**An appreciation of techniques for mitigating privacy threats through appropriate security controls.**

There are a number of different ways in which your privacy online can be affected, including;

1. **Backdoor** – Bugs or exploits used to bypass security controls and gain access to your device or computer often from outdated or unpatched software.

*Solution* – Although hard to detect keep devices up-to-date with the latest patches.

1. **Direct-Access Attacks** – An attacker gains physical access to your device or computer.

*Solution* – Protect your devices in locked rooms/houses/offices when unattended and password protect them.

1. **Eavesdropping** – An attacker gains access to a network in order to monitor it and gain information.

*Solution* – Keep up-to-date antivirus, anti-malware, firewall and possibly download a network monitor to view your network traffic for unusual activity.

1. **Malware** – A program or software with malicious code, designed to infiltrate or damage a user’s computer or network.
2. *Viruses* – Malicious programs disguised or hidden within other programs that can replicate themselves, they can damage or modify data.
3. *Worms* – Similar to viruses but often spread through email.
4. *Trojans* – Malicious programs disguised as legitimate programs, cannot spread by themselves instead trick users into executing the program.
5. *Spyware* ­– Malicious programs that monitor user activity on a host or network such as personal information and banking details and return the information to the attacker.
6. *Ransomware* – Malicious programs that attempt to extort money from the victim, different levels of ransomware with some being ineffective and some encrypting files and documents until ransom is paid.

*Solution* –

* Keep up-to-date antivirus and anti-malware.
* Use caution when downloading or opening files/links/attachments.
* Do not click pop-ups.
* Only use freeware from legitimate sources.
* Be careful with website URLs.

(BBC Bitesize. 2021)

1. **Social Engineering** – Social engineering is a term referring to the manipulation or tricking of someone into giving out personal details.
   1. *Blagging* – An attacker will create an imaginary scenario to fool a victim into disclosing personal details. E.g. Nigerian prince fraud/an attacker claiming to be your bank or position of authority.
   2. *Phishing* – An attacker will send emails and texts to their victims attempting to manipulate personal details generally through links. E.g. A fake lottery or prize draw/impersonating a bank.
   3. *Pharming* – An attacker will create domain names very similar to popular websites and clone them, they will also send out fake links that will re-direct to their domain fooling people into entering their details. E.g. Ebayy.com domain name which looks identical to the eBay website.

These three different methods of social engineering attacks are generally used together but can work independently.

*Solution* –

* Be vigilant online when releasing personal details.
* Use caution when downloading or opening files/links/attachments.
* Be careful with website URLs.
* Be vigilant if using a public computer.
* Do not be fooled by something that seems too good to be true.

1. **Misconfigured Access Rights** – This is where incorrect permissions are set up allowing unauthorised individuals to view data or information not authorised to them.

*Solution* – Setting up the correct access rights and permissions on a computer or network when used by many different users is essential for data privacy and integrity.

1. **Unpatched and/or outdated software** – Attackers can gain access to your system by finding bugs and exploits in older versions of software or even the latest version.

*Solution* – Always keep your antivirus, antimalware and the majority of programs you use up-to-date with the latest versions and patches.

1. **Default and Weak Passwords** – A very common way for an attacker to gain access to computer when using default and weak passwords.

*Solution* – There are many sites and tools available to create a random selection of characters for you but a good password should follow the general guideline;

* A mix of upper and lower case characters
* Special characters/symbols
* Numbers
* Contain at least 8 characters
* Not something that is easily guessed by knowing you
* Not a word
* Ideally change your password on different websites and regularly

(Lacey, 2020 & Amankwa, 2021)

# References

Amankwa, E., 2021. Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, 12(04), pp.233-249.

BBC Bitesize. 2020. *Other cyber security threats - Fundamentals of cyber security - AQA - GCSE Computer Science Revision - AQA - BBC Bitesize*. [online] Available at: <https://www.bbc.co.uk/bitesize/guides/znnny4j/revision/4>

BBC Bitesize. 2021. *Threats to networks - System security - OCR - GCSE Computer Science Revision - OCR - BBC Bitesize*. [online] Available at: <https://www.bbc.co.uk/bitesize/guides/zj89dxs/revision/2>.

Lacey, N., 2020. *Teach yourself the Fundamentals of Cyber Security*. [online] Droylsdenacademy.com. Available at: <https://www.droylsdenacademy.com/force\_download.cfm?id=3377>//\*\*WARNING\*\*// downloads a PDF, access through main site.