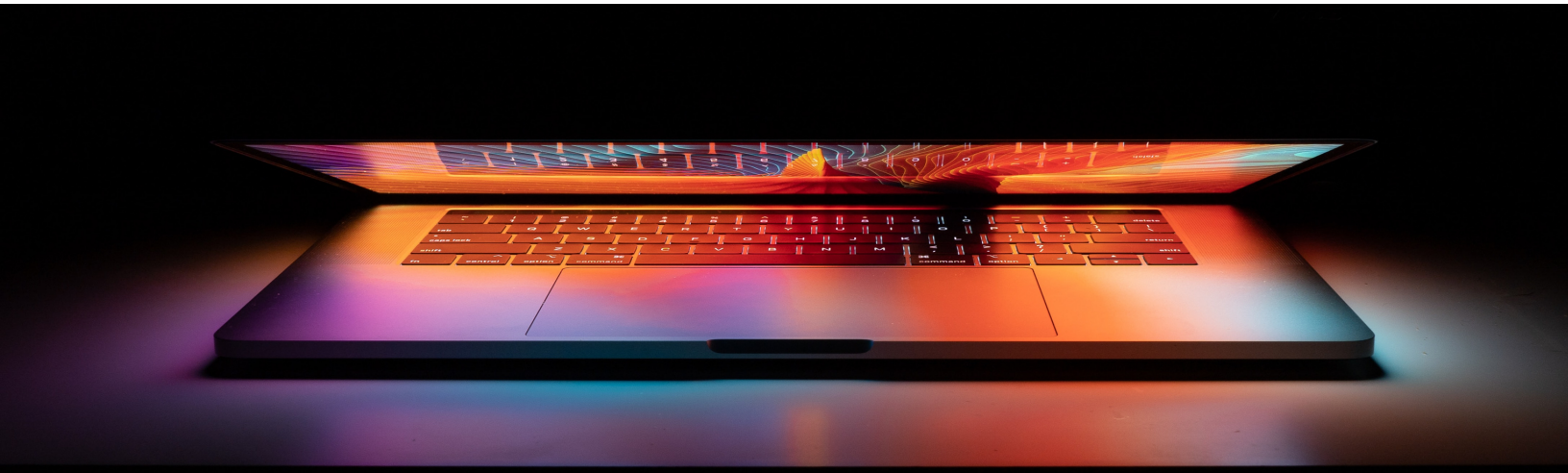
PLUMAS COUNTY TECH TIPS

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**

Transitioning to SharePoint

SharePoint is web-based collaboration and document management platform. Though highly flexible, it is primarily used to store documents, and communicate information across organizations. The main way we are going to implement SharePoint at the County is to transfer any department-shared folders currently on our server Oscar to SharePoint. This means that if you are currently a member of a department shared folder, you will soon be receiving an email welcoming you to the SharePoint group specific to your department. (Please note that some departments have already been transitioned over.) I will be reaching out to link the SharePoint to your individual OneDrive accounts so that the file structure looks exactly the same as the shared folders.

Transitioning to SharePoint (continued)

We know change can be scary, but this is a major security improvement that actually gives you more collaboration tools. By moving to SharePoint, multiple employees can work on the same document at the same time, it is extremely easy to share documents with others both inside and outside the county, everything is stored on a cloud server which means more storage for everyone, and the SharePoint sites and documents are only accessible by members of the group. If you are interested in learning more about SharePoint, we highly recommend visiting this website for some great resources: https://365trainingportal.com/sharepoint/

Phish Alert Button

Thank you to everyone who has completed the Phish Alert Button (PAB) training and those that are actively using the button! You all have reported over 87 suspicious emails since rolling out the program, and 8 of those emails have been deemed high-level threats. This means that you are helping us prevent potentially catastrophic breaches. When you use the button to report a suspicious email to KnowBe4, the email is scanned for potential threats. If the email is found to be clean, you'll receive an email back from me letting you know that it is clean and nothing to be worried about. If the email is found to be a threat, our entire Microsoft 365 domain is then searched for the same parameters as the threat email and automatically deleted from all email inboxes it went to. The more emails you report, the more data KnowBe4 collects and helps clean out of our system. A few things to keep in mind:

1. Emails in your "Junk email" folder do not need to be reported with the PAB. If they are already flowing into "junk", Microsoft has already deemed them as potential spam, etc. so there is no need to report it.
2. You won't receive a reply to every email you report using the PAB. If you don't receive a reply to an email you reported, the email is either spam or a threat and you've done all you need to do.
3. If you use Outlook and still don't see the PAB, call us and we'll install it for you.

