

PLUMAS COUNTY TECH TIPS

WHAT YOU NEED TO KNOW ABOUT TECHNOLOGY TODAY



INSIDE THIS ISSUE:

PHONES - **1**
SECURE PASSWORDS - **2**
PHYSICAL SECURITY - **2**
MICROSOFT EMAILS: DAILY
BRIEFING - **3**

CONTACT US:

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

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, it also alerts them who is calling. Check it out for yourself! Can't remember the co-workers extension? Use the button on your phone that looks like an open address book to search the directory. Once you press the button, press 2 for Corporate directory, or use the down arrow to highlight Corporate directory, enter the first or last name of the co-worker and click the "Search" button to find who you are looking for. *Please note that this only works for Cisco phones on our network. This includes all departments except for Child Support Services and Behavioral Health.*

Secure Passwords

A very simple but often overlooked element that can help your security is password security. Often commonly used passwords will be guessed by malicious actors in the hope of gaining access to your accounts. Using simple passwords or having recognizable password patterns for employees can make it simple for cyber-criminals to access a large range of accounts. Once this information is stolen it can be made public or sold for profit on the deep web. We understand the difficulty in remembering a long password, but as you can see in the graphic, the more characters a password contains, the harder it is for a malicious actor to crack.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

 > Learn about our methodology at hivesystems.io/password

Implementing randomized passwords can make it much more difficult for malicious actors to gain access to a range of accounts. Other steps, such as two-factor authentication, provide extra layers of security that protect the integrity of the account. Here are some suggested Dos and Don'ts for passwords:

- **DO** use a combination of uppercase and lowercase letters, symbols, and numbers.
- **DON'T** use commonly used passwords such as 123456, the word "password," "111111", or a word like, "monkey".
- **DON'T** use a solitary word in any language. Hackers have dictionary-based systems to crack these types of passwords. If you insist on using a word, misspell it as much as possible, or insert numbers for letters. i.e. pi\$t@ci0
- **DON'T** use a derivative of your name, the name of a family member, or the name of a pet. In addition to names, do not use phone numbers, addresses, birthdays, or Social Security numbers.
- **DON'T** use the same password across multiple websites. If remembering multiple passwords is an issue, you can use a password manager to securely store your passwords.
- **DO** use abbreviated phrases for passwords. You can choose a phrase such as "I want to go to England." You can convert this phrase to an abbreviation by using the first letters of each word and changing the word "to" to a number "2." This will result in the following basic password phrase: iw2g2e. Make it even more complex by adding punctuation, spaces, or symbols: %iw2g2e!@
- **DON'T** write your passwords down, share them with anyone, or let anyone see you log into devices or websites.
- **DO** change your passwords regularly.
- **DO** log out of websites and devices when you are finished using them.
- **DON'T** answer "yes" when prompted to save your password to a particular computer's browser. Instead, rely on a strong password committed to memory or stored in a dependable password management program.

Physical Security

If you're one of those people who leave their passwords on sticky notes on their desk, you may want to throw them away. Though many attacks are likely to happen through digital mediums, keeping sensitive physical documents secured is vital to the integrity of Plumas County's security system.

Simple awareness of the risks of leaving documents, unattended computers and passwords around the office space or home can reduce the security risk. By implementing a 'clean-desk' policy, the threat of unattended documents being stolen or copied can be significantly reduced.

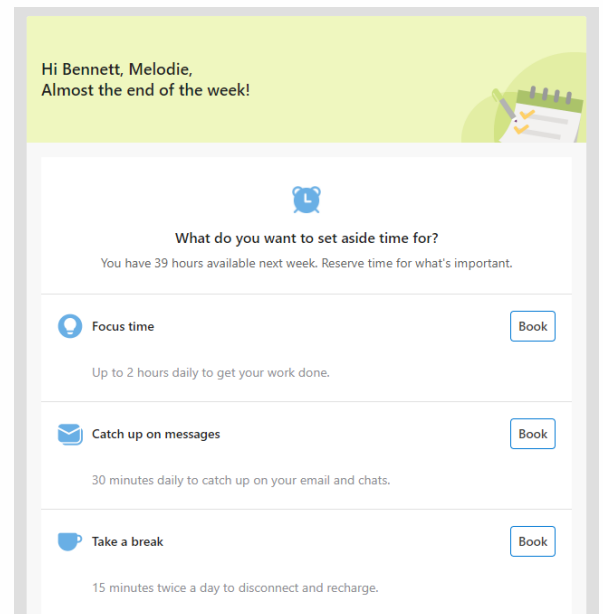
Microsoft Emails: Daily Briefing

Within Microsoft's O365 offerings, new services are continually launched throughout the year. The email that you may have received recently is called Briefing. The subject line was "Your daily briefing" and the sender is viva-noreply@microsoft.com.

What is Briefing, and what can it help me do?

Microsoft built this daily Briefing email to help you stay in control of your calendar and be intentional about your day. When you have action items or meetings, you will receive an email about any relevant items to help you better prepare for the day ahead, including:

- Outstanding commitments, requests, and follow-ups to and from other collaborators in email that might have fallen through the cracks.
- Documents related to today's meetings that you might want to review beforehand.
- Suggested focus time you can schedule to help get independent work done.



Data privacy and security

Briefing emails are personal and private and are only sent to you directly in your mailbox, which cannot be accessed by anybody else in your organization, including your IT admin or your manager. Briefing emails do not include any new personally identifiable information about anybody else in your organization. Your Briefing emails are based on information that you already have access to but can't quickly aggregate without help. For example, if you want to determine what commitments you made to others, you could manually review each email in your mailbox. The Briefing email helps you avoid this time-consuming process.

As Microsoft continues to release new services, or continue to develop existing services, we anticipate that you may see more of these in your email mailbox.

For additional information or more detail about Briefings, please visit:

<https://docs.microsoft.com/en-us/briefing/be-overview>

<https://docs.microsoft.com/en-us/briefing/be-faqs#for-briefing-users>