Networks and the Internet
Module 5 Lessons 5.10

Context of the Lesson

The Big Idea: Students will learn common mistakes in password creation, as well as how to make strong passwords and protect their information.

Prerequisite Knowledge and Skills:

- Knowledge of computing devices
- Using computing devices for everyday tasks
- Basic understanding of how use computing devices
- Basic understanding of what not to do using computing devices

Connections to SOLs:

- Computer Science 5.10

Objectives of the Lesson

Learning Targets (I can...):

- I can create strong passwords
- I can identify weak passwords
- I can keep my passwords safe
- I can name different ways to protect a computer
- I can apply confidentiality to my information

Formative Assessment

- Verbal testing
- Group and individual activities
- Instructional aids
- Written testing

Materials

- Visual Aid for instructor to write on (e.g., chalkboard, projector, dry erase board, easel)
- Handouts for students (optional)
- Computer (optional)

Lesson Structure and Activities

Warm Up *[5-10min]*, answers to be written out by instructor on visual aid

Ask: Have you ever heard of someone having their account or information stolen because someone 'hacked' their account?

- Responses will vary.

Ask: Have you ever made your own account password for a computing system or website? (School accounts with student-controlled passwords count.)

- Responses will vary.

Explain to students that they will be learning about passwords and cybersecurity.

Launch (Engage) *[10-20min]* :Teacher Directed Instruction:

Vocabulary:
Authentication – The process of making sure that someone is who they say they are. Someone whose identity is trusted is authenticated.
Confidentiality – Protecting information from being given to people who shouldn't know it.
Malware – Software designed to harm computers, breech security, extract information, or attack users such as viruses, rootkits, trojans, spyware, ransomeware, and botting programs.
Antivirus – Software designed to remove most common forms of malware (specializing in viruses).

Explain authentication as needed. It is not strictly a computer concept, and can apply to figuring out if someone is who they say they are in any situation. What if the bank let anyone have your money? What if your school didn't recognize you as a student and wouldn't let you in the building?

Explain confidentiality as needed. It is also not strictly a computer concept, and can be explained as simply as "don't talk to strangers" or "keeping secrets". Emphasize the idea of not sharing information with people you don't trust. If someone can't prove they are trustworthy, you shouldn't give them information, and neither should a computer. A good computer security policy never divulges any information to someone it cannot trust is someone who should have that information.

Explain how usernames and passwords are used on computing systems (as in a login page), on networking equipment (to access the network, like a Wi-Fi password), and on the internet (to use an online account, like Email). Link it to authentication first, and confidentiality second. The person needs to prove they are someone who is allowed to access that information or place by giving proof (usually a password) that they are allowed in (authentication), and if they cannot, no information or access should be shared (confidentiality).

Passwords should have at least eight characters, preferably more. A very common way of determining password is called brute force, which is when every combination of possible passwords is tried one by one. If a password cracker knows you used only 8 characters, they can narrow down your password pretty fast. If they knew it was 24 characters, it would take significantly more time.

It may not be necessary to go over why at a 4th or 5th grade level, but it should be enough to explain that if you only used ‘A’ and ‘B’, then a two character password could have four different combinations (2 by 2). Now add the rest of the alphabet. (26 by 2) Now add it in lowercase (26+26 by 2), now add the numerals, (26+26+10 by 2). Now make it an 8 character password vs a 24 character password (496 vs 1488). It’s more complicated then that but the high amount of combinations multiplied by the amount of characters in the password is the basis of it.

Passwords should include different types of characters: Letters, UPPERCASE (ABCDE) and lowercase (abcde), Numbers (12345), symbols (!@#$%), and if allowed, spaces (a b c d e). Something worth mentioning is that passwords that include sentence grammar like spaces are often called passphrases instead of passwords.

Passwords preferably should not include words from a dictionary. This is due to them being vulnerable to a “dictionary attack”, which tries words and common letter replacements like apple and @pple.

