GLOBAL INITIATIVES
& SOLUTIONS

CYBER SECURITY:
ONLINE ACCOUNTS & PASSWORDS

Written and Edited by Myles Bolton
Designed by Fraser Anderson

WHAT THIS WILL TEACH YOU?

LEARNING OBJECTIVES:

1. What password vaults are.
2. How to create a strong password.
3. What passphrases are.
4. Social Engineering.

RE-USING PASSWORDS

THE THREAT OF CYBER CRIME

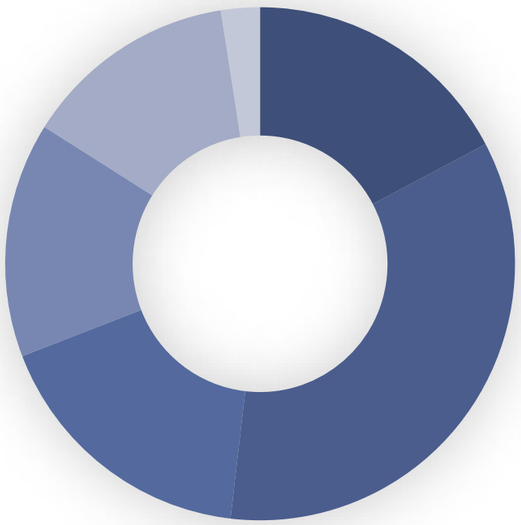
Imagine a scenario where you became a victim of password theft; you also decided beforehand that you wanted to use the same password that was stolen across multiple accounts. The attacker now has the opportunity to carry out further breaches with that same password.

It is important that all accounts under your ownership utilise their own unique password to avoid the aforementioned scenario from happening.

PASSWORD SURVEY

Hackers will take advantage of common errors made by users. Businesses tend to fall victim to wide scale attacks due to employees not regularly changing their passwords.

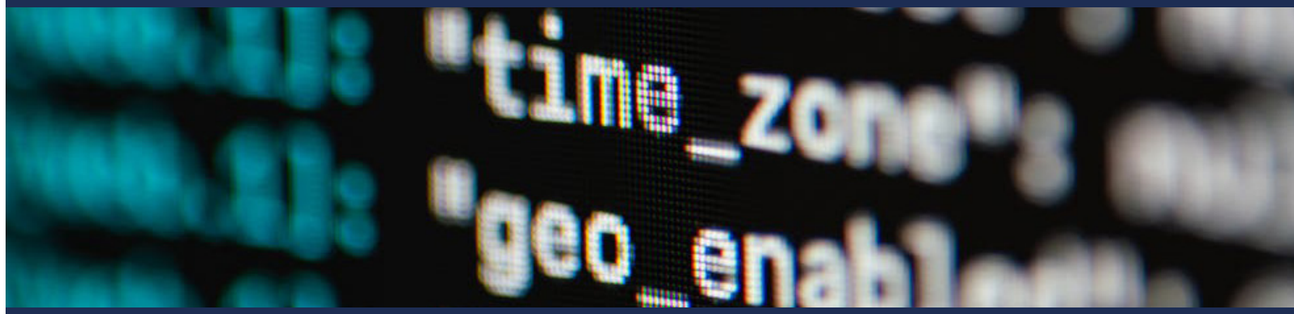
How Often do you use the same password for your online accounts?



- I never use the same password.
- I use the same password 5-25% of the time.
- I use the same password 26-50% of the time.
- I use the same password 51-75% of the time.
- I use the same password 76-99% of the time.
- I use the same password all of the time.

PASSWORD VAULTS

Password vaults exist in aims to mitigate the issues of password memorability, promoting more unique password usage across user accounts. These will be covered in a later section.



PASSWORD STRENGTH:

COMPLEXITY VS LENGTH

Apart from keeping your passwords unique, it's also important to ensure that they are of adequate strength.

Most businesses recommend a password length of around 11 characters long, although security firms suggest a minimum length of 16 characters long.

On top of this, a strong password will consist of an arbitrary mix of character types and symbols. An example of a strong password can be referred to below.

foVV18&^zzop!!wu

One issue presented with strong passwords is their ease of memorability. Users will often argue that they find themselves resetting their passwords a lot due to forgetting the password.

It's a misconception that passwords need to be both complex and long, a strong password can actually be achieved through its length.

Password crackers are as smart as the developer who programmed them. Most common attacks will utilise a brute force approach which will check all possible character combinations.

PASSPHRASESAREA WONDERFULTHING

THE USEFULNESS OF PASSPHRASES

It was found that simply extending the length of a password can greatly mitigate the chances of a password breach by a factor of 10. How do we aid in memorability if we do not have the resources to invest in a password vault? The answer: **Passphrases.**

Passphrases are simply a combination of common words linked together to form one long password. The title is an example of a passphrase!

