DIGITAL SECURITY: PASSWORD

Workshop created by Yusuf Ganyana (twitter.com/flesymz) for DiGITAL YOU 2022 (#DigitalYou)

Time: Approx. 120 minutes

Essential question

What difference would it make if you switched from an easy-to-guess password to a secure one?

Established Goal

Participants in this session will learn the importance of protecting their devices and data as the use of computer systems and the Internet grows.

Objectives:

By the end of the lesson, participants will be able to:

- Have a basic understanding of Digital Security
- Learn why strong passwords are necessary.
- Amass tips to safe guard their digital device and data.

Training Session Materials:

- Projector and presentation slides
- Handouts of presentation in case there is no projector
- Copies of workshop schedule
- Copies of handouts and instructions for activities
- Stationery: posters, markers, pens, notepads, sticky notes
- Copy of attendance sheet
- Copies of photo consent form
- Copies of evaluation/survey form

LEARNING OVERVIEW

A password is your first line of defense against unauthorized access to your computer and personal information; each day, more than seven million data breaches occur. If you use a secure password, you are less likely to be attacked by hackers and malicious software.
Despite exponential technological advancement and reliance on computers and the Internet, human error continues to be the weakest link in this endeavor as hackers develop new tactics to breach systems and accounts.
This workshop will raise awareness about how to stay safe in the digital world.

This workshop was inspired by Tactical Tech's Digital Enquirer kit.

Workshop type: Offline

DIGITAL SECURITY: PASSWORD

Workshop created by Yusuf Ganyana (twitter.com/flesymz) for DiGITAL YOU 2022 (#DigitalYou)

FACILITATION NOTES

INTRODUCTION - 10 minutes

- The host explains housekeeping rules such as:
  - Location of bathrooms
  - Use of cellphones
  - Photo consent,
  - Signing the attendance sheet
  - Share the workshop schedule
- Host to welcome the facilitator(s)
- The facilitator(s) to introduced themselves, give a brief overview of the workshop i.e. title, objectives, and expected outcomes.
- Facilitator(s) should solicit participant expectations and adjust the lesson accordingly.
- Facilitator(s) to give a brief overview of Tactical Tech and the GOETHE INSTITUT.

ICEBREAKER - 5 minutes

PASSWORD CHARADE

[INVITE] Participants to write down an easy-to-guess password on a sticky note but not their actual passwords.

- Collect the sticky notes and arrange them on a table, face down.
- Using the signed attendance form, select a participant at random and have them "act out" a password without speaking.
- **[ENCOURAGE]** the other participants guess what it is.
- **[REMIND]** them to continue until five minutes are over.

– MAIN LESSON –

60-90 minutes

[ASK] ***What is it that we are trying to protect?***

***Note**: Tell a story to which they can relate.*

EXPLAIN

I am not sure how you would feel if you misplaced your phone. I would literally experience a mini-heart attack, demonstrating how indispensable digital devices have become. It should come as no surprise that our smartphones know us better than we know ourselves; for example, our phones are aware of our conversations (Call history, SMS from friends and family), our exploits (photos and location history), and so on. The privacy of the data that we generate, as well as the privacy of our families, and friends must be protected.

[ENCOURAGE] participants to identify some of the data on their smartphones.

[REMEMBER] Pause periodically to make sure the concept is understood

[ASK] ***What is Digital Security?***

Sample response

The safeguarding of information, devices, and accounts against unauthorized access and malicious attacks, allowing people to use social media, the internet, and online services (such as digital banking) while maintaining the confidentiality and integrity of their sensitive data.

Simply put, defending our digital identity or, in hypothesis, digital self-defense.

[PAUSE] Questions?

[ASK] Why is digital security important?

Sample responses

It enables people to use social media, the internet, and online services (such as digital banking) while protecting the confidentiality and integrity of their sensitive data.

- To protect the **confidentiality** of our online presence.
- Reduce the possibility of data breaches; **integrity**.
- Grant authorized users access to the information; **availability**.

[EMPHASIZE] To effectively implement digital security, you must continuously learn the new trends.

[PAUSE] Questions?

[ASK] How can we prioritize a good digital hygiene?

[EXPLAIN] Digital hygiene is a set of practices that you follow religiously in order to keep your data and devices secure.

Sample responses

- Be aware that you are a target for cybercriminals.
- Never take shortcuts, such as reusing the same password.
- Use a PIN or password to lock your device, and never leave it unprotected in public.
- Keep your software and hardware up to date.
- Install apps only from reputable sources.
- Double-check the links before clicking; do not open links or attachments in unsolicited emails or texts.
- Protect yourself with anti-virus and anti-malware software.
- Set up strong passwords and enable Two-Factor Authentication.
- Always back up important data frequently.
- Before using external devices, always scan them for virus.
- It's advisable to use a VPN if you connect to a public network.

[PAUSE] Questions?

[ASK] ***What is a password?***

Sample response

A combination of letters, numbers, and special characters used to verify identity and grant access while preventing unauthorized access.

