

# PLUMAS COUNTY TECH TIPS

WHAT YOU NEED TO KNOW ABOUT TECHNOLOGY TODAY



## INSIDE THIS ISSUE:

MULTI-FACTOR  
AUTHENTICATION - 2  
USING FRESHSERVICE  
TICKETING - 3  
SENDING AN ENCRYPTED  
EMAIL IN MICROSOFT 365 - 3  
BACKING UP YOUR  
COMPUTER - 3

## CONTACT US:

HANIF - (530) 283-**6263**  
MELODIE - (530) 283-**6147**  
JEREMIAH - (530) 283-**6335**  
GREG - (530) 283-**6336**

## Welcome Back!

Welcome back to our Monthly I.T. Newsletter! Do you have something you are dying to know about I.T. or is there something you've always been curious about? Feel free to email Melodie @ [melodiebennett@countyofplumas.com](mailto:melodiebennett@countyofplumas.com) and I'll either include it in the next newsletter or I'd be happy to answer your question(s) directly.

## War in Ukraine

If you've been following the news, you know of the turmoil in Ukraine and you've probably also heard of potential cyber attacks affecting the U.S. While the chances of Plumas County being directly targeted are very slim, it's always great to be on high alert and if you see or hear of anything suspicious related to I.T., please reach out to us.

# Multi-Factor Authentication

Multi-factor authentication (MFA) is a security system that requires two or more methods of authentication from different categories that verify a user's identity to log in, which is a major component of a secure network. Think of it like an ATM, where both a physical card and a personal PIN are needed to access information about any given bank account.

When it comes to information security, the MFA plays a crucial role. It protects information from possible hacks, keeps an eye on employee accounts, and scares hackers away. Besides this even though their login credentials are leaked by accident, it protects users.

Relying on just one form of authentication can leave companies vulnerable, especially as ransomware attacks become more frequent and sophisticated. No system is one hundred percent safe from attempted attacks but adding MFA can be a major line of defense. There are many advantages to MFA.

**Increased Security.** The primary benefit of MFA is that it provides additional security layers and decreases the chance of consumer identities becoming compromised. By requiring users to provide multiple credentials prior to accessing accounts, hackers are prevented from using stolen passwords, devices, or other individual pieces of information to enter your network.

**Reduced Risk from Compromised Passwords.** While passwords are the most common form of authentication, they are the least secure. People may reuse or share passwords, which can also be stolen or guessed, leading to exposure for account holders and system administrators. The rise in password thefts through phishing, keylogging, and pharming has raised many concerns for organizations across the globe. All these concerns can be laid to rest through the implementation of MFA. For example, a user would receive a prompt to confirm secondary authentication even if the password is stolen. This will help prevent any data loss. A good practice is to require unique, complex passwords. A better practice is multi-factor authentication.

**Customizable Security Solution.** Each authentication factor offers multiple options, providing enterprises with the ability to customize the user experience to meet their needs. With Microsoft 365, we have three options to set up MFA, which allows each employee to choose which option works best for them.

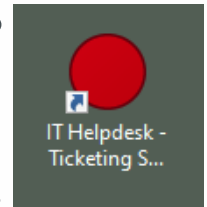
While MFA comes with its share of cons, it is still considered one of the highest levels of security that all organizations should aim to implement to keep their employees, networks, and customers secure.

Put simply, MFA reduces the risk of a security breach drastically, and sensitive data stays protected. If you have questions about MFA, please reach out to I.T.



## Using FreshService Ticketing

To use FreshService to put a ticket into I.T., you should see a red dot icon on your desktop that looks like the icon to the right:



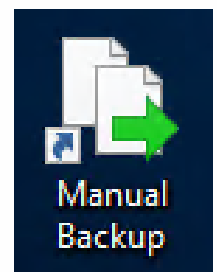
If you don't see the icon, you can also go to [plumascountycalifornia.freshservice.com](https://plumascountycalifornia.freshservice.com). Once you have logged on, you should see the "New Ticket" button at the top right corner of your screen. If you have trouble logging in, please contact Melodie at I.T. When the ticket page opens your name will automatically be inserted into the "Search a requester" line. Please provide a subject about the reason you are contacting I.T. and leave the status as "Being Processed". You can then choose the urgency, impact, and priority levels. Please make sure to include as much information as possible in the description and include an attachment if you can take a snipping or screenshot of the issue. Again, if you have trouble accessing your Fresh Service account, please email Melodie at I.T. @ [melodiebennett@countyofplumas.com](mailto:melodiebennett@countyofplumas.com).

## Sending an Encrypted Email in Microsoft 365

Sometimes, it is very important to send an encrypted email, especially while working for the County. Encrypting your email will keep all but the most dedicated hackers from intercepting and reading your private communications. Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. So how does it work now that we'd moved to Microsoft 365? All you need to do is include "Encrypt, Encrypted, or Encryption" in the subject line of your email. The message will be sent to the recipient, but the email will have a lock icon when it is received. The recipient will also receive a message at the top of the email when the email is open that says "Encrypt-Only - This message is encrypted. Recipients can't remove encryption." This means that the message is only able readable by the recipient. If you receive an encrypted email, you may be prompted to sign in to your Microsoft 365 account. Try it out for yourself!

## Backing Up Your Computer

By backing up your data, you prepare for the worst possible scenarios that can happen in life. Maybe your house gets broken into, and your computer is stolen. Maybe a natural disaster hits; like an earthquake. A normal power outage can fry the coding of your hard drive. There are plenty of threats in the modern world to your data. By backing up your data, you ensure the redundancy of your most important files. We've made it extremely easy to manually backup your work desktop. On your desktop, you should see a manual backup icon that looks like the image to the right:



To back up your documents, all you need to do is double-click on the icon. This will automatically create a backup to our County of Plumas domain. If you need to access anything from your backup, we can create a shortcut on your desktop, and if your computer unexpectedly dies, we will have a backup we can restore from. Please note that this manual backup only creates a copy of your Desktop and Documents. We highly recommend that you manually backup at least weekly, but we also would like to note that backing up your data is completely optional. If you are uncomfortable backing up your data to the County domain, there are additional options. Please reach out to I.T. if you'd like to explore additional options.