**Lesson 5: Passwords**

A look at practicing strong passwords, a simple technique to stay cybersecure. Perhaps the simplest way you can protect yourself against cyber threats would be to practice **password safety**. Think about all the places where passwords are needed and utilized-- your phone, online shopping platforms, social media, email, and bank accounts. Creating strong passwords is the easiest and most common way to secure your cyber information. Passwords offer the first line of defense against malicious cybercriminals who try to access your personal data. Your devices will be more protected from cyber attacks if your passwords are secure.

A close-up of a lock and password

Description automatically generated

**Strong Passwords**

**Hackers** conduct **password attacks** by guessing your password based on commonly used words, or more often, programming computers to run algorithms to crack passwords for them. That's why it is important to make your passwords **long *and* complex** to make it close to impossible for cybercriminals to solve them.

Here are a couple of additional tips to create a strong password:

* Use a mix of lowercase and uppercase letters
* Incorporate numbers and special characters
* Have at least 8 characters
* Avoid using personal information (name, age, birthday)
* Do not use consecutive keyboard combinations
* Use a [random password generator](https://www.lastpass.com/features/password-generator) for maximum strength

**Try It Yourself**

Attempt to create your own solid, secure password! Try adding words that are meaningful to you so it'll be easier to remember (but not using obvious personal information like your birthday, name, etc.). For example, if you like to eat pasta, your favorite season is winter, and the last place you visited was New York City, a password you could make is: **P@sta\_w1nter\*N3wY0rk**. When you've completed this exercise, verify the strength of your password on <https://www.security.org/how-secure-is-my-password/>.

**Additional Tips**

Furthermore, you should follow these rules regarding password safety habits:

* Don't give your passwords to anyone.
* Change your passwords regularly, preferably semiannually or after a cyberattack/data breach.
* Maintain different passwords for all accounts and websites so hackers won't have access to multiple accounts with one password.
* Consider using password managers to remember all your passwords (instead of writing them down on sticky notes). Don't worry, these managers have many layers of security to protect against attacks.
* Don't enter in passwords when you're on unsecured Wi-Fi connections.
* When an Internet browser asks to remember your passwords, select "never."
* In addition to passwords, add security questions and multi-factor authentication on devices and websites to keep your information secure.

To sum up, maintaining a strong password is a both a straightforward and powerful way to manage your cyber risk and practice good security norms.