LOUISIANA DEPARTMENT OF EDUCATION

Office of Teaching and Learning

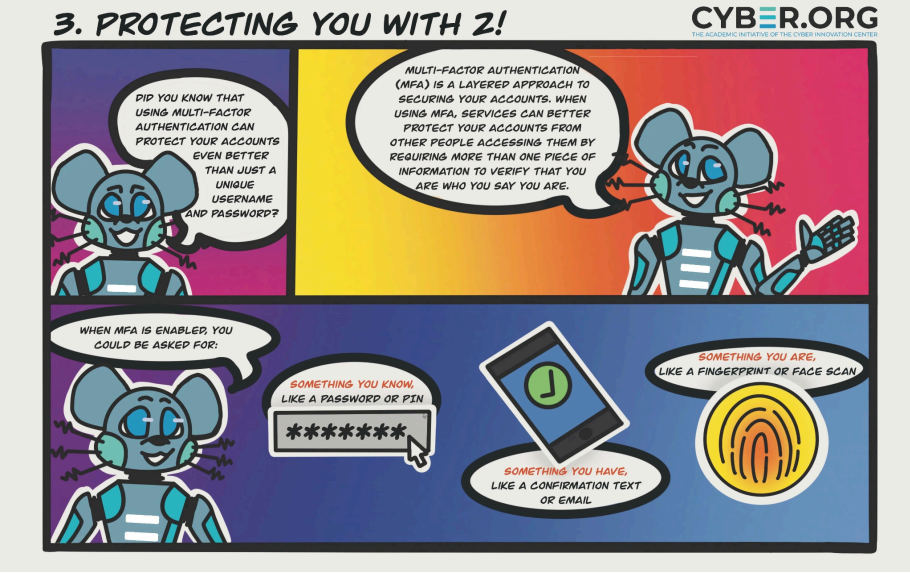
Student Guide to Cybersecurity

What is cybersecurity?

- Measures taken to protect computers from unauthorized access and digital data from unauthorized use.

What are some examples of cybersecurity measures?

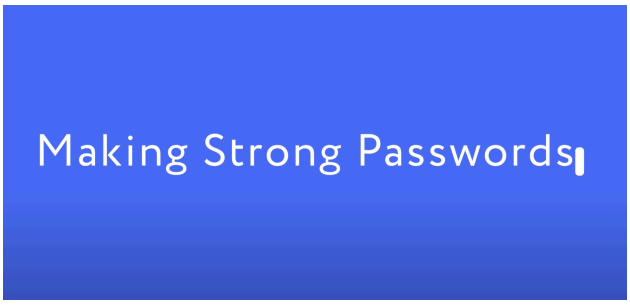
- Multi-Factor Authentication (MFA)
  - Multi-Factor Authentication is when a system, such as an app or website, requires multiple authenticators to verify your identity.
  - It increases security because if one authenticator is compromised, there are others to fall back on that other people will not have access to.
  - Examples of authenticators:
    - something you know: a password or PIN
    - something you have: a card (e.g., debit card) or mobile token (e.g., a single-use access code sent to your phone that expires after a certain length of time)
    - something you are: fingerprint, facial recognition, etc.
  - Check out Cyber.org's "The Adventures of Pascal and Python" MFA explanation:[1]



Pro Tip: Check the privacy settings on your online accounts to make sure 2-step verification or multifactor authentication is set up.

[1] This work from Cyber.org is used with permission. The original work is available at https://cyber.org/sites/default/files/2023-04/April%20Comic.jpg.

- Strong passwords
  - Use long passwords (at least 12 characters) that combine upper and lowercase letters, numbers, and symbols (e.g., OrangeCatsRQTies!).
  - Develop mnemonics (learning techniques to aid information retention) to help you remember your passwords.
    - Use this site to help you develop a mnemonic!
  - Use a different password for everything.
  - Avoid basing passwords off personal information.
  - Watch the video below to learn more!



Try using the chart below to help you create a strong password: (Do not use these examples as your password!)

1. Start with a **phrase**. Think of a quote or group of words that will be easy to remember.	**"i can do this"**
2. Write down just the **first letter of each word** in the phrase.	**i c d t**
3. **Capitalize** some of the letters.	**I c D t**
4. Add one or two **memorable numbers or symbols**.	**Ic@ndoth1s!**
5. **Memorize** it. Repeat your new password in your head so it sticks.	

[2]

- Privacy settings
  - Turn off location sharing on your social media apps.
  - Set your audience for social media posts to "friends only."
  - Many apps will ask for permission to access and/or share your data. You should restrict third-party app access to keep your data secure.
    - Ex. Third-party apps may request access to your social media account, phone camera, or contacts list to allow you to share photos between apps or connect you to more "people you may know." Check with an adult before allowing such access.
  - Bonus: Even if your privacy settings are set properly, do not fill out superfluous online quizzes and questionnaires about your personal information.

- Keep your software up-to-date
  - Updates often fix security flaws and add or improve security features.
  - Play Cybersecurity Lab to see some examples of updates to software that help keep your data safe!

- Use wi-fi you can trust
  - Personal Wi-Fi at home
  - Public libraries and schools
  - Make sure your connection is encrypted to protect your data by checking for these two things:
    - look for https before the website address
    - look for a lock symbol to the left of the address bar ex.

  - Check out Cyber.org's "The Adventures of Pascal and Python" MFA explanation

Use what you have learned here to work through these online safety lessons. Scroll down and choose your grade level to begin.