Activity – Cyber Hygiene and Strong Password

Activity 1: How secure is my password?

Aim - to learn which password combinations are the hardest to guess or crack.

1. Visit the site How Secure is My Password?
2. Enter a word of your choice to see the time to crack the password
3. Try increasingly complex passwords to see how the time-to-crack changes

For example, try the following passwords:

- chocolate
- chocolatemilkshake
- Ch0c0l@t3
- Ch0c0l@t3M1lksh@k3!

https://tinyurl.com/3y95h5ka

Activity 2: Design the strongest passphrase

Let’s design a secure password

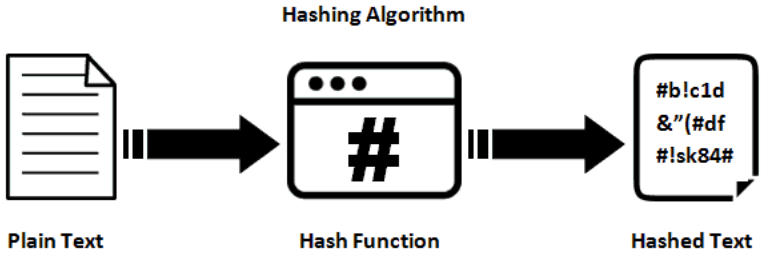
1. Write an easy-to-remember statement: a lyric from a song or a scene from a movie, a narrative about a place you've visited, or any other phrase you recall.
   - `The cat is Milo and the dog is Otis`
2. Take the first letter from each word (with capitalisation)
   - `TciMatdiO`
3. Change letters to numbers and symbols where possible
   - `Tc1M&td10`
4. Add a symbol for extra length and complexity
   - `Tc1M&td10!`
5. Check your password at How Secure is My Password?

Password Cracking

- Password cracking means **recovering passwords from a computer or from data that a computer transmits**.
  - For instance, a brute-force attack where all possible combinations are checked is also password cracking.

- Most passwords are stored using a key derivation function (KDF).
  - This takes a password and runs it through a one-way encryption cipher, creating what's known as a "hash."
  - The server stores the hash-version of the password

What is Hashing?



Hashing algorithms are one-way programs, so the text can't be unscrambled and decoded by anyone else

Hashing algorithms are used extensively in cryptography for encrypting keys or messages

- Examples include MD2, MD4, MD5, and SHA-1
- Message Digest 5 (MD5) uses a 128-bit hash, and Secure Hash Algorithm (SHA) uses a 60-bit hash.
- The more bits in a hash, the greater the security of the encryption process

Activity 3

Hash Hunt: Decrypt & Decode

Let’s see how easy it is to crack common password hashes

1. Navigate to Crack the Hash
   - You will see a list of password hash cracking challenges
   - **Note:** You need to create an account to submit answers
2. Decrypt the answers using Hashes.com
   - Hashes.com is a database of known password hashes

- Communicate effectively within your group to share findings and collaborate on decrypting the answers

https://tryhackme.com/r/room/crackthehash

https://hashes.com/en/decrypt/hash

Activity 4

Password Quiz

https://forms.gle/5b5iaasoifUAFvTy7

What is Cyber Hygiene?

Cyber Hygiene – A Baseline Set of Practices

Cybersecurity hygiene is a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today.

1. Identify and prioritize key organizational services, products, and their supporting assets.
2. Identify, prioritize, and respond to risks to the organization's key services and products.
3. Establish an incident response plan.
4. Conduct cybersecurity education and awareness activities.
5. Establish network security and monitoring.
6. Control access based on least privilege and maintain the user access accounts.
7. Manage technology changes and use standardized secure configurations.
8. Implement controls to protect and recover data.
9. Prevent and monitor malware exposures.
10. Manage cyber risks associated with suppliers and external dependencies.
11. Perform cyber threat and vulnerability monitoring and remediation.

Sources:
- *10 Steps to Cybersecurity*, UK Government Communications Headquarters (GCHQ)
- *20 Critical Security Controls*, Center for Internet Security (CIS) aka SANS 20
- *Cybersecurity Framework*, National Institute of Standards and Technology (NIST)
- *Resilience Management Model*, Carnegie Mellon University, Software Engineering Institute CERT Division
- *Review of Cyber Hygiene Practices*, European Union Agency for Network & Information Security (ENISA)
- *Strategies to Mitigate Cyber Security Incidents*, Australian Signals Directorate (ASD)

Strong Password

- Millions of passwords were compiled into a dataset to discover the top 200 most often used passwords worldwide in 2021 by a password management service called **NordPass**.

  - Secure passwords are difficult for others to guess or for computers intended for this purpose to crack.

  - Password's cracking entails a computer doing a brute force attack on a large number of password combinations until it discovers the one that is your password. Passwords that are simple and widely used are easily cracked.

Strong Password - Findings

According to NordPass 2021 report. The most common passwords globally are:

- 123456
- 123456789
- 12345
- qwerty
- password
- 12345678
- 111111
- 123123
- 1234567890
- 1234567

https://tinyurl.com/28nmbjw9

Strong Password - Findings

- Password choices are often attached to cultural preferences. For example,
  - In the UK, "liverpool" was the third most popular password, with 224,160 hits
  - In Chile, the name of Chilean football club "colocolo" was used by 15,748 people - making it the fifth most common choice
  - "christ" was the 19th most common password used in Nigeria, used 7,169 times
  - "bismillah", an Arabic phrase meaning in the name of Allah, was used by 1,599 people in Saudi Arabia – the 30th most common choice.