

Protecting Your Online Accounts

If you've ever created an online account, you've probably had to choose a password. Passwords are meant to protect sensitive and personal information. Occasionally, hackers or scammers may try to gain access to your account. By choosing secure passwords and by being aware of scammers tactics, you can increase your chances of keeping your information safe.

Vocabulary Terms

Password Manager: a program that's accessible by one password but keeps track of all your other passwords so you never forget them.

Urgent Message: a notification stating that one of your accounts has an issue that needs to be resolved ASAP.

PIN: a personal identification number (PIN) is a numerical passcode typically used to unlock an electronic device.

1. Determine if each scenario is probably a scam by writing a Y (yes) or N (no) next to each situation.

 Y A text from a random financial institution letting you know you're locked out of your account and need to click the link to regain access.

 Y A phone call notifying you that you won a free 7 night cruise!

 N A letter in the mail from your doctor's office reminding you about your past due bill.

 Y A poorly written email from a very distant relative claiming they need financial help.

2. True or False (circle one):

☒ T F It's important to be cautious about who you are interacting with online.

3. Draw a line to match the correct term to its definition:

Security Questions	Requires you to sign in with a password to receive a link or passcode that is sent to your phone or email to continue.
Two Factor Authentication	Verification beyond a password if you are logging in from an unrecognized device or location.
Suspicious Activity	Answering a personalized question to verify it's you.

4. What's your biggest takeaway?

Answers will vary.