Passwords should not be recycled. Using the same password at different locations allows a cyberattacker to get into one of your accounts and thus get into all of them. If you need to use the same password on multiple accounts, absolutely do not use the same password on your email or account controlling accounts as you do for others. If your email is compromised, then accounts that use that email address are also in danger, as the attacker can change your password to whatever they please due to how websites handle password resetting: requiring a email. There have been recent cases (Spotify “breach”) where significant amounts of people were made victim due to reused passwords.

Show examples of good and bad passwords. **These were all taken from very popular examples of passwords and should not be used.**

GOOD:

Tr0ub@d0r$13 – This would defeat a dictionary check due to the high amount of substitutions, is much longer than eight characters, and uses lots of different symbols. It may be difficult to remember, which makes it a password you may end up writing down or forgetting, which leads to other problems. Passwords should be memorable and hard to guess by others and computers.

Correct+Horse+Battery+Staple – This is much more memorable.

Abs0lutely secure secret c0de – While it is true that this is very vulnerable to dictionary attacks, this password is significantly long at 29 characters, includes spaces, numbers, capital and lowercase letters, and conveys no private information.

BAD:

password

swordfish

apple123

Your birthday.

When selecting a password be sure that it is something people cannot figure out about you. If you make a password about a hobby, make it a ‘detail’ about that hobby. Putting ‘ilovelego’ is much worse than ‘stackinglegobrickskyscrapers’. Not only is it shorter, but it’s not only easy to guess, it’s probably a sentence you’ve directly said to someone if they asked you what you enjoy and you said ‘I love LEGO.’

Malware, or commonly computer viruses, are software that can lead to cyber criminals taking control of your computing systems, stealing information from you, or harming and damaging the software in your computing systems.

Malware includes computer viruses, trojans, worms, rootkits, spyware, and generally is a catch all term for **mal**icious soft**ware** that exists to harm computers. Over time “computer virus” has become a catch-all term for many forms of malware. When being specific, viruses refer to a type of program that replicates itself to disturb performance and memory. Trojans are applications that appear to be safe programs but are actually dangerous. Worms are network-borne malware. Rootkits make it easier for other software to infect you by destabilizing your computer’s security. Spyware is software that hides and spies on your information. Ransomware is software that disables the user’s access and often demands a ransom to unlock the computer with no guarantee of success beyond the word of the person harming your device. They have differences, but you don’t need to explore them at a 5th grade level.

Security breaches are what can occur when a cyber criminal gets past authentication and can see confidential information to take and to destroy, and to hack and to control. Some even steal information or control your computer, holding it hostage for a ransom.

Offline backup of data helps by allowing you to recover from any destroyed or ransomeware-infected data and verify the data has not been changed by someone else by comparing it.

If a computer were infected by ransomware and you have a backup of it, you could simply reinstall the data from the backup and continue working with that computer.

Explain antivirus software that monitors and helps deal with viruses and other malware. Many organizations provide free antivirus software for members, but when searching online for it on your own, be careful! Many software that claim to prevent malware are actually malware in disguise. Look to see what brands are trusted.

Explain firewalls that help control network traffic and network passwords that (if shared to only the authorized people) help prevent unauthorized individuals from accessing your networks at school and at home.

Firewalls gate what connections can go into and out of a device. They can be software or actual hardware devices that sit between the internet and you.

Explore *[10-25min]* :Joint/Guided Practice | Student Practice:

- Give classwork or assign homework on password strength.
- Demonstrate the properties of a strong password (length, dictionary-attackable, uppercase, lowercase, symbols.)
- Show students dangers of sharing information and easy passwords, as well as how to make a strong password.
- Let students practice using online learning resources.

Summarize *[5-10min]* :Debrief :

- Ask: Do you understand the need for stronger passwords?
- Ask: Do you understand the importance of authentication? Of confidentiality?

Extensions:	