|  |  |  |  |
| --- | --- | --- | --- |
| Module Code | DWD 507 | Module Title | DWD 507 Cyber best practices |
| Student ID | 3201807 | Name | Jack Bradley-Coombes |

**Instructions**

In this activity you will list the best protocols for dealing with each cyberthreat and have 2 sources per point and 50 to 70 words on each point

* **Malware**

Malware is a malicious software which infects computers, and can harm them in many ways, like taking data or locking you out. Making backups for your valuable data and running an anti-virus software can help protect your device from malware. If your device is already infected, you should disconnect said device from the network, starting your device in safe mode, deleting any temporary files, then running a virus scan. Once the virus is detected have the antivirus delete it. After removing the virus it’s a good idea to change any passwords or other sensitive information.

Sources: <https://www.kaspersky.com/resource-center/threats/how-to-get-rid-of-a-computer-virus> , <https://support.microsoft.com/en-us/topic/how-to-prevent-and-remove-viruses-and-other-malware-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5>

* **Spyware**

Spyware, also known as adware, is a software then when installed on your computer, can send pop-ups to your device, redirect to certain websites, or record what websites you visit, usually for advertisement purposes. In extreme cases, some spyware can track what keys you type, allowing them to read your passwords to use for malicious purposes. The best way to avoid spyware is to be careful online, avoid clicking pop-ups, be wary of sketchy software, and don’t click links in emails, unless you are 100% sure they are safe. Using an antivirus is also always a good idea. Running your anti-virus or a specialized anti spyware problem is the best way to root out the spyware and remove it from your system.

Sources: <https://www.cisa.gov/news-events/news/recognizing-and-avoiding-spyware> , <https://us.norton.com/blog/how-to/detect-spyware>

* **SQL injections**

SQL Injection (SQLi) is an attack that makes it possible to execute malicious to Structed Query Language (SQL) statements. A majority of modern websites and applications connect to Structed Query Language (SQL) databases, making them vulnerable to SQLi. A good way to protect yourself from SQLi is to use strong login credentials and only store necessary data for an application to function. Websites can use database filters to filter out malicious code from users and restrict access to their databases.

Sources: <https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks/#prevention-methods>, [Cyber Security on the Web: DWDD507-V1 : Security and Testing (instructure.com)](https://atcnz.instructure.com/courses/3658/pages/cyber-security-on-the-web?module_item_id=19264)

* **Phishing links**

Phishing is a type of attack that attempts to steal money or information from you, by pretending to be a trustable source, and having you click malicious links. These attacks are usually sent by email but could be in other places like social media or websites. A good way to avoid phasing is to be suspicious of links, look for errors or differences in links before clicking them and make sure you trust the source you received them from. If caught by a phishing attack, you should call your bank to lock your account and backup any other sensitive data.

Sources [Cyber Security on the Web: DWDD507-V1 : Security and Testing (instructure.com)](https://atcnz.instructure.com/courses/3658/pages/cyber-security-on-the-web?module_item_id=19264), <https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>

* **Man in the middle**

Man in the middle attacks is an attack that allows attackers to steal your information, usually done through public Wi-Fi. The attacker can view your activity and steal any information you access while on the same connection. Good ways to protect against Man in the middle attacks could be, never accessing any sensitive data or passwords on public Wi-Fi, or never using public Wi-Fi altogether. Its also good to ensure websites have valid SSL certificates when visiting.

Sources: <https://www.strongdm.com/blog/man-in-the-middle-attack-prevention>, [Cyber Security on the Web: DWDD507-V1 : Security and Testing (instructure.com)](https://atcnz.instructure.com/courses/3658/pages/cyber-security-on-the-web?module_item_id=19264)

* **D.O.S attacks**

Denial of Service (DOS) attacks can make your application unable to function for a period of time, resulting in the app becoming unusable for a period of time, breaking trust, and resulting in costly bills due to wastage of cloud hosting resources. Good ways to prevent this type of attack would be using services capable of detecting and deflection spam requests.

Sources: [Cyber Security on the Web: DWDD507-V1 : Security and Testing (instructure.com)](Cyber%20Security%20on%20the%20Web:%20DWDD507-V1%20:%20Security%20and%20Testing%20(instructure.com)), <https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/>