CYBERSECURITY BASICS

Cybersecurity is all about the safety of information—our identity, our personal data, and our financial assets—when we're online.

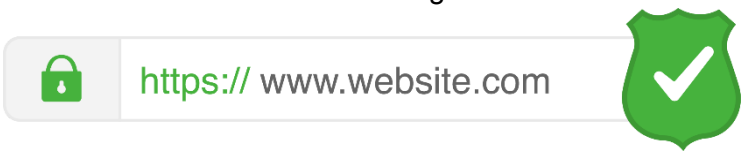
Cybersecurity means that 1) your personal data is accessible only to you or others you authorize, and that 2) your devices—laptops, desktop computers, mobile phones, tablets—work properly and are free from malware.

SECURE WEBSITES

If you're going to enter personal information on a website, make sure the website is secure so your information is safe.

There are two things to look for when you visit a website:

1. a padlock icon next to the address bar
2. a website address that begins with HTTPS



TIPS FOR STRONG PASSWORDS

- Don't share your password with others. Passwords should be kept private.
- Gmail requires a password that is a minimum of eight characters.
- It should not be easy to guess, like "password" or "123456."
- Don't include personal information, like your address or name.
- Don't use the same password on multiple accounts and websites.
- Make the password longer. The best defense is length.
- Use short phrases like "cowshelpmakecheese."

TIPS TO RECOGNIZE ONLINE FRAUD AND SCAMS

- Have you heard of the person or organization before?
- If you are familiar with the person or organization, can you check to be certain they are not being impersonated? i.e. ask them a question only they would know, check for proper email or phone number.
    - If you're unsure if an email or call from an organization is legitimate, contact the email or phone number listed on their official website.
- Can you tell who the email message is from?
- Does the email have mistakes?
- Are they asking for your information?
- Are they trying to rush you into a quick action?

- Is it too good to be true?

DOS AND DON'TS TO AVOID SCAMS

Don't

- **Give any personal information** to something that could be a scam. This includes name, email address, credit card number, or password.
- **Reply to or engage with the fraudster.** Doing this can notify the scammer that they've reached a real person, which can result in more scam emails.
- **Click any links or buttons.** Doing this can take you to untrustworthy websites.
- **Download any files or attachments.** They could contain viruses or malware that harm your computer or collect your personal information.

Do

- **Be skeptical.** If you think something may be a scam, it probably is**.**
- **Read emails carefully.** Remember to read emails and text messages carefully, checking to make sure you know the sender. Apply the other tips we presented to determine if something is a scam.
- **Look up information on your own**. Do look up contact information, information on a company, or, your account information on your accounts on your own. Go directly to the company website or to your own account information to check. Don't go to any website through the scam email.