# 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.

# 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.”
* For more information about creating accounts and safe passwords, watch the AT&T Connected Learning course Accounts and Passwords at [https://digitalliteracy.att.com](https://digitalliteracy.att.com/).

# Protect Yourself from Online Fraud and Scams

Types of Common Scams

**Phishing**

Scammers “fish” for sensitive information like passwords, Social Security Numbers, credit card and bank account details, or other personal data. Phishing occurs when fraudsters or scammers use fake emails, text messages, phone calls, social media profiles, websites, online games, surveys, or quizzes, or free Wi-Fi to gain access to sensitive information. Once you enter your information on a fake site, they will have you "hooked." The scammers can use this information to gain access to your money or steal your identity.

**Social Engineering**

Social engineering occurs when a fraudster uses emails, text messages, phone calls, or social media profiles to gain your trust by convincing you they are someone they are not, to get personal information or money from you.​ Examples of social engineering include a person who

* Claims to be a friend or family member in trouble,
* Pretends to be a company with a great discount or offer, or
* Claims to be working on behalf of a government agency, organization, or collection agency.

Dos and Don’ts to Avoid Scams

**Don’t**

* **Don’t give in to the pressure to act now.** Take the time you need to verify the request.
* **Don’t give any personal information** to something that could be a scam. This includes name, email address, credit card number, or password.
* **Don’t share your personal PIN, password, or passcode.**
* **Don’t give them money,** including gift cards, prepaid debit cards, or transfer money.
* **Don’t reply or engage the fraudster.** Doing this can notify the scammer that they’ve reached a real person, which can result in more scam emails, phone calls, or text messages.
* **Don’t use the contact information or link from the person who contacts you**.​
* **Don’t click any links or buttons.** Doing this can take you to untrustworthy websites.
* **Don’t provide remote access to your device.** That person would have complete control over it, including the ability to access your personal data or install malware.
* **Don’t download any files or attachments.** They may contain viruses or malware that could harm your computer or collect your personal information.

**Do**

* **Do take time to investigate the request**. Check with a trusted person to verify it’s safe.
* **Do be skeptical.** If you think something may be a scam, it probably is**.**
* **Do put the suspicious email into your spam folder.**
* **Do look up contact information from another source.** Go directly to the company’s website or check a statement you received in the mail.
* **Do only access websites that begin with HTTPS.**
* **Do discuss with a trusted person.** If you are unsure about the request, talk to someone you trust, like a friend or family member. Don’t let them rush you into making a quick decision. ​
* **Do register your phone number with** [**DoNotCall.gov**](https://www.donotcall.gov/) to request that telemarketers not call you.
* **Do close pop-up windows** by holding down the ALT and F4 keys on a Windows keyboard or Command-W on a Mac. Don’t click on any buttons on the pop-up -- that includes the X!
* **Do use strong passwords** that include upper and lowercase letters, numbers, and special characters. ​Longer passwords are also stronger passwords.
* **Do regularly update and patch your devices** to ensure the latest security updates are installed.​​
* **Do use multi-factor authentication** that requires two methods to verify access to your account, including a username and password, and another method such as a code sent to your email.

**How to Identify if You’ve Been Scammed**

Here are some tips to help you determine if you have been scammed.

* **Unexpected transactions show up on your bank or credit card statements**​.
* **Items you ordered and paid for did not arrive**, and when you try to report the issue to the seller, you do not get a response. ​
* You receive an email that there have been an **unusual number of unsuccessful sign-in attempts for one of your accounts**, but you have not tried to log in.
* **You can’t log into your account**, and you cannot reset the password.
* **You can’t withdraw money from your account,** and when you log into your bank account, the balance is zero, or it has been closed.
* **The person you were communicating with disappears**. You reach out to them via email, text, or social media, but they no longer respond, or you can’t locate their online profiles anymore. ​
* You **notice signs of malware on your device**, such as pop-up ads that are hard to close, new or unfamiliar toolbar icons, or your computer or mobile device not responding as fast as it used to.

**How to Report Scams**

Here are a few actions you can take if you identify or fall victim to a scam.​

* If you come across a phishing scam impersonating a known organization, you can **reach out to** **the organization being impersonated.** For an IRS phishing scam, forward it to [phishing@irs.gov](mailto:phishing@irs.gov).
* **Mark fake emails as spam or junk.** This helps email providers identify and prevent scams.​
* **Contact bank and credit card companies** right away if you notice any unauthorized transactions.
* **Freeze your credit report** so someone else can’t apply for credit cards or loans in your name.
* **Change your passwords** if you think someone is trying to access your account, you gave your password, or you were notified that your account may have been compromised through a data breach, unsecured internet network, malware, or phishing attempt.
* **File a complaint** with one of the following federal or state agencies:
  + Federal Trade Commission at [reportfraud.ftc.gov](http://reportfraud.ftc.gov/)
  + Federal Bureau of Investigation's Internet Crime Complaint Center at [www.ic3.gov​](http://www.ic3.gov/)
  + Your state’s attorney general at [usa.gov/state-attorney-general​](https://usa.gov/state-attorney-general)
* **Report suspicious activity** to your phone and internet service provider. If you think your identity was stolen or your information was exposed in a data breach, **check the** [**IdentityTheft.gov**](https://www.identifytheft.gov/) **website** to explore your options, report the theft, and create a recovery plan. ​
* **Stay Alert: Protect Yourself from Scams**
  + Be cautious of unexpected phone calls, texts, or emails asking for your personal, account, or credit card information. AT&T will never request sensitive details through these channels.
  + Get free mobile security with the AT&T ActiveArmor® App, which is available to AT&T and non-AT&T customers. Download the free app to:

✔ Block and filter spam calls and texts

✔ Get alerts when companies have a data breach

✔ Device security to protect your phone and your personal data on it

* To report Suspicious Activity
  + For AT&T Internet Service Customers: Forward suspicious emails or other activity related to AT&T to [abuse@att.net](mailto:abuse@att.net).
  + For AT&T Wireless (Cell Phone) Customers: Block and report spam calls in the the AT&T ActiveArmor® App

**DISCLAIMER:** If AT&T is not your internet or wireless service provider, please contact your provider for guidance on reporting suspicious activity and available security resources.

Some mobile security features—such as Caller ID, Spam Text Protection, and Auto Fraud Risk Call Blocking—are only available to AT&T wireless customers. These rely on AT&T’s network-level protections and are not accessible to users on other carriers.

For more information about how to be safer online, watch the AT&T Connected Learning course, Online Fraud and Scams, at [https://digitalliteracy.att.com](https://digitalliteracy.att.com/).

**Learn More**

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