Date: April 3, 2020
Submission date: April 10, 2020
Teacher: Mr.Smith

Networks Research Task

ICS2O1-02

Terry Su

Milliken Mills High School

Terry Su

Network Security Systems

Anti-Spyware

Malware is an umbrella term for software programs or codes that may be harmful to a computer, they are designed by cybercriminals to disrupt, damage or gain unauthorized access to a computer system. Spyware and adware are two specific types of malware.

Spyware is a category of software that intercepts information and sends it to a third party. It tracks a computer user's activity and gathers personal information without consent. They take up an enormous amount of your computer's resources, cause the device to run slowly leading to crashes often, and even overheat your computer causing permanent damage. On the other hand, Adware functions to provide revenue to the developer by generating online advertisement on the user's interface. Adware is one of the least dangerous types of malware but can negatively impact a user's experience by causing the computer and browsers to run slower.

Specifically for preventing spywares, an anti-spyware is a type of software that is designed to detect and remove unwanted spyware program installations. An anti-spyware detects spyware through rules-based methods that flag common spyware programs. Anti-spyware softwares finds and removes spyware that has already been installed on the computer, or prevents spyware from being downloaded in the first place. However, most modern security programs bundle the anti-spyware functionality in antivirus protections, personal firewalls, etc. Nonetheless, anti-spyware may be ineffective against newer forms of spyware that have yet to be discovered and are hard to be identified by security softwares.

Some other good ways to prevent your device from being compromised with spyware are to keep your device updated, not opening unknown links/attachments, and to use a secure browser.

Social media is regularly used by many nowadays and contributes to the problem of personal information misuse. It may involve tracking a user's preferences to harvest data or messages leading to privacy leaks. To limit this risk; not posting information about yourself, not posting pictures of yourself or others without consent, and using a unique password for each social network helps reduce the chance of privacy violations.

Anti-Virus

A computer virus is the main type of malware that can damage and distort computer function. Once inside a computer, a virus can replicate itself and spread onto other computers in your network. They can corrupt data, manipulate files, spam contacts, lead to failed system performance or take over the entire computer. Computers are infected by viruses often due to an action that allows the virus to enter the computer. Common ways to be infected are; opening unknown links/attachments from emails which sometimes fake legitimate messages, downloading software from an illegal website, clicking on suspicious ads and having security vulnerabilities. Theoretically, all computer devices including phones and tablets are able to receive a virus, as long as there is a way for it to attach it's software onto the computer.

Antivirus softwares are used to detect and remove viruses from your computer. In order to achieve its claim to protect your device, antivirus softwares are designed to scan web pages, files, software and applications that are travelling in your network. They recognize suspicious behavior in a program and seek to block out or eliminate the virus causing the trouble. Installing a trusted antivirus software on your computer is one of the most effective ways to prevent known viruses. The main issue is that no existing antivirus is 100% failure-proof. Cybercriminals innovate by using unrecognized coding that appears unharmful to antivirus software. Unfortunately, new advanced infections have been known to slip past the filters, an antivirus software may not be able to protect you from these. However despite the imperfections, premium antivirus softwares are still one of the best ways to stay secure.

In addition, other effectual ways to prevent your devices from being infected may be to: secure all personal information with strong passwords, apply all computer updates immediately, always backup your files and stay alert of suspicious websites or emails.

