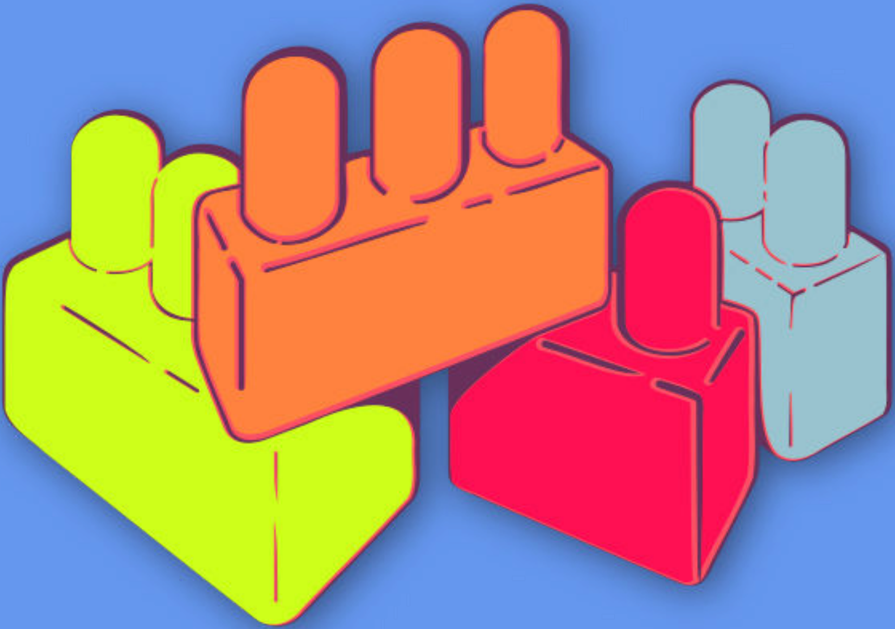
CYBERWOMEN



Digital security basics 1

Building stronger passwords

INSTITUTE FOR
WAR & PEACE REPORTING

Contents

Building stronger passwords

- **Objective(s):** In this session, you will review with participants the implications of a compromised password, how they are commonly compromised, and how to create stronger passwords and develop better password habits.
- **Length:** 45 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - How to secure your computer[2]
- **Needed materials:**
  - Projector
  - Slides
  - Paper
  - WiFi/internet access to download KeePass

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/

[2] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

This session is based on the module “Safer Password Practices” developed by Cheekay Cinco, Carol Waters and Megan DeBlois for LevelUp

Leading the Session

Part 1 - Introduction

1. Start this session asking participants:
    - When was the last time they changed any of their passwords?
    - Do they have different passwords for their different accounts?
    - Do they have their password written on a post-it note?
    - Do they have all their passwords stored on a document?
    - Do their phones have a password?

Part 2 - Why are Passwords Important?

2. Before you begin talking about the importance of passwords, ask participants to list all the information that is being kept safe through a password. What information do they have in their email accounts, social media accounts, cell phones? What would happen if someone else were able to access that information?
3. Now, share with the participants some reasons why passwords are important:

    - Passwords provide access to a number of important accounts such as email, banking accounts, social networking sites, etc.

    - These accounts often contain sensitive information, and also allow us to “be ourselves”, permitting organic interaction with others using various digital services - this might entail sending a social networking message, sending an email, making an online purchase, etc.

- They may also allow us to appear to be others - anyone with access to an account password can, in effect, act online as if they were the account owner.
- Passwords also provide access to a number of other things - Wi-Fi access points, unlocking mobile devices, logging-in to computers, decrypting of devices, files and more

Part 3 - What Can Happen If Your Password is Compromised?

4. In this part of the session we will share the papers with the participants and ask them to list all the platforms they can remember they have an account on. Now ask participants to list what might happen if someone had their password and could accessed their accounts or devices:

    - Important information or files could be stolen (copied) or deleted; if they are stolen, you may or may not realize it immediately. This could be anything from sensitive documents and files, to address book contacts and email messages.
    - Money and other funds could be stolen or spent, via access to credit cards or bank accounts.
    - Email or social media accounts could be used to send spam, or used to impersonate you or your friends, family, and colleagues.
    - Account access could be held in exchange for a form of "ransom" - this could include money, access to contacts, or access to other accounts.
    - Someone with a password could use this access to monitor communications and activities without your knowledge.
    - Access to your email could set off a "domino effect" where it is used to reset passwords to other accounts by requesting password reset links, eventually locking you out of many other accounts if the password remains unchanged.

Part 4 - How are Passwords Commonly Compromised?

5. Share some of the common practices that can end up with other people having access to your passwords:

    - When they are shared with others, or stored in an easily discoverable way - a commonly seen example is a computer login password written on a post-it note, and then stuck onto the same computer or nearby.
    - When someone witnesses a password being entered on your screen and writes it down or remembers it.
    - If using an email client without SSL (https) session-wide, only at the login page, this leaves passwords and other information vulnerable as they are visible by anyone with access to the connection after logging in.
    - A device is physically accessed, and passwords are able to obtained through "Save My Password" or "Remember Me" settings saved on websites via a browser - this is especially possible if full-disk encryption isn't used on a device.
    - Malware, such as a keylogger which can document every keystroke on a device and send it to a waiting third-party, can reveal not just passwords but potentially a great deal more personal or sensitive information.
    - Platforms can also be hacked or vulnerabilities in their systems cause that their users information is exposed.

Part 5 - How Can We Make our Passwords Stronger?

6. Explain that if we use the same passwords for everything, and that password is compromised, all our accounts can be compromised. Share some qualities of safer, stronger passwords with the group:

Length: to put it simply – the longer, the better! 12 characters is a highly recommended minimum for strong passwords, and 20 characters is even better.

Complexity: use a password that's alpha-numeric, using upper and lower case letters, with a generous mix of numbers and special characters.

Changed Regularly: regularly change your passwords, particularly for your most sensitive accounts, and definitely change them if you receive an authenticated (not phishing) email telling you that a particular service has had user accounts and passwords compromised.

Using passphrases (imagine several passwords strung together into a "sentence" or phrase) is another example of a strong password practice – here are a few examples:

> NoALaMineriaEnAmericaLatina ("Say no to mining in Latin America")
>
> AbortoSiAbortoNoEsoLoDecidoYo (Abortion yes, Abortion no, that's for me to decide)
>
> NosotrxsNoCruzamosFronterasEllasNosCruzanANosotrxs (We didn't cross borders, borders crossed us)

7. Ask participants to take a few minutes to begin creating some examples of strong passwords. Remind participants that they should think about how sensitive the information is in a given account while they consider the length or complexity of their passwords – they may want to use their strongest passwords for their most important accounts, while using less complex (but still strong!) passwords for less important accounts.

References

- https://level-up.cc/curriculum/protecting-data/creating-and-managing-strong-passwords/input/safer-password-practices/