AUTHENTICATION

Password Safety

Passwords – Good or Bad?

Ex 1. Passw0rd!

Ex. 4
SquidGames2021

Ex. 5
Rone*HK%5

Why are Passwords so Important?

Warm Up: Why are passwords so important?

1. Silently think about the question above.

2. Turn to your neighbor and discuss what your ideas.

Discuss as a Class

Learning Objectives

1 Learn about three different password attacks.

2 Learn how to create strong passwords that can defeat these attacks.

3 Practice creating strong passwords that are memorable.

What is a password?

A secret word or phrase that is used to restrict access to something, usually an online account.

Passwords are Compromised by:

- Brute Force Attacks

- Dictionary Attacks

- Password Reuse Attacks

Let's break it down:
Brute Force Attack

What does brute mean?

An absence of reasoning or intelligence.

What is Force?

To make a way through or into
by physical strength

Putting it back together: Brute Force Attack

An attack that relies on the strength of modern computing to try all possible combinations to find the correct password.

Defeating brute force attacks!

Strong Password Characteristics:

- Letters (Upper and Lower)
- Numbers (0 through 9)
- Symbols (!, $, # , %, ?)
- At least 8 characters long

Let's break it down:
Dictionary Attack

What is a Dictionary?

A book that list of words and their intended meaning.

Putting it back together: Dictionary Attack

An attack that uses dictionary words and a list of commonly used passwords to guess to correct password.

Defeating Dictionary Attacks!

Avoid:

- Commonly used passwords
- Full words or sentences

Be safe by:

- Breaking up words with numbers or symbols
- Remove vowels
- Replacing letters with symbols or numbers

Let's break it down: Password Reuse Attack

Reuse

To use something again or more than once.

Putting it back together: Password Reuse

An attack that relies on a reused passwords to gain access to your account.

Defeating password reuse attacks!

Never reuse your passwords.

Avoid creating passwords that are similar to your other account's passwords.

Password complexity

A Bad password:

- Contains personal information (pet names or birthdays)
- Has repeating letters, numbers or symbols
- Is similar or the same as a password from another account
- Has unbroken full words or sentences

A Good password:

- Has a good variety of letters, numbers and symbols
- Breaks up words with letters or symbols
- Is always 8 characters or longer
- Is Unique

Password etiquette

Never share your password with anyone!

Memorize your password!

Create a story for your password

Relate passwords to the website or service

Transform a phrase or quote

Passwords – Good or Bad?

Ex 1.
Passw0rd!

Ex. 2
!@9YAt#f3h

Ex. 3 woRA70

Ex. 4
SquidGames2021

Ex. 5
Rone*HK%5

Group Activity – Create a Password

& Worksheet

Wrapping Up

We learned about three different password attacks.

We learned how to create strong passwords that can defeat these attacks.

We practiced creating strong passwords that are memorable.

Think about what you learned