Assignment 2

**IT Technologies**

**Cybersecurity**

**What does it do?**

Cybersecurity is the defence of IT networks and systems through the use of firewalls, access control lists, and physical security, and many others. The main focus of cybersecurity is working to combat hackers and scammers, who try to steal money and personal data for their own advantage.

One major component is physical security, as once a hacker gains access to a device already connected to a network, or can connect their own device, they can easily bypass all security measures. This very instance occurred in 2014 when hackers gain access through physical security measures to Sony headquarters in Culver City, California. Reports from the hackers claimed that they gained access to the building through an unlocked door and used an administrator’s credentials to gain control of the network. Most security measures are implemented to prevent access from outside the network, not from within the network itself. This is where vlans and subnetting can be used to break up a private network into sections, which requires more work from a hacker to access the whole system.

Ways to implement physical security are restricting access to only those who require it, removing access once it is not required, locking down unused ethernet ports, restricting access to IT equipment and locking IT cabinets. But at lot of the problems with physical security is through people allowing access to hackers by being tricked or scammed.

Phishing is one way for a hacker to gain access to a network through the end user. Phishing is sending an email while posing as a corporation, government sector, a bank or another form of authority. They then convince the end user that, for example, the CEO wants them to pay a large sum of money to someone outside the organisation, or that the person receiving the email owes the Tax department money, and this needs to be paid immediately or they will have a warrant issued for their arrest. This preys on people’s fear and will often be distracting enough that it prevents the victim from thinking critically, making them more compliant. A Phishing email can also take the form of a corporation informing the user that their account has been hacked, and they need to reset their password through a link, which leads not to the official website of the corporation, but a copy the hacker has created. Once the end user has entered their username and password, the hacker can then use the credentials to access other accounts that may use the same password.

The best way to increase physical security where it relates to people is to educate everyone on what to look out for, and to remain vigilant and sceptical, and to look for details that will give away if an email is fraudulent. It is crucial that people think about what others have to gain by asking you to do a particular thing, like sharing information about yourself or signing up for a free service. It can be surprising what kind of personal information people will give away on social media, when asked by social engineers to participate in a game where people list the information most commonly used in password recovery, such as name of childhood pet, or name of the street they lived on as a child. This information can be sold between data miners or used by hackers to gain access to bank accounts or email accounts, where they can steal money or gain more personal data. It is important to restrict the information which is shared online to those you know and can trust, whenever possible.

Lastly, a firewall is a good basic defence against unlawful access. A firewall, such as NAT, is used on a router to prevent access from outside the network, unless a request was first made from inside the network, to which it can respond. This prevents a hacker from utilising an unused port to gain access to the router.

**What is the likely impact?**

As more people are using the internet for a wide variety of purposes, cybersecurity should be an important focus, for individuals and corporations. It is estimated that in 2019, cybercrime cost the global economy $1.5 Trillion. This drives up the cost of business and taxes, as corporations and governments spend more on cybersecurity measures. Hackers can use company data for corporate espionage, sharing trade secrets or even effect the stock price.   
For individuals the cost can be financial, or in the case of identity theft, can have other consequences. Hackers can use personal data to discredit someone or stalk and harass them. Nearly two thirds of internet users have had their personal data stolen at some point. Identity theft can cause significant disruption to people’s lives, by people having to prove fraudulent purchases or transfers were not done by them. Once a hacker has someone’s personal details, the can continue to open bank accounts and credit cards in the victim’s name, continuing the stress to the victim.

The impact cybersecurity has, when implemented correctly, is to provide security to individuals and corporations. Considering that corporate cybercrime is such a large industry, it is vital that more companies take cybersecurity seriously, and invest in employees, products and training to ensure they do not lose profits, consumer personal data entrusted to them, or positive public perception if a breach occurs.

Cybersecurity is a growing industry to combat the rise in cybercrime, so the demand will continue to create more positions in cybersecurity. These positions can consist of:

* Graphic Designers – Who design advertising designed to inform and teach others about cybersecurity
* Social Engineering Trainer – Who teach employees about the importance of cybersecurity and the way a hacker can try to scam them
* Network Security Admin – Who monitor networks for criminal activity and signs of a breach
* Social Media consultant – Who educate others on the dangers of social media
* Ethical Hackers – Who test systems by acting as potential hackers

**How will this affect you?**

I experience cybersecurity in my daily life in the form of two-factor authentication on a lot of devices and programs I use. When banking, my bank will send me a passcode to authorise a transfer over a certain amount, and when making purchases with my smartphone, I have a fingerprint lock and a passcode to prevent unauthorised access. I now use longer, more complex passwords than I have in the past, and I have different passwords for banking, emails and other accounts. This can be more difficult to remember, but it means if someone does gain access to one of my passwords, they won’t gain access to everything.

