Keeping your passwords safe.

Most cyber criminals don't hack in. They log in!

The majority of cybersecurity crimes, identity thefts and financial crimes in ME start with a person losing a password, falling victim to a phishing scam, or simply using poor passwords in the first place. The criminal accesses our data using these passwords.

Q: What makes a good password?

A: A longer password is a better password. Modern computers can crack passwords very easily. However, for every character you add, the task gets harder. Consider 12 or more characters as a rule.

Q: How do I remember passwords?

A: Passwords should be long, but they don't have to be random. Consider using a sentence. For example, "victoria-loves-PB&J" is an excellent password that is easy to remember and hard to crack.

Q: What is two-factor authentication?

A: Two-factor authentication is when you use a PIN code sent to your phone, an app, or biometrics in conjunction with your password. Good identity management requires something you know (like a password) and something you have, (like a cell-phone). The two keep you safe if you lose one!



10 Rules of a Good Password:

****

1. Keep it personal, but not too personal.

Passwords should be personal to you, but not personal about you! If it's too personal, it can become easy to guess. Never use easy to guess personal dates, names of family members, or addresses in your passwords!

2. Change it every year.

It is likely that at some point you will lose a password. The only way to fix that is to change the password. We recommend changing all passwords once peryear. Set a calendar date and make that family password change day. If you do it together, you keep the whole family safe.

3. Never reuse email passwords.

Statistically, your email password is the most likely password you will lose. For this reason, never use your email password on another account or service. If you lose the email password, the criminal can get into your other accounts using the same password.

4. Always enable two-factor authentication.

Always enable two-factor authentication on email accounts, social media accounts, streaming accounts, cloud storage, financial apps, and any service that contains personally identifiable data. Two-factor authentication is still your best defense against losing a password.

5. Streaming and social accounts

Sharing passwords on social media or streaming accounts often leads to breaches and identity theft. If you are sharing an account with friends or family members, you're increasing your chances that someone will make a mistake and lose the password.

6. Never save it in your browser.

Never save a password in the browser. The "remember my password" function that many browsers use to help you log in to websites are very insecure and allow attackers to easily get all of the passwords someone has saved on the computer. Consider using a Password Manager Application instead if you cannot remember all of your passwords (we can't remember ours, so we use a Password Manager too!)

7. Try a fake one first.

Many emails contain attachments or links that ask you for your username and password. Fake ones that are trying to trick you don't know the difference between your real password and a fake one. To check if the document or linked website knows the difference, try using an intentionally incorrect password first. if it let's you in — you avoided the trap!

8. When in doubt, change it.

If you have any concern that a password may be compromised, changing it is the best course of action!

9. Longer is better than complex.

Passwords that you can't remember are not great passwords. Try using a sentence like the example on the left side of this poster instead of random characters. Longer is better than complex.

10. Don't recycle passwords.

If you can help it, never reuse passwords on any account that stores personal information.

Brought to you by the **State of Maine**