Firewalls

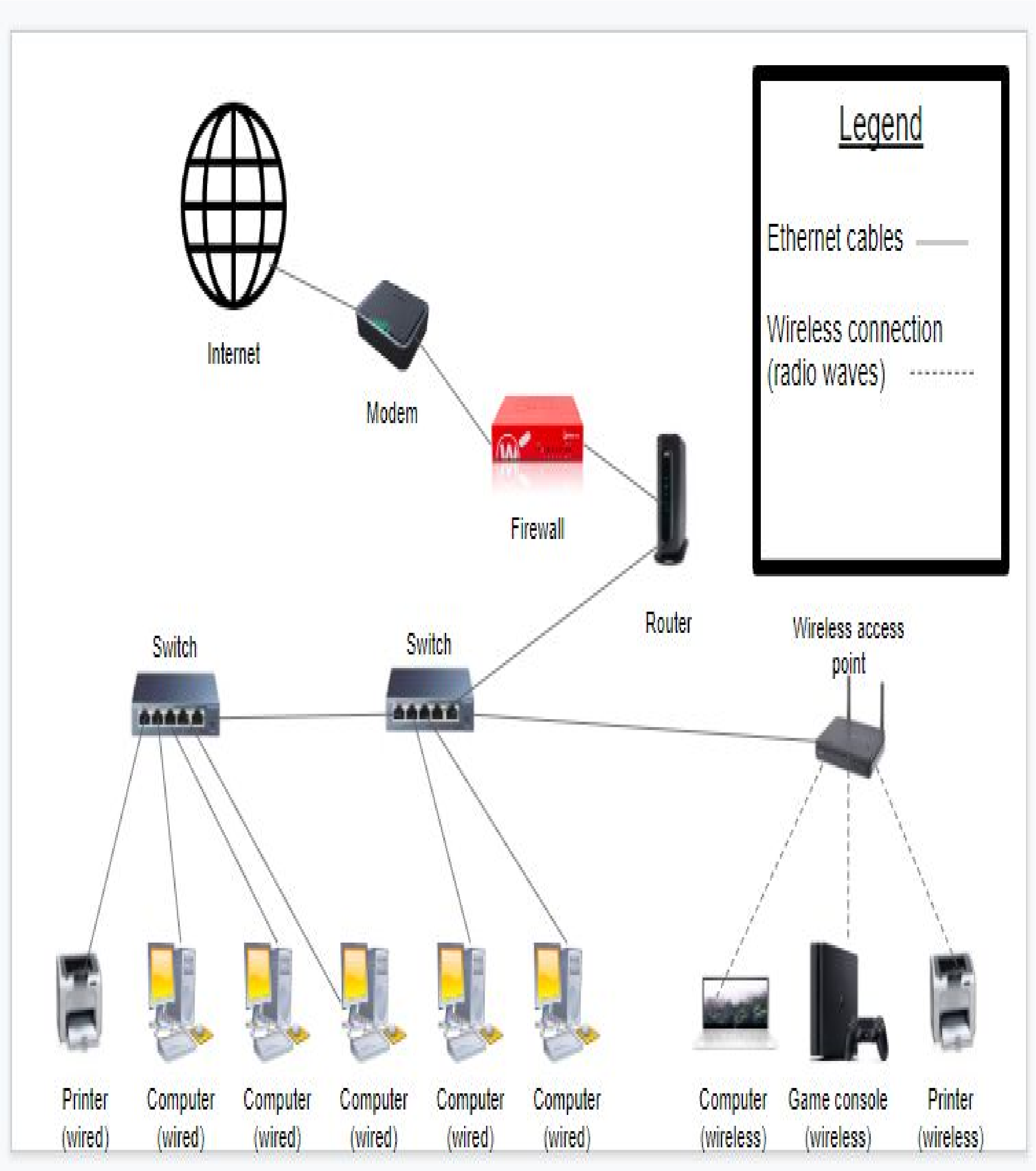
A firewall is a system that filters incoming data packets and outgoing data packets to and from the internet for network security. It is used to prevent most malicious traffic from entering a private network and cause harm while allowing all legitimate network traffic to flow freely through the firewall, creating a safety barrier between a private network and the public internet. Some basic methods that different firewalls use to filter traffic are: packet filtering, stateful inspection, and using a proxy server.

Firstly, the most common firewalls are packet filtering firewalls. It is when a firewall intercepts all network traffic to and from a private network and evaluates it against a set of custom rules to determine if it is allowed to flow into the network. The rules may typically be the source IP address, source port, destination IP address, and destination port. Secondly, Stateful inspection firewalls not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering. Lastly, Proxy servers are usually installed to boost the performance of the network but may also be used as firewalls. Proxy servers hide your internal addresses so that all communications appear to originate from the proxy server itself by masking the IP address for privacy and security. It essentially provides the most protection.

