Lesson Title: Strong Passwords

Content Area: Privacy and Security

Overview:
This lesson shares the importance of creating strong passwords for use in digital environments. An important component to digital privacy and security is ensuring personal passwords are strong and unable to be easily compromised. Weak passwords can lead to hardware damage, identity theft, and financial loss.

Objectives:
After participating in this lesson, adult learners will be able to:

- Explain the importance of strong passwords
- Identify the characteristics of strong passwords
- Apply the characteristics of strong passwords to create/modify their personal passwords

Materials & Supplies:
The following materials and supplies are needed for this lesson:

- Digital devices: computers, tablets, smartphones (activity 1, activity 2)
- Access to the Internet (activity 1, activity 2)
- Keyboard Image (activity 3)
- Flip Chart & Markers (activity 3)
- Password Slips & Bowl (activity 3)

Preparation:
In preparation for this lesson, facilitators should:

- Review lesson plan
- Ensure Internet connectivity and check website links
- Print keyboard images
- Print and cut password slips

Terminology:
The following terms will be discussed during the lesson:

- **Password**: a combination of keyboard letters, numbers, and characteristics that must be entered to gain admission into many online services (e-mail, social media accounts, online shopping accounts, etc.)
- **Password Manager**: a service that allows users to store various passwords and other sensitive information in a virtual vault that is locked and stored on the company's servers, usually for a fee
- **Two-factor Authentication Services**: a means of accessing information by having two-factors (or steps) in the verification process. Typically, users are asked to prove their identity by providing simple credentials such as an email address and a password. A second factor of authentication such as a physical token, phone call, text verification, is then used to add an additional layer of security

Background Information:
People use locks on cars and security alarm systems on houses to protect their possessions. Passwords when using electronic devices are designed to protect personal information. Risks associated with using weak passwords include people impersonating you to access your bank account and other financial services, purchase items online, impersonating you in social media networking sites, and accessing private information on your computer. Passwords can be used to log onto a computer, sign into online accounts (e-mail, social networking, shopping, etc.), unlocking a cell phone or tablet, etc. Having a strong password can reduce, not eliminate, the risk of being hacked and having personal information stolen.

Activity 1: Password Strength Tester

NOTE: *Remind participants to not share their password (even as an example) during this lesson.*

Have participants enter a current password into a password strength tester: https://www.cscan.org/PasswordStrength/. This password strength tester is maintained by the Centre for Security, Communications, and Network Research with the School of Computing, Electronics, and Mathematics at the University of Plymouth in England. It is a trusted password strength testing site.

After entering their password, have participants assess their score:

- What was the strength?
- What was the categorical rating?
- What are strong features of the password?
- How could participants make their password stronger?

Activity 2: Forming Strong Passwords

Show participants a video(s) about password creation:

- https://www.youtube.com/watch?time_continue=163&v=pMPhBEoVuIQ
- https://www.youtube.com/watch?v=aEmF3Iylvr4

NOTE: *It is recommended to show the videos mentioned in this lesson on a screen projector with speakers. However, if that equipment is not available to you, have participants view the video on their own devices and then proceed with the activity.*

NOTE: *Both of these videos reference crooks. Remind participants that while there is a risk with any online activity, the goal is to reduce risk and create a strong password. You do not want to cause fear or concern for your participants, since they may already be untrusting of digital services.*

Facilitators should lead a discussion about different strategies for creating and maintaining strong passwords. Many digital platforms set their password requirements, so it is always recommended to check the minimum password requirements before creating a password.

- **Length**: most platforms require a password to be at least 8 characters, but many security experts recommend passwords to be at least 12 to 14 characters in length.
- **Unpredictability**: passwords should not include names, dates, street addresses, birth cities, common word (like the word password), etc. A mixture of numbers, symbols, capital letters,

and lowercase letters is recommended. Capital letters should be in the middle of the password, not reserved for the beginning or end.

- **Keyboard Patterns**: using a special pattern on a keyboard to create a password should be avoided. This was once considered a way to create random passwords, but it is no longer effective.
- **Phrases**: Security experts are now recommending that phrases be incorporated into a password, but the phrases should not be famous/well-known. They should be abbreviated and not be word-for-word. For example, "I ate mashed potatoes for dinner" could be "eye8M@SHEDpot@toe$4d!nner".

The same password should not be used for multiple accounts. Some security experts recommend using a password manager. Password managers are services that provide a place for users to store various passwords and other sensitive information in a virtual vault that is locked and stored on the company's servers, usually for a fee.

It is also recommended to not share passwords in-person, over the phone or in a text message, or by e-mail. Legitimate companies will not ask for a password.

Some sites offer or require a two-factor authentication services. Users have to complete two-factors (or steps) in the verification process, which typically involve a username/password for the first factor. The second factor of authentication such as a physical token, phone call, text verification, is then used to add an additional layer of security. Adding two-factor authentication services to accounts provides more security.

