

Use a similar password, but with identifiers to tell you what site or system for which the password is used. First create a strong static password using what you learned above. Then make up a set of rules that help you identify where the password will be used. For example, use the first letter of the name or the application or site, the last letter of the name of the site, and the number of letters in the name. For example, using the “t@Af0mf7” password, the password for your Amazon account would be “aN6t@Af0mf7”. This also addresses the issue of adding length to a password based on a short phrase. Use rules that make sense for you and don’t share them with others.

Another way to keep multiple passwords secure is to use a password manager. Password managers, safes, or vaults are digital tools for storing password and account information. They may be on your local device or you may use a server-based or cloud-based manager. With a password manager, you need only remember one password – the one you’ll use for the manager itself. Some password managers take the matter of secure passwords one step further and generate strong passwords for you.



Three things to remember if you choose to use a password manager: 1) make sure the master password is something you will remember. Losing it means losing everything in your password manager; 2) make sure to backup your password manager; and 3) if you are planning to use a password manager at work, make sure it has been approved by your management.

A few last tips about passwords:

- ◆ **Change your passwords regularly. Yes, even your non-work related passwords.**
- ◆ **Never share your password with others. If someone has a legitimate need to have you logged on to a system (perhaps for tech support), always enter your credentials yourself rather than telling them your password.**
- ◆ **Never write down your passwords and leave them under your keyboard, on a sticky note on your computer, in an unlocked desk drawer, or other place where they could be found by someone.**
- ◆ **Don’t forget to use strong passwords on your mobile devices, too.**

By making your password strong and secure, you protect your information, your identity, and your workplace.



<http://infosec.mt.gov>



**Information
Systems
Security
Office**

Passwords

In this increasingly digital world we live in, passwords are the keys to nearly everything we do. We use them to access email, social media, bank accounts, online shopping, health care records, our child's school website – not



to mention all the systems we use at work each day. With just a password, a malicious person could empty your bank account, sabotage a system where you work, view your health care information, or even steal your identity. The tips

and tricks here can help you create strong passwords and manage them safely.

State of Montana policy requires that you have a password that is at least eight characters long and must be changed every 60 days. In addition, your password should contain uppercase, lowercase, numeric, and special characters. The password "Hacked1!" is an example of a password which meets all the suggested criteria but still is a weak password that could be cracked in less than one day. Clearly, meeting the minimum requirements isn't good enough.

The first problem with Hacked1! is that it uses a dictionary word as its main component. Dictionary words in any language are very easy to crack, as are names of people and places. Adding a number and/or special character at the end of a word is common and easily

cracked. Hacked1! is also only eight characters. By policy, that is the minimum required, but longer passwords are more secure passwords, so follow that rule whenever you can.

So how do we make stronger passwords while still making them memorable? One way is to use a phrase as the starting point for your password. For example, let's use the phrase "these are a few of my favorite things". Using the first letter of each word, it would be "taafomft". That's a weak password, but we can make it better by using uppercase in places and by substituting numbers or special characters: "t@Af0mf7". To make it truly strong, we should add to the length, perhaps by defining some of our favorite things like kittens, puppies, and babies, resulting in "t@Af0mf7:KP&b". The addition of those five characters on the end takes this password from something that could be cracked in a day to one that would take 423 centuries to crack!

Remember these tips for creating passwords:

- ◆ **Do make your password more than eight characters if possible. Longer is better.**
- ◆ **Do make them something you can easily remember, but others wouldn't guess.**
- ◆ **Do use a mix of uppercase, lowercase, numbers, and special characters.**
- ◆ **Don't use dictionary words, names, or places as your password.**
- ◆ **Don't just substitute numbers or special characters for lookalike letters in a word.**
- ◆ **Visit <https://passfault.appspot.com/> and test your password.**

Stop and think for a minute. How many systems or sites do you use that require a password? For every different site, account, or system you should have a different password. It's not uncommon for people to use the same password for most, if not all, of their accounts. The danger to this is when one site is compromised and your credentials stolen, the bad guys have access not just to your Facebook account, but your bank account or work systems as well. Here are some suggestions for dealing with all those passwords you need to remember.