Firewalls are able to prevent most malicious data and traffic from penetrating into your network. However, they cannot protect you against modern viruses as most firewalls are not configured with newer virus definitions. Firewalls also do not avert intruders trying to trick computer users into compromising their computer's security. For example, they may send an email to lure for sensitive information. If permission is granted through the internet, a firewall would not be able to prevent resulting damages. Hackers could possibly access and misuse your computer or network, often by tricking you into downloading malicious software that will damage your computer or giving up personal information, by email or social networks. One of the most common hacker strategies is phishing. They create phishing emails that appear to have come from a close friend/relative or a legitimate organization. These emails generally try to create an urgency or panic to trick users into giving out their personal details. Firewalls cannot prevent this.

A firewall DMZ(demilitarized zone) is a zone without the protection of a firewall. It is used to divide a network into two parts, by taking devices inside a protected network and putting them outside the firewall. By doing this, malicious activities will be detected before going through the firewall and into the private network. A firewall DMZ is commonly used by companies to protect internal information sometimes by placing public servers like web or email servers outside the firewall. They may even add an additional firewall for extra security.

SOHO Network Diagram



Works Cited

Admin, byBCom, et al. “What Is Spyware, Adware, and Malware? • Dakota Central.” *Dakota Central*, www.dakotacentral.com/knowledge-base/what-is-spyware-adware-and-malware/.

Alexandru. “10 Key Growth Hacking Strategies for Any Business.” *Medium*, ART Marketing, 6 Mar. 2020, artplusmarketing.com/10-key-growth-hacking-strategies-for-any-business-4d436e5220b6.

“Antivirus, Anti-Spyware, & Anti-Malware Software.” *Malwarebytes*, www.malwarebytes.com/for-home/products/.

“Barracuda Networks.” *What Is a DMZ (Networking)? | Barracuda Networks*, www.barracuda.com/glossary/dmz-network.

Beaver, Kevin. “Check IT List: How to Prevent Spyware.” *SearchSecurity*, TechTarget, 23 May 2005, searchsecurity.techtarget.com/tip/Check-IT-List-How-to-prevent-spyware.

Benton, Brian, et al. “Infected! 10 Tips How To Prevent Malware On Your Computer.” *Redshift EN*, 22 Dec. 2018, www.autodesk.com/redshift/10-tips-on-how-to-prevent-malware-from-infecting-your-computer/.

Cutolo, Morgan. “Should You Be Worried About Your Cell Phone Catching a Virus? (Spoiler Alert: Yes!).” *Reader's Digest*, Reader's Digest, 30 Aug. 2018, www.rd.com/advice/saving-money/cell-phone-virus/.

“Dryden Municipal Telephone Service.” *What Can't a Firewall Protect against? " Dryden Municipal Telephone Service*, www.dmts.biz/faqs-firewalls/what-cant-a-firewall-protect-against/.

Ferrell, Robert G. “The 5 Different Types of Firewalls.” *SearchSecurity*, TechTarget, 13 May 2019, searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls.

Garcia, David. “Leaking Privacy and Shadow Profiles in Online Social Networks.” *Science Advances*, American Association for the Advancement of Science, 1 Aug. 2017, advances.sciencemag.org/content/3/8/e1701172.

Geeks on Site. “What Is Antivirus Software and How Does It Work?” *Geeks on Site*, 25 Oct. 2017, www.geeksonsite.com/computer-security/what-does-virus-scan-do-how-antivirus-software-works/.

“How Does Malware Impact Your Computer's Performance?” *Computer Services in Peoria*, 31 Mar. 2017, www.clearpathit.com/how-does-malware-impact-your-computers-performance.

Symanovich, Steve. “Why Antivirus May Not Be Enough.” *Official Site*, us.norton.com/internetsecurity-privacy-why-antivirus-may-not-be-enough.html.

“What Is A Computer Virus?” *NORTONâ¢ - Antivirus Software and Spyware Removal*, ca.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

“What Is a Firewall?” *Cisco*, Cisco, 28 May 2019, www.cisco.com/c/en_ca/products/security/firewalls/what-is-a-firewall.html.