



**Grades
4-6**



Junior Grades Lesson 4 Handout

Passwords & Passcodes

***Now that you have a Positive Digital Footprint,
how do you protect it?***

Creating strong passwords:

Longer is stronger!

Long passcodes are harder for others to guess. Most online accounts require a minimum passcode length of 10 characters; however, a recommended length is 12-15 characters.

Characters:

Characters in a passcode refer to symbols consisting of letters in upper (capitals) and lower (small) cases, figures from 0 to 9 and characters such as !, #, ^, *, \$, %, etc.

Use a passphrase!

A passphrase can be a few random words used together that are easy to remember. If you need help thinking of one, try using a combination of words that rhyme.

Passphrase:

Passphrases often contain more characters than passwords do, but fewer components (for example, four words instead of 12 random characters).

Never use any personal or private information in a passcode or passphrase, such as information that someone might already know or easily get from someone else.

Do not use repeating numbers like '777' or use a number count like '123' / '321', or a significant date like a birthdate or phone number. These are too easy to guess!

Create passcodes with a variety of characters! Include uppercase letters (ABC) and lowercase letters (abc), numbers (123) and symbols (!, @, #). Using all four types makes for a super strong passcode!

Protecting Passwords

Creating a strong password is very important, but that's only the first step to keep it safe. The second step is to keep it to yourself! Here are just some ways you can protect yourself and your passwords:

Always use a unique passcode for each profile because, if a password is stolen from one account, other accounts will still remain protected!	Do not reuse old passcodes – even if the old passcodes were for other accounts or profiles.
Best practice is to change passcodes from time to time because even strong passwords can eventually be guessed. You can set a date on your calendar to remind you to do this.	Don't share passwords with friends, not even best friends! Depending on your rules at home, passwords should be shared with parents/guardians only, for emergency purposes.
Be aware of physical surroundings! Watch out for others trying to look at your password as you type it into your computer or other devices.	Avoid logging into accounts on other people's devices, as passwords can be easily retrieved. If absolutely necessary, be sure to log out of profiles and devices when finished.

Your Turn!

Create some examples of passwords that follow the rules of '*creating strong passwords*' listed above.* Try making examples that would be easy for you to remember, but difficult for anyone to guess.

*Reminder! Once a password has been written down or shared with their peers, it should not be used as an actual password for one of your online accounts!