**Lecture**

Passwords are an important part of staying safe online. They protect our data when using accounts on different websites. This information can vary from the videos we watch, our emails, and our social media accounts. Having a bad password can make it possible for someone who isn’t you to take over your account and gain access to that information. They can even take control and create posts that are not from you.

**(ask the class) How would someone break into someone else’s account?**

There are a few ways. First is simple guesswork. A person can research you online and find out information about you. If you use social media that information is easier to find. That is a reason you shouldn’t use your address or pets name in your password.

The next is a dictionary attack. This type of attack uses a computer to try many different passwords in a row. They will sometimes use enormous lists of words such as the dictionary. This attack can also try passwords that could have been obtained from websites that have been hacked before. The internet is full of thousands of passwords that have been leaked from breaches. This hacker can try each one of those while performing this attack.

This is also why you should change your passwords every couple of months. This makes sure that passwords taken from a breach can't be found and used.

The next attack is what is called a brute force attack. This type of attack uses a computer to try to crack passwords by guessing every possible password it could be. This list usually is created after the hack goes through public information on you. This could include pets names, graduation dates, birthdays, family members, etc. The hacker can then use this information to create a list of possible passwords to try to log in. Making your passwords separate from what you post online can really help to keep you secure. Increasing the length of your password makes the hacker have to guess that many more passwords to find yours as now they need to make their list include passwords that are many different lengths.

Using common passwords is a very bad idea as those will be the first one the hacker tries.

**(ask the class to guess the most common passwords)**

**(Correct Answers:**

**Top 12 most common passwords**

|  |  |  |
| --- | --- | --- |
| 1. **123456** | 1. **123456789** | 1. **qwerty** |
| 1. **password** | 1. **1234567** | 1. **12345678** |
| 1. **12345** | 1. **iloveyou** | 1. **111111** |
| 1. **123123** | 1. **abc123** | 1. **qwerty123** |

This is why you need to make your password unique.

An easy way to come up with passwords is to take a favorite number, a favorite food, a favorite character from a book or movie, and a symbol, and combine them to make a password.

Your password should have at least **2 uppercase letters, 2 numbers, 1 symbol**, and it needs to be over **8 characters.**

Passwords written by people tend to be easier to break as they tend to follow a pattern as they need to be easily remembered.

I recommend using a password manager. These programs will be able to store passwords for the user. They can also generate passwords that are very difficult for a computer or a hacker to break. The passwords look like this. **b@:H)Rk$T+$66]6H**

They are hard to remember but they are very secure and the password manager can remember it for you and you can retrieve it whenever you need it.

Consider looking here for a password manager <https://en.wikipedia.org/wiki/List_of_password_managers>