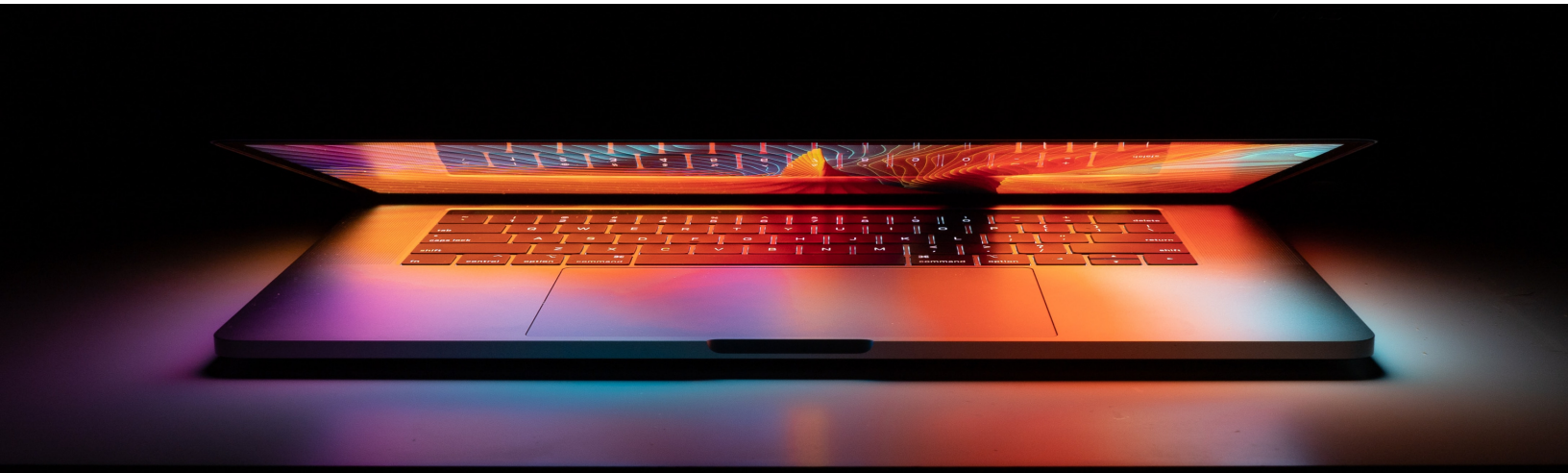
PLUMAS COUNTY TECH TIPS

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**

Webcams

Webcams, like most things, range from simple to complex. A simple Webcam setup consists of a digital camera attached to your computer, typically through the USB port. All you have to do is plug the camera into your computer via USB and you are ready to go! The camera part of the Webcam setup is just a digital camera -- there's really nothing special going on there. The "Webcam" nature of the camera comes with the software. Webcam software "grabs a frame" from the digital camera at a preset interval and transfers it to another location for viewing

Once it captures a frame, the software broadcasts the image over your Internet connection. There are several broadcast methods. Using the most common method, the software turns that image into a JPEG file and uploads it to a Web server using File Transfer Protocol (FTP).

If you don't have have a webcam, but would like one, please reach out to us.

How Hackers Get Your Passwords and How to Protect Yourself

https://blog.knowbe4.com/how-hackers-get-your-passwords-and-how-to-defend

Despite the world's best efforts to get everyone off passwords and onto something else (e.g., MFA, passwordless authentication, biometrics, zero trust, etc.) for decades, passwords have pervasively persisted. Today, nearly everyone has multiple forms of MFA for different applications and websites AND many, many passwords.

The average person has somewhere between three to seven unique passwords that they share among over 170 websites and services.

Password Theft

Theft of passwords is by far the most prolific type of password attack, usually by social engineering of some type, but it can also be due to malware and hacking tools. The most common theft method is a traditional phishing email where the sender is pretending to be some organization that the potential victim has a relationship with, which contains a message and link prompting the user to type in their real login name and password.
Today, most malware looks for and attempts to steal as many passwords as it can. If the victim gets tricked into running malicious content, the malware will look in many areas to find and steal the user's passwords, including:

- Device memory
- Browser password caches and storage areas
- On storage disks
- As typed in by the user
- Extracting them from running programs and processes

Another way hackers get user passwords is by compromising websites and services that a user authenticates to. The average user logs into over 170 different websites and services in a given year, and each of those websites and services is a potential take-over target for hackers. Oftentimes, no one knows the website/service has been compromised and the passwords stolen until many months to years later. Because most users share the same passwords among multiple unrelated websites and services, it allows one compromised password to more easily lead to further compromises of other websites and services that the user belongs to.

Password Guessing

Passwords can also be guessed. All the attacker needs is an accessible login portal the victim can log into with a login name and password, and the ability to guess multiple times over a long period of time. Then, the attacker manually guesses or uses an automated password guessing tool. The shorter and simpler the password, the easier it is to guess. If the involved login portal does not have "rate throttling" or "account lockout", an attacker can guess a dozen to thousands of times a minute.

Password Hash Theft and Cracking

Another popular password attack is password hash cracking. In most modern-day operating systems, any typed in password is transformed by a cryptographic hash algorithm into a representative hash of the password (i.e., password hash).

A user's password hash is stored in password authentication databases that the operating system uses to authenticate the user. If an attacker can retrieve a user's password hash, however they do this, they can guess at (i.e., crack) the password hash by comparing it to a bunch of possible passwords that have already been pre-computed to their hash. This is known as password hash cracking.

Unauthorized Password Resetting or Bypass
Another common password attack is for a hacker to utilize a method which resets the user's password or simply bypasses it altogether. Most popular large authentication systems allow users to self-reset their own passwords. These are needed because one of the most popular support calls is a user forgetting or needing to reset their password. Password calls to tech support are so common that if they were all handled by a human, it would require significantly more resources and money than the involved organization has to spend. So, many/most organizations create or enable a self-help portal that the user can use to reset their password. Unfortunately, hackers know about these two and will use various tricks to reset the user's password without the user's permission.

In summary, passwords are compromised by the many tens of millions each year, using password theft, guessing, hash cracking and unauthorized password resetting.

What is Microsoft Teams?

Microsoft Teams is a persistent chat-based collaboration platform complete with document sharing, online meetings, and many more extremely useful features for business communications.

Microsoft Teams features make it stand out from other collaboration software:

- **Teams and channels.** Teams are made up of channels, which are conversation boards between teammates.
- **A chat function.** The basic chat function is commonly found within most collaboration apps and can take place between teams, groups, and individuals.
- **Document storage in SharePoint**. As we transition all employees to the Microsoft Standard Business subscription starting in June, we will be moving all shared folders to SharePoint. More information on SharePoint will be shared in the next newsletter.
- **Online video calling and screen sharing.** Enjoy seamless and fast video calls to employees within your business or clients outside your business.
- **Online meetings.** This feature can help enhance your communications, company-wide meetings, and even training with an online meetings function that can host up to 10,000 users. Online meetings can include anyone outside or inside a business.
- **Audio conferencing.** With audio conferencing, anyone can join an online meeting via phone.

When it comes down to it, we are encouraging the use of Microsoft Teams because it is extremely user-friendly and can facilitate a work environment between remote users or within a large business.

Microsoft Teams is included in Office 365 for free, so any Office user can enjoy all the benefits of this collaboration solution. If you would like to be set up with Teams, please contact Melodie.