It's also known as a digital signature because it uniquely identifies you.

[**ASK**] ***Why is a password important?***

Sample response

Safeguard your data from unauthorized access, preventing the loss of valuable information, financial breaches, identity theft, and other problems.

[PAUSE] Questions?

[ASK] ***What is a passphrase?***

Sample responses

It functions similarly to a password, but it uses a combination of random common words to create a sentence-like digital signature that only the owner understands.

[PAUSE] Questions?

[DISCUSS] ***Why is it recommended to use a passphrase as a password alternative?***

Sample responses

- Longer than a traditional password for added security.
- Easy to remember
- Difficult to crack.

[PAUSE] Questions?

Activity

CREATE A PASSPHRASE USING A DICES

[REMEMBER] Congratulate them of completing this task.

[ASK] ***What makes a password weak?***

[INVITE] Participants to go to this website, enter the passwords they wrote during the icebreaker, and share their thoughts.

Response sample

1. Using personal information
2. Uses common words and keyboard patterns
3. Using dictionary words; unless creating a passphrase
4. Reusing old passwords or using the same password in multiple locations
5. Using default passwords
6. Using a password with fewer than eight –characters
7. Storing your password in a location that is easily accessible, such as a sticky note or an unsecured file on your computer.

[EMPHASIZE] Even a strong password can be weak if not safely stored. It's the same as building a large metal safe to store all of your valuable items and then placing the key directly on top of the safe; it won't provide any security.

[PAUSE] Questions?

[ASK] ***Why do people use weak passwords?***

[INVITE] Participants to deliberate on this

Response sample

- It can be challenging to remember all of the passwords for the various services that require them.
- Because users are accustomed to shortcuts, passwords are frequently reused.
- When a strong password is not required by a system policy.

[PAUSE] Questions?

[ASK] What are the effects of using a weak password.

Response sample

- You become a target for hackers.
- You may become the victim of identity theft.
- Your compromised data could be used to commit a crime.
- Blackmail
- Loss of privacy

[PAUSE] Questions?

[ASK] ***What questions can we ask ourselves to create a stronger password?***

Response sample

- Is passphrase support available?
- Is it the recommended length?
- Does it include a mixture of characters?
- What does it do to prevent hackers' latest tricks?
- Is it unique to my other passwords?
- Is any personal information contained in it?
- Is it complex enough to be hacked, yet simple enough to be remembered?
- Can multi-factor authentication be used?

[**ENCOURAGE**] participants to refrain from making obvious character substitutions. For example, hackers now incorporate the letter "O" instead of the zero "0" in their code.

[PAUSE] Questions?

[ASK] ***What is multi-factor authentication (MFA)?***

Sample response
It is a type of electronic authentication in which a user is only granted access to a website or application after successfully presenting two or more pieces of evidence to an authentication mechanism.

[PAUSE] Questions?

[ASK] ***Why is MFA important?***

Sample response
MFA prevents unauthorized access to your personal data even if your password is compromised, because compromised credentials cannot provide the additional authentication factors required.

[PAUSE] Questions?

[**ASK**] How does MFA work?

Sample response
It makes use of two or three authentication factors:

- Something familiar to you, such as your **password**.
- Something you own e.g. a one-time code sent to your **smartphone**.
- Something unique to you, such as your **fingerprints**.

[ASK] How can you secure your password?

Sample response

- Always be on the lookout for phishing attempts and do not share your password with anyone.
- Make use of anti-malware software.
- Change your password to a passphrase.
- Be sure to change any automatically generated or default password.
- Avoid writing passwords down.

- Never use your password on a public wireless network that is not secure. If you suspect your password has been compromised, change it immediately.
- Avoid allowing your computer to remember your password.
- Enable two-factor authentication.

[ASK] ***What are the best practices for keeping my password safe when using a public computer?***

[POINT OUT] While public computers are convenient, they are more prone to being infected with malicious software.

- Use a reputable online spyware detection program.
- Disable autocomplete or the password-saving feature; do not save your login information.
- Always log out before closing the browser window.
- Clear your history and temporary Internet files by using Incognito mode.
- Be on the lookout for people who are staring at your screen.
- Avoid keying sensitive information into a public computer, such as a financial transaction that could reveal a password.
- Do not make use of your external drive. It could pick malicious software.

Q&A

[ASK] ***What questions do you have for me?***

[INVITE] and encourage the participants to ask questions or seek clarification to a point that wasn't clear or to some extent, unmet expectations.

— CONCLUSION —

10 minutes

By practicing good digital hygiene, we can limit the most common mistakes we make that lead to the exposure of our passwords to malicious people. This will protect our privacy. It is not just about keeping our devices running smoothly; it is also about keeping us safe from an ever-growing list of online threats.

Wrap up

[DISTRIBUTE] the evaluation form and allow them time to complete it.

[REMEMBER] Gather the forms before they depart.

[THANK] them for their participation, and **[ENCOURAGE]** them to share what they have learned with family and friends.

- END