Since the birth of IT until today, we are all connected in one way or another with the internet in many ways. Even if we were born prior to the “digital age”, from when we are born our personal information is entered into a computer, when we first visit a doctor, when we get our drivers license or an ID card, when we open a bank account and all the social media, shopping, web browsing history and emails in between that. Our information is in what we commonly refer to as “Cyberspace”. Cyber being the prefix as anything related to something computer related, networks

## Cyberattacks!

Information is power and data creates information, therefore it would be true to say that all data is of high value and therefore vulnerable to attack for the purposes of theft, disruption or misuse. An organization or government network could come under attack for political issues or just to cause disruption/wreak virtual havoc or more commonly these days, financial gain and terrorism. Our own personal computer or devices can come under attack to gain personal or sensitive information about us or simply to knock out our system or information just to annoy us. All these attacks are commonly known as “Cyberattacks”.

## What is Cybersecurity?

Cybersecurity is the practice of protecting ourselves from cyberattacks. Installing policies, security experts and software to monitor our networks, systems, software and data.

## Why is Cybersecurity important?

Our lives rely so much on technology now that technology effects the way we travel, the lights in our house and keeping the food in the refrigerator on. Our information is stored in databases all over the place; government departments, hospitals, banks, phone companies, real world and online stores, email accounts, online games and various other applications that we use for business and entertainment.

The traffic lights, the air traffic control at airports, the trains and even the garbage man relies on data to keep our lives running smoothly and safely. Our police and military have sensitive information and real time information systems to secure our way of life. Telecommunications to connect us together with phone calls, video calls, chats, emails and tweets just to name some of the services, not to mention linking all of us together via the internet.

We are constantly creating data even if we don’t know it by going about our normal daily lives, watching something on tv, reading a webpage, using GPS, searching something up on the internet or giving a thumbs up to a picture or video.

A cyberattack at a personal level can leave us disconnected, our identity stolen, our personal information and memories lost.  
A cyberattack at a commercial level can ruin a company due to downtime, stock prices, customer lists, marketing or prototypes stolen, lower buyer or investor confidence.  
A cyberattack on a government level can mean personal information stolen on a massive scale. It could cause the shutdown of services such as health, transport and even effect the countries currency rate. In a worse case scenario, foreign governments could even affect the politics of a country.  
A cyberattack on a police or military level could severely risk our security. Evidence tampering, witnesses and potential suspects safety, knowledge of police surveillance operations, identities of law enforcement personal. Potentially this could lead to a large variety of crimes committed and being unsolved. If our military intelligence was cyberattacked it would affect the safety of our peacekeepers and ultimately our countries security. A worse case scenario is we could theoretically be invaded or the intelligence leak cause a war.

## Types of Cyberattacks

·         Malware

·         Ransomware

·         Distributed denial of service (DDoS) attacks

·         Spam and Phishing

·         Social engineering

MALWARE – is a term used to describe malicious software or “fake software”. Normally this software is downloaded from the internet or via an email. The user may think they are opening an attachment or installing a useful application, but actually its fake software that gets installed usually in the background. This software can steal, delete or encrypt your data. (Malwarebytes)

RANSOMWARE – is a type of malware that encrypts data or denies access to a system until a ransom is paid. Ransoms are usually paid in untraceable cryptocurrency. Once payment is received a code is sent to the owner or technician of the system to enter in to regain full access. The most common way to be infected with ransomware is via a phishing email. (Department of Homeland Security, 2016)

SPAM and PHISHING – Where spam is widely known as “junk Mail”, email that is unsolicited or unwanted. Phishing however is a cleverer type of spam. The email will appear to be from a legitimate source. The email may have a format and logo of a legitimate company and sometimes may even be addressed to you personally by name or simply say G’day mate! The email may ask for a reply or give a link to a website that also looks legitimate and have a similar URL that we would expect. Unknowingly the receiver is reply to or entering in personal information to a fake source.

DDoS – “*Distributed denial of service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems*”. (Rouse, 2019)

SOCIAL ENGINEERING -

## Implementing Cybersecurity

Unfortunately, in cybersecurity there is not a one system fits all as cyberattacks can come from multiple platforms and levels. Having the best firewall will still not defend an organization if its staff are untrained or stringent policies are in place. Consider for example your home computer. If your firewall pops up a warning that a website is not safe, but you click “it’s ok” and continue anyway, then all the technology and cost involved in developing that software is not the be all and end all solution. A company might spend thousands of dollars on hardware, software and personal; but if an employee plugs in their USB stick that they have been using at the local café, this could also infect the company’s network.

# References

Department of Homeland Security. (2016, July 11). *Ransomware \_ CISA.html*. Retrieved from Cybersecurity and Infrastructure Security Agency (CISA): https://www.us-cert.gov/Ransomware/Ransomware \_ CISA.html

Malwarebytes. (2019). *What is Malware\_ \_ Malwarebytes.html*. Retrieved from www.malwarebytes.com: https://www.malwarebytes.com/malware/What is Malware\_ \_ Malwarebytes.html

Rouse, M. (2019, April). *What is a DDoS (distributed denial of service) attack?* Retrieved from SearchSecurity: https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack/What is a DDoS Attack (Distributed Denial of Service Attack)\_.html