The next step on our journey to become more educated on cybersecurity awareness is to take a Security Awareness Proficiency Assessment. This is another required training that is expected to take 10 minutes of your time. You'll receive an email from KnowBe4 that you've been registered for the training on Tuesday, September 6th and you'll have three weeks to complete the assessment. This will help guide us through what cybersecurity issues are most important to you. As always, if you have any questions or need assistance of any kind related to KnowBe4, please let us know.

Should I Connect to Public Wi-Fi?

Wi-Fi users are at risk from hackers, but fortunately, there are safeguards against them. The recent explosion of free, public Wi-Fi has been an enormous boon for working professionals. Since these free access points are available at restaurants, hotels, airports, bookstores, and even random retail outlets, you are rarely more than a short trip away from access to your network and your work. This freedom comes at a price, though, and few truly understand the public Wi-Fi risks associated with these connections. Learning how to protect yourself will ensure your important business data remains safe.

The Risks of a Public Wi-fi

The same features that make free Wi-Fi hotspots desirable for consumers make them desirable for hackers; namely, it requires no authentication to establish a network connection. This creates an amazing opportunity for the hacker to get unfettered access to unsecured devices on the same network.

The biggest threat to free Wi-Fi security is the ability of the hacker to position himself between you and the connection point. So instead of talking directly with the hotspot, you're sending your information to the hacker, who then relays it on.

While working in this setup, the hacker has access to every piece of information you're sending out on the Internet: important emails, credit card information, and even security credentials to your business network. Once the hacker has that information, they can — at their leisure — access your systems as if they were you.

Hackers can also use an unsecured Wi-Fi connection to distribute malware. If you allow file-sharing across a network, the hacker can easily plant infected software on your computer. Some ingenious hackers have even managed to hack the connection point itself, causing a pop-up window to appear during the connection process offering an upgrade to a piece of popular software. Clicking the window installs the malware.

As mobile Wi-Fi becomes increasingly common, you can expect Internet security issues and public Wi-Fi risks to grow over time. But this doesn't mean you have to stay away from free Wi-Fi and tether yourself to a desk again. The vast majority of hackers are simply going after easy targets, and taking a few precautions should keep your information safe.

Use a VPN - A virtual private network (VPN) connection is a must when connecting to your business through an unsecured connection, like a Wi-Fi hotspot. Even if a hacker manages to position himself in the middle of your connection, the data here will be strongly encrypted. Since most hackers are after an easy target, they'll likely discard stolen information rather than put it through a lengthy decryption process.

Turn Off Sharing - When connecting to the Internet at a public place, you're unlikely to want to share anything. You can turn off sharing from the system preferences or Control Panel, depending on your OS, or let Windows turn it off for you by choosing the "Public" option the first time you connect to a new, unsecured network.

Keep Wi-Fi Off When You Don't Need It - Even if you haven't actively connected to a network, the Wi-Fi hardware in your computer is still transmitting data between any network within range. There are security measures in place to prevent this minor communication from compromising you, but not all wireless routers are the same, and hackers can be a pretty smart bunch. If you're just using your computer to work on a Word or Excel document, keep your Wi-Fi off. As a bonus, you'll also experience a much longer battery life.

Stay Protected - Even individuals who take all the possible public Wi-Fi security precautions are going to run across issues from time to time. It's just a fact of life in this interconnected age. That's why it's imperative to keep a robust Internet security solution installed and running on your machine. These solutions can constantly run a malware scan on your files, and will always scan new files as they are downloaded.