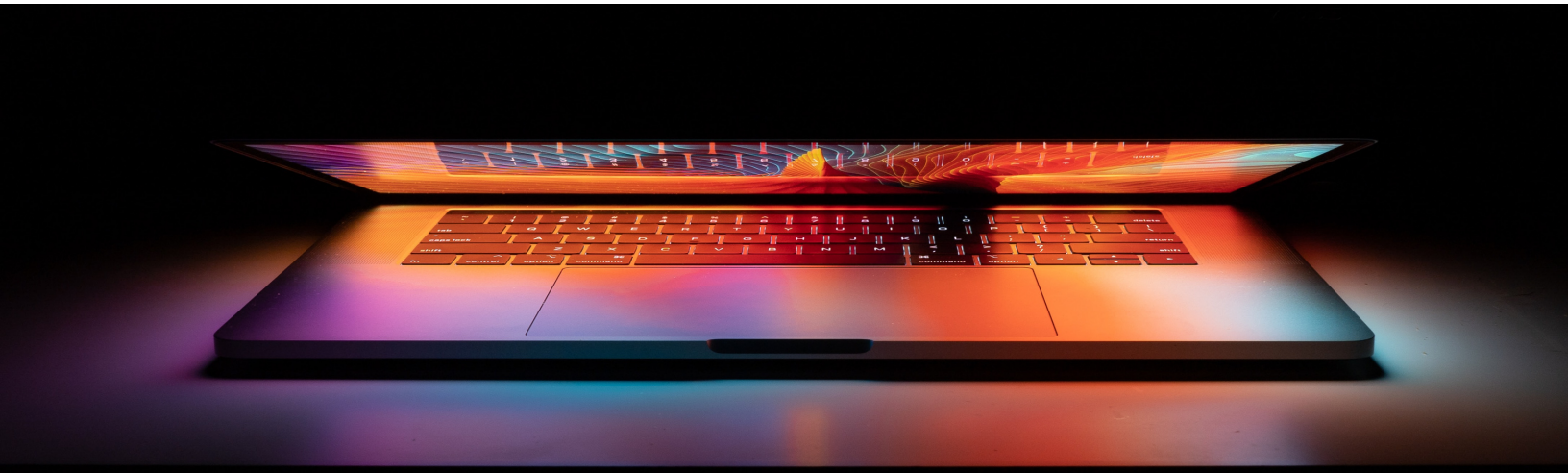
PLUMAS COUNTY TECH TIPS

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**

You've been phished?

Phishing is a type of cybercrime where hackers try to gain access to sensitive information, such as usernames and passwords, by pretending to be a person or organization they trust.

Cybercrime is getting more serious by the month. Hackers are getting better at tricking people into clicking on fraudulent links or opening up malicious attachments in emails.

According to the preliminary results from our initial baseline campaign, we are 13.2% phish-prone. The baseline phish-prone percentage is 15.5% for government entities so overall, we are doing pretty good. That's no reason to become lax though - more phishing tests are coming so be on the lookout. We'll also be installing a "Phish Alert" button in Outlook for everyone to easily report suspicious emails. Keep being vigilant and remember, this is intended as a way to learn what not to click on.

Microsoft 365

We've been hard at work getting everyone updated to the Microsoft 365 full business suite. With a subscription to Microsoft 365, you get:

- The latest Office apps, like Word, Excel, PowerPoint, and Outlook.
- The ability to install on PCs, Macs, tablets, and phones.
- 1 TB of OneDrive cloud storage.
- Feature updates and upgrades not available anywhere else.

As we make this transition, we want to make sure everyone has a better understanding of some of the major benefits/changes. You'll hear us talking about OneDrive and SharePoint a lot so here is a breakdown of what they are:

What is SharePoint?
SharePoint is primarily known as a collaboration tool. It's part of the Microsoft 365 platform (also known as Office 365), which means your team can work on documents at the same time. Before we moved to 365, the document was locked if one person had it open. Now, you'll be able to work on the same document at once, so much easier and more convenient.

What is OneDrive?
OneDrive is also integrated within the Microsoft 365 platform. Microsoft has designated this product as a cloud storage solution that you can use to store documents, notes, photos, music, videos, or other types of files. With OneDrive you can access your files from nearly any device, and you can share them with others. Consider this your "personal" drive. You can save anything you want here and if your department has a shared drive, your OneDrive will be linked to the SharePoint site. No one has access to the files in your OneDrive except for you until you share them (if you choose to).

Unlike other cloud file storage offerings, OneDrive operates as an offline synchronization engine. In short, this enables you to access your files even if you have a poor internet connection or a limited one.

Are SharePoint and OneDrive the Same?
The straightforward answer is no; these products are not the same. OneDrive is a vanilla online folder system used for storing files. SharePoint also has this function, but this platform has many other features.

SharePoint comes with collaboration features, a customer management system, and various dashboards. However, when comparing OneDrive vs. SharePoint, the confusion over which to use comes from the fact these two products have many similarities.

SharePoint vs. OneDrive: Similarities
SharePoint and OneDrive are both developed by Microsoft and can be accessed via the Office 365 platform. Despite this, they are not the same program, and each one has a different use case.

Here's a brief overview of their similarities:

- Storage Space – Each product allows you to store your files within Microsoft's cloud storage facilities. You can access your files remotely from any device, whether using laptops, smartphones, or tablets.
- Enterprise Security – Security is a hot topic within the online world. Microsoft offers enterprise-grade security, consisting of high-level encryption and secure SSL connections, with 2048-bit keys included.
- Worldwide Access – As long as you have an internet connection, you can access your files from anywhere in the world.

SharePoint vs. OneDrive: Differences

The primary difference between OneDrive and SharePoint can be found within the scope of each product. OneDrive was designed to act as a cloud storage system for personal and business users. It was never intended to go beyond this purpose.

On the other hand, SharePoint aims to make collaboration simpler, allowing you to provide a better standard of service to your customers, and manage various aspects of your brand. In other words, the difference between OneDrive and SharePoint is in which needs they were designed to address.

There are still a few departments we've yet to upgrade, but if you're ready to be upgraded, feel free to give any of us in I.T. a call. The upgrade typically takes between 15 and 30 minutes, but could take longer depending on the speed of your computer.

New MFA 'Prompt Bombing' Attacks

While multi-factor authentication (MFA) significantly reduces an organization's threat surface by making the stealing of credentials much harder, a new attack takes advantage of phone calls as the second factor.

Whenever cybercriminals can successfully leverage the victim themselves as part of an attack, they will. And that appears to be the case in a new attack by cybercriminal group Lapsus$. In this new attack, first detailed by Wired, Lapsus$ has taken advantage of various platforms' MFA implementation that uses either a phone call or pushing a button on the screen of their mobile phone.

The attack method is rather simple – call the victim employee a multitude of times at 1 AM when they're sleeping, and - according to Lapsus$ on their official Telegram channel – [the victim employee] "will more than likely accept it. Once the employee accepts the initial call, you can access the MFA enrollment portal and enroll another device."

According to reports, Lapsus$ has successfully used MFA prompt bombing against Microsoft to gain access to the internal Microsoft network via an employee's VPN.

Users of MFA need to be made aware of these types of techniques via security awareness training to group this kind of unexpected prompting in with phishing emails, social engineering scams on social media, etc. – anytime they interact with something that provides access that they were not expecting to see should be considered suspicious.