There is no limit to what you can do with passphrases, any combination of words can form a phrase and will always lead to a greater increase in security and memorability.

PASSPHRASESAREAWONDERFULTHING PASSPHRASESAREAWONDERFULTHING
PASSPHRASESAREAWONDERFULTHING PASSPHRASESAREAWONDERFULTHING

SOCIAL ENGINEERING

COVERED TOPICS

- Social engineering.
- Open-Source Intelligence (OSINT).
- Social engineering techniques.
- Social engineering attack vectors.
- Other useful concepts.

SOCIAL ENGINEERING

Quite simply defined as "any act that influences a person to take an action that may or may not be in their best interests."

In the context of cyber security, **social engineering** is the psychological manipulation of people into performing actions or divulging confidential information.

This is done for the purpose of information gathering, committing fraud or gaining access to a system.

This course will give an overall awareness of the ways that you can be exploited so you will be able to think like an attacker. With this knowledge at the back of your mind, you will now be harder to manipulate.

> ***any act that influences a person to take an action that may or may not be in their best interests.***

OPEN-SOURCE INTELLIGENCE (OSINT)

Before we get into social engineering, It is important to realise there is likely a lot of information about you already accessible to the public.

Much of this is hard to keep track of or is difficult for you to access or change.

Open-source intelligence (OSINT) is the collection and analysis of information that is gathered from public/open sources for some purpose.

CYBER SECURITY: ONLINE ACCOUNTS & SECURITY

SOCIAL ENGINEERING

TECHNIQUES

There are **six** types of human biases that can be exploited:

1. Authority (your boss is telling you to do it).
2. Intimidation (something bad will happen if you don't).
3. Consensus (everyone else is doing it).
4. Scarcity (there is little of it making it more valuable).
5. Urgency (you need to act quickly without thinking it over).
6. Familiarity (you like it/them).

Any number of these techniques can be used for a single attack.

These techniques work better when the victim is vulnerable in some way such as being alone or lacking access to factual information.

ATTACK VECTORS

An attack vector is a specific path, method, or scenario that can be exploited to break into a computer system. Think of it as the steps the attacker takes to exploit the victim.

There are four main types of attack vector for social engineering:

1. Vishing/"Voice Phishing" (Social engineering over a telephone system):

- Can be used for reconnaissance purposes to gather more detailed intelligence on a target(s).

2. Phishing (sending a fraudulent message designed to trick a victim into doing something):

- This is usually done to either extract useful information or get them to click a malicious link.
- Often very general and are sent to many with the expectation that very few people will fall for it

3. Smishing (Using SMS text messaging to lure victims into a specific course of action):

- Usually done for the same reasons as phishing.

4. Impersonation (pretending or pretexting to be another person):

- Usually done to gain access to a system or building without verification.

CYBER SECURITY: ONLINE ACCOUNTS & SECURITY

CURIOSITY

At times, people can be exploited in rather creative ways (such as through our curiosity)

University of Illinois Urbana-Champaign study:

https://experts.illinois.edu/en/publications/users-really-do-plug-in-usb-drives-they-find

University of Illinois Urbana-Champaign study:

297 USB drives were left around the university campus grounds.

They were given innocent sounding files that alerted the researchers when opened (with an Internet connection).

135 of the 297 USBs (45%) ended up alerting the researchers (a file was opened).

Almost all of them (98%) were picked up and removed from where they were originally dropped.

More USBs could have been accessed (but no files were opened).

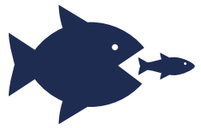
More could have opened the file than reported (but no Internet connection).

What if they were not really USBs and needed to be in a particular location?

OTHER USEFUL CONCEPTS

Tailgating – Gaining entry to a restricted area secured by an unattended electronic access control by following a person who has legitimate access. Common courtesy is exploited in some way to gain access (e.g. the legitimate person may hold the door open for you).

Spear phishing – A more sophisticated phishing attack that targets a few people at most. Unlike phishing attacks which are often very general, these attacks rely on a large amount of research on the victims. If you hold a high level position in a company or have access to valuable information, you must be vigilant for these kinds of attacks. The success rate is expected to and often is much higher than general phishing attacks.



CYBER SECURITY: ONLINE ACCOUNTS & SECURITY

Water holing – This is a targeted social engineering strategy that exploits the trust victims have in websites they regularly visit. This is done by creating a phishing attack that impersonates this website to instantly gain the trust of the victim. It is often a specific company/organisation that is targeted by this when they publicly give out a website service their employees use.

Baiting – A real-world Trojan horse that uses physical media to exploit the curiosity and/or greed of the victim (think USB study from earlier).