Cybersecurity Basics Learner Handout

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

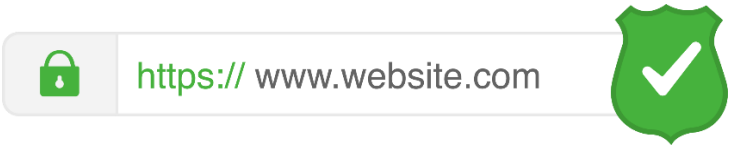
Cybersecurity means that 1) your personal data is accessible only to you or others you authorize, and that 2) your devices—laptops, desktop computers, mobile phones, tablets—work properly and are free from malware.

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

- Avoid common words 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.
- Don't share your password with others. Passwords should be kept private.
- Make the password longer. The best defense is length. Longer passwords don't need to be complex and hard to remember.
- Use short phrases like "cowshelpmakecheese."

Tips to Recognize Online Fraud and Scams

- Have you heard of the person or organization before?
- 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.

Learn More

Visit digitalliteracy.att.com for more courses and to help build skills and confidence using technology.

Today’s training is provided by NCOA, AT&T and the Public Library Association.