Show participants a video about two-factor authentication services:

- https://www.youtube.com/watch?v=Y4pzMHe_gp0

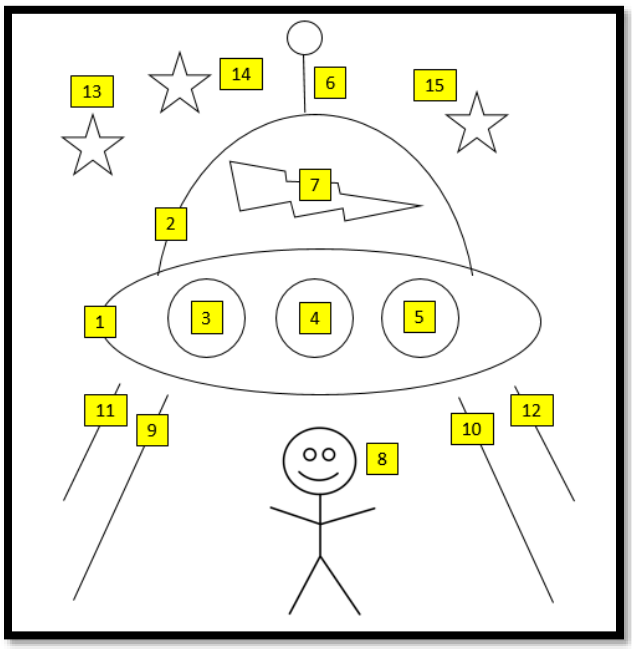
Not all account types, websites, etc. offer two-factor authentication services, but these should be enabled whenever possible. Facilitators may want to demonstrate two-factor authentication services, as long as it does not pose a security threat with their personal accounts and information.

Facilitators should emphasize that many social media platforms have personality quizzes, "about me" sections, etc. that generally ask personal information – birthdate, birth city, car make and model, name of a favorite teacher, school mascot, favorite color, pet's name, etc. These quizzes may seem harmless, but they offer personal information that may be used in a password. This information should never be shared on social media sites; it gives criminals additional information to guess passwords.

Activity 3: Password Challenge

Depending on the size of the group, facilitators may choose to subdivide participants into smaller groups. Each participant needs a copy of the keyboard image. Each group needs a flipchart and markers. This game is similar to the game "hangman" – however, hangman promotes a negative image of suicide, so this activity involves an alien abduction. The scene is comprised of 15 components.

Facilitators should show the participants the top 25 most-used passwords from SplashData. These are examples of weak and overused passwords. Lead a quick discussion about why these passwords are ineffective.



The top 25 most-used passwords from SplashData should be printed on individual strips of paper and placed in a bowl. One participant will be the "host" and choose a password from the bowl. The host will record blank spaces for each character of the password. Participants will take turns guessing characters – remember they can be upper or lower case letters, numbers, or special characters. Each time a character is correctly guessed, the character is recorded in the blank. Each time a character is incorrectly guessed, a part of the alien abduction scene is drawn. The game ends when the password is correctly guessed or when all components of the alien abduction scene are drawn. As a way to make the game easier, facilitators could consider the guess of any letter would be for both upper and lower case. For example, guessing the letter "a" include both upper case A and lower case a.

The game continues until each person in the group is the host. Other variations include the host creating a strong and effective password (using the characteristics described in activity 2) and participants have to guess the strong password.

NOTE: *Remind participants that these passwords are the top 25 most-used passwords and should not be used as strong passwords.*

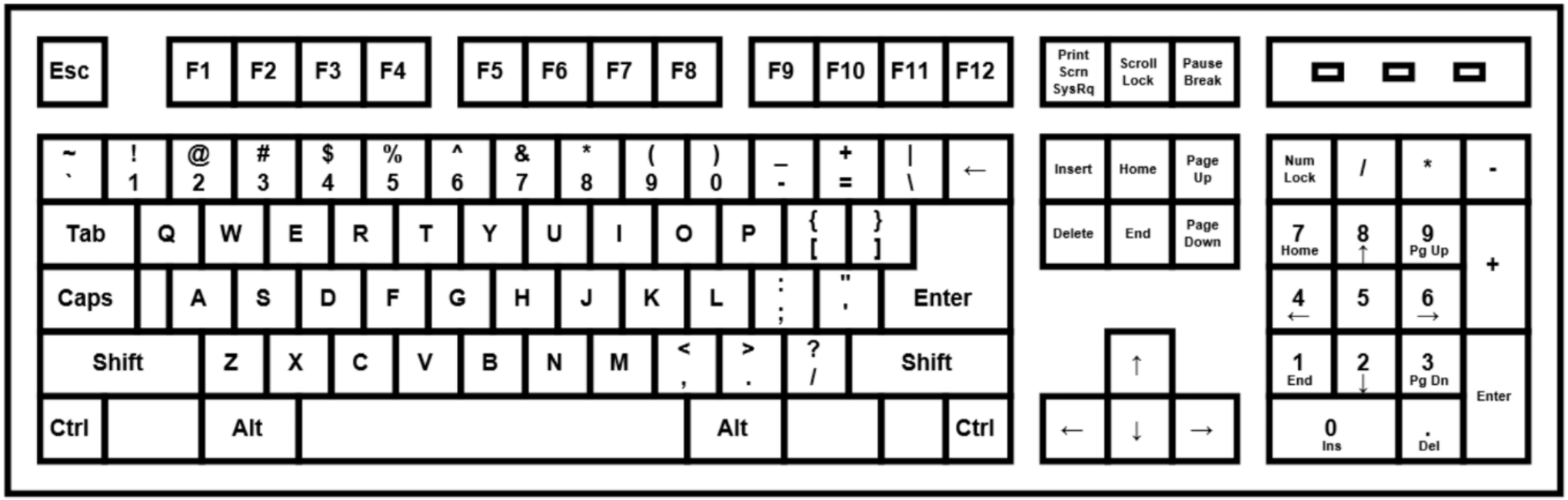
Reflection:
While the intent is for the activity to build privacy and security skills related to technology, it is important for the facilitator to lead a debrief discussion at the end of the lesson. Potential debrief questions could include:

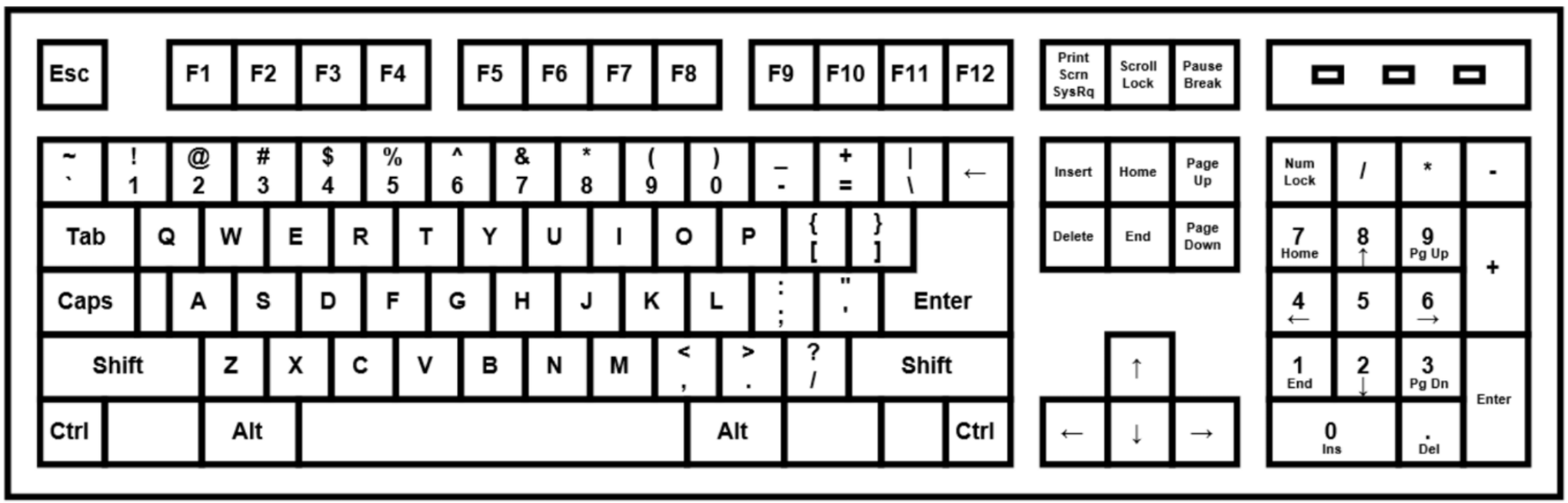
- Why is it important to have strong passwords?
- What are some tips for having strong passwords?
- What is one change you can make to your passwords as a result of this lesson?

NOTE: *Remind participants to not share their password (even as an example) during this lesson.*

Resources:

- https://www.wired.com/story/7-steps-to-password-perfection/
- https://www.techsafety.org/passwordincreasesecurity/
- https://www.cscan.org/PasswordStrength/ProtectingYourselfOnline.pdf
- https://www.commonsense.org/education/lesson/strong-passwords-3-5





Keyboard Image: to be used with Strong Passwords Lesson, Activity 2

SplashData Top 25 Passwords in 2018

123456	111111	princess	football	charlie
password	1234567	admin	123123	aa123456
123456789	sunshine	welcome	monkey	donald
12345678	qwerty	666666	654321	password1
12345	iloveyou	abc123	!@#$%^&*	qwerty123

NOTE: *These are examples of poor, weak, and overused passwords. For strength and security, these passwords should not be replicated.*

to be used with Strong Passwords Lesson, Activity 3