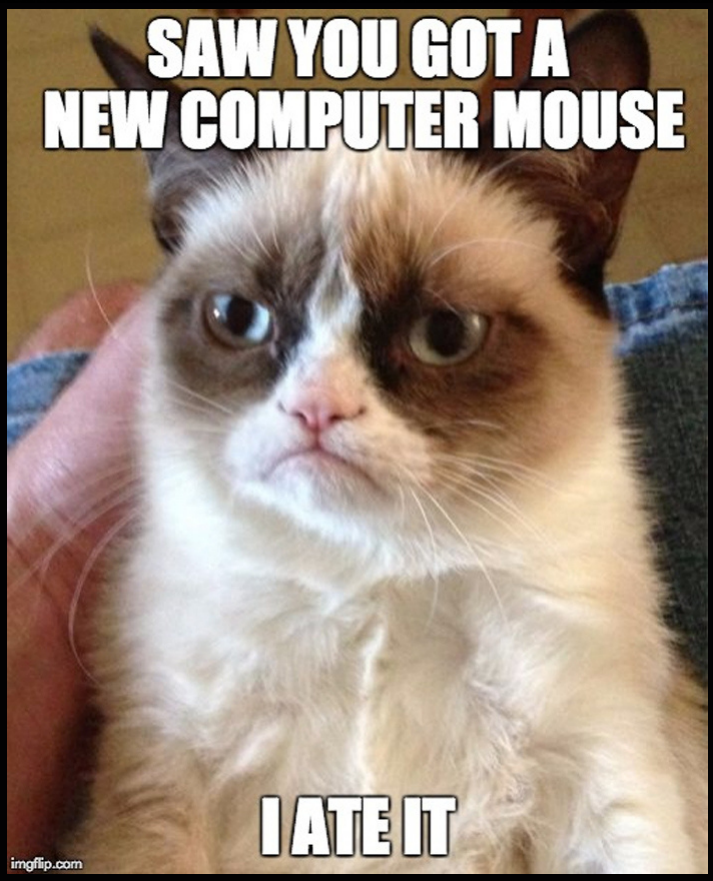
CONTACT US:

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

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

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

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



I.T. Security Checklist

This month, we wanted to share some basic security items you should always be thinking about when it comes to technology. Check out the following list and see how many items you can check-off! For those items that you can't check-off, consider finding ways that you can check them off in the future.

Basic Security Checklist Items

- Read and familiarize yourself with the Plumas County Acceptable Use Policy.
- Do not share County computers or mobile devices with others.
- Set a strong password for all devices.
- Use multi-factor authentication (MFA) whenever possible.
- Keep your work and personal accounts separate whenever possible.
- Adjust privacy settings. Your devices, apps, and browsers, all come with default privacy and security settings. Make sure you thoroughly go through them and limit access to sensitive data. Do not permit location tracking or camera and audio access unless necessary.
- Immediately report anything suspicious, including unauthorized access or suspicious activity, to I.T.

Secure Your Workstation

- Never allow a third party to use a workstation or otherwise access or use your systems and data without supervision and appropriate contractual protections.
- Do not download or install unauthorized or unapproved software or applications from the Internet.
- All confidential, proprietary, and sensitive information should be encrypted or otherwise secured.
- Never plug in or transfer sensitive County information to a mobile storage device (e.g., a CD, USB drive, etc.)
- When submitting personal or other sensitive information via a website, make sure you see the site's address begin with "https," as opposed to "http." Think "s" stands for secure. "Https" uses encryption to send information across the Internet, thus, reducing the risk that the information will be improperly accessed.
- Think before you submit. Once submitted to a website or transmitted through an online communication service, the information is public. You never know where the information will show up. There is no such thing as deleting information from the Internet. The Internet is forever.

Follow Password Protocol

- Use a minimum 14-character passphrases for passwords, with a mix of numbers and special characters.
- Don't include personal information in the passphrases. (e.g., birthday, pet's name, maiden name)
- Do not reuse passwords for multiple accounts - use unique passwords for all your accounts.
- Do not write down or store your passwords unencrypted.
- Change your passwords on a regular basis.

Audit your inbox

- Periodically go through all your inboxes and delete spam/junk emails.
- Check for phishing emails with signs of urgency in the messaging, incorrect email domain or senders, typos in the email body, and suspicious attachments and links, especially in emails that ask for sensitive information about you or the County.
- Always proceed with the understanding that no public email or messaging service (e.g., services provided by online services such as Google, Yahoo!, Skype, and others) is secure and that all communications will be stored and, potentially, viewed by others.
- Avoid sending highly sensitive information through unsecured email.
- Do not forward internal emails, documents, or other information to a personal email address or download it to personal devices for access outside of our systems. We cannot protect the information once it is removed or shared outside our systems.
- Do not get hooked on someone's fishing line. Do not reply to or click on links in emails, pop-ups, or websites that ask for personal information, or health information. Never click on links or open files in an email from someone you do not know or were not expecting.
- Think before you open. If you do not know the sender, are unsure of why the attachment was sent, or if it looks suspicious, do not open the attachment. Better to verify with the sender than infect your computer, or worse, the network.
- PDF files are a very popular way of distributing viruses. Before opening a PDF, be sure you know where it came from.
- Watch out for phishing emails and phone scams.

Lock Devices, Clear Desks

- Lock all your electronic devices that may contain sensitive information, such as laptops, mobile phones, and tablets, when not in use.
- Make sure you don't leave sensitive data such as passwords, account details, or contracts, on your desk in case an attacker enters your workplace.
- Maintain a clean workspace. Putting sensitive information out of sight helps to protect it from accidentally being viewed.
- Lock your screen whenever you step away from your computer. Quick tip – press the Windows key and the "L" key at the same time to quickly lock your computer.

Report concerns and ask questions!

A Few Friendly Reminders from I.T.

Phones - Did you know that when you want to call a county co-worker, you don't have to type in (530) 283-extension? Simply dial the last 4 digits of the phone number. Not only is this the easiest way to dial a co-worker, but it also alerts them to who is calling. Check it out for yourself!

Don't forget to Encrypt Sensitive Emails - Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than the intended recipients. So how does it work? All you need to do is include "Encrypt, Encrypted, or Encryption" in the subject line of your email.