**AWARE OF MALWARE**

**Submitted to:**

**Agpoon, Claire**

*BSIT 3A IAS1 ACT 5*

**Submitted by:**

**Mr. Gabriel Thomas Torneros**

*Teacher*

**March 14, 2022**

**Aware of malware**

**Introduction (brief background about malware):**

According to Lutkevich, B. (2022, June 13). Malware. Is a malicious software in computer, it is any program or file that intentionally harmful to a computer network server.

**Purpose:**

The purpose of this study is to be aware about malware viruses or any threats attack on the computer. To protect and secure all the personal identity, files and other credentials, and avoiding data breach and hacking.

**1. How secure do you think chien's network is from virus attacks?**

* Based on the scenario, he followed the policy guidelines for antivirus threats to avoid thinking' about what he needed to do to resolve this kind of situation. Actually, he doesn’t have to worry about it if the anti-virus and threat protection on his device, is always activated in Window Security. He needs to always check and update to see if there are any malicious threats or viruses on every machine to defend against malware infections. Even if they have firewall protection, it will be possible to receive any certain virus threats and malware that potentially bypass these defenses or evade detection. Because they don't know if their students download, any application that they don't know has a virus or open a site that they don't know is phishing. Especially now, it has a lot of viruses or hacking that can get your credentials and use them for any crimes. Therefore, he needs to tell his students that they’re not allowed to download anything or click on any website. In addition, teach their students about viruses and hacking to give them ideas and help them avoid this kind of problem.

**2. What areas has chien not secured?**

* Based on the case scenario. He cannot secured from phishing site and anything malware or unauthorized access. Because even they apply or put a firewall or antivirus software, they can still possible to bypass the protection via, downloading application in infected webpage or website. Also through transferring files via flash drive, if the flash drive has infected that they don't know. It will spread it in another computer and so forth. Therefore, he just need to check always the third-party apps and they can always update and check the scanner virus and window security and put a Data encryption to protect the system from unauthorized access and to enhance data security.

**3. What recommendations would you make to chien?**

* I recommend it to put them a data encryption to protect their system from unauthorized access and malware viruses to secure any credentials, files, sensitive data and against data breaching. If they have add a data encryption to their security, it can strongly secured there on virus threats because it can secure it to protect the credential status in email attachment, website or else. They need to update always the security and block all third party cookies.