My work now occasionally sends out phishing emails to the staff to teach us what to look for, and how easy it can be to fall for a phishing email. This has taught me to be more sceptical of the emails I receive.

In February of this year parents had their ISP’s mail server hacked and the hacker used their password to gain access to their other accounts, as they used the same password for many of them. Thankfully the hacker didn’t gain access to the email account they use for password recoveries, and we were able to change all their passwords.

Learning about IT has made me much less likely to use public Wi-Fi, as others on the network can access your internet traffic from any page that isn’t encrypted. There is also the possibility that a hacker could set up an access point with the name of a free Wi-Fi to entice unsuspecting people to use the Wi-Fi for banking, or other secure logins, giving the hacker their login credentials.

Learning about cybersecurity is vital to reducing the chance of having personal data hacked. No technology is foolproof, and there is no way to guarantee that there will never be a data breach. The best way we can combat cybercrime is educate ourselves, educate others, and think about what others have to gain from our online behaviour.

**References**

Bort, J., 2020. *How The Hackers Broke Into Sony And Why It Could Happen To Any Company*. [online] Business Insider Australia. Available at: <https://www.businessinsider.com.au/how-the-hackers-broke-into-sony-2014-12?r=US&IR=T> [Accessed 10 April 2020].

Cisco. 2020. *What Is Cybersecurity?*. [online] Available at: <https://www.cisco.com/c/en\_au/products/security/what-is-cybersecurity.html> [Accessed 10 April 2020].

Cyber.gov.au. 2020. *Home Page | Cyber.Gov.Au*. [online] Available at: <https://www.cyber.gov.au/> [Accessed 10 April 2020].

GBHackers On Security. 2020. *A Rising Of E-Commerce Cyber Attack & Most Dangerous Threats Of 2019*. [online] Available at: <https://gbhackers.com/a-rising-of-e-commerce-cyber-attack-most-dangerous-threats-of-2019/> [Accessed 10 April 2020].

Hashed Out by The SSL Store™. 2020. *The Top Cyber Security Trends In 2019 (And What To Expect In 2020) - Hashed Out By The SSL Store™*. [online] Available at: <https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/> [Accessed 10 April 2020].

Itgovernance.co.uk. 2020. *Cyber Security*. [online] Available at: <https://www.itgovernance.co.uk/what-is-cybersecurity> [Accessed 10 April 2020].

Mcafee.com. 2020. *Economic Impact Of Cybercrime Report | Mcafee*. [online] Available at: <https://www.mcafee.com/enterprise/en-au/solutions/lp/economics-cybercrime.html> [Accessed 10 April 2020].

Medium. 2020. *Why Browsing On Starbucks Wi-Fi Is Dangerous And How You Can Best Play It Safe*. [online] Available at: <https://medium.com/gigareef/why-browsing-on-starbucks-wi-fi-is-dangerous-and-how-you-can-best-play-it-safe-959e7716f412> [Accessed 10 April 2020].

Minute, 2020. *Cybercrime Costs Global Economy $2.9M Per Minute*. [online] Infosecurity Magazine. Available at: <https://www.infosecurity-magazine.com/news/cybercrime-costs-global-economy/> [Accessed 10 April 2020].

PhoenixNAP Global IT Services. 2020. *17 Types Of Cyber Attacks To Protect Against In 2020*. [online] Available at: <https://phoenixnap.com/blog/cyber-security-attack-types> [Accessed 10 April 2020].

Rand.org. 2020. *Examining The State-Of-The-Art In Cybersecurity*. [online] Available at: <https://www.rand.org/randeurope/research/projects/cybersecurity-state-of-the-art.html> [Accessed 10 April 2020].

Technology.org. 2017. *Biggest Cyber Attacks And Their Cost For The Global Economy*. [online] Available at: <https://www.technology.org/2019/07/17/biggest-cyber-attacks-and-their-cost-for-the-global-economy/> [Accessed 10 April 2020].

Us.norton.com. 2020. *Do You Worry About Cyber Safety? Learn Some Smart Defenses.*. [online] Available at: <https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html> [Accessed 10 April 2020].