International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 12, December-2020

Cybersecurity Defense

Md Tapon Mahamud Jony
B.sc in EEE, MBA

***Abstract*:- An intruder can access your real life from your virtual life data! Now a day's data breach is one of the common words from small to multinational companies. Now days, many companies spent billions of dollars only to protect their private or public data. From this journal I tried pulling up the matrices and your role while you are entering to the internet world and protect yourself from the different types of hacker who are waiting for your small tiny mistakes.**

Table of Contents

1. WHY PERSONAL DATA PROTECTION IS SO IMPORTANT?

Do you know a hacker can access your real life from your virtual life data! Let's learn how to manage your personal devices and your personal data. It includes tips for protecting your devices, creating strong passwords and safely using wireless networks. It also discusses maintaining your data securely. Your online data is worth something to cyber criminals. This e-book covers authentication techniques to help you maintain your data securely. It also covers ways to enhance the security of your online data with tips about what to do and what not to do online.

Figure 1: Data Protection

2. PROTECTING YOUR COMPUTING DEVICES

Your computing devices store your data and information for your online life. To protect yourself from the intruders you need to keep your information secured. Below is a short list of steps you can take to protect your computing devices from hacking.

3. KEEP THE FIREWALL ON

Firewall must be on to protect your devices from unauthorized access. Whether it is a software firewall or a hardware firewall on a router, the firewall should be turned on and updated to prevent hackers from accessing your personal or company data. Although few applications required firewall should be turned off to install them onto the device. Think twice before installing such application which required firewall off.

Figure 2: Firewall and device

4. Use Antivirus and Antispyware

By using efficient antivirus software you can prevent many malwares to gaining access of your devices. So choosing right antivirus program is very crucial. Malicious software, such as viruses, Trojan horses, worms, ransomware and spyware, are installed on your computing devices without your permission, in order to gain access to your computer and your data. Viruses can destroy your device data, slow down your computer, or take over your computer from anywhere of the world. One way viruses can take over your computer is by allowing spammers to broadcast emails using your account. Spyware can monitor your online activities, collect your personal information, or produce unwanted pop-up ads on your web browser while you are online.

Figure 3: Antivirus importance

A good rule is to only download software from trusted websites to avoid getting spyware in the first place. Antivirus software is designed to scan your computer and incoming email for viruses and delete them. Sometimes antivirus software also includes antispyware. Keep your software up to date to protect your computer from the newest malicious software. These are few common antivirus application widely used by the users i.e Microsoft Security Essentials, Bit Defender, Kaspersky, Avast, Norton, AVG, Comodo, Reve etc.

5. MANAGE SECURITY UPDATES REGULARLY

Hackers are always trying to take advantage of vulnerabilities in your operating systems and your web browsers. To protect your computer and your data, set the security settings on your computer and browser at medium or higher. Update your computer’s operating system including your web browsers and regularly download and install the latest software patches and security updates from the vendors. Sometimes we get irritated when see an update notification from vendor, don’t ignore this once there is any update notification from vendor you should read the description first what is new in the update then allow.

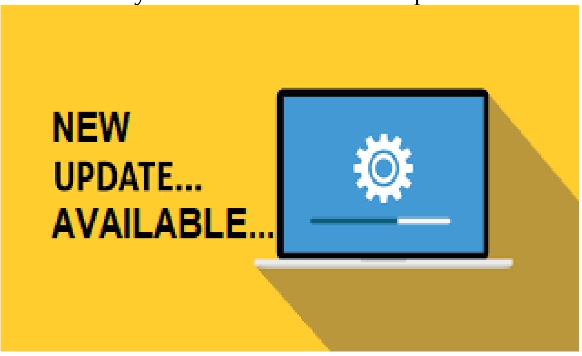

Figure 4: Manage security patches

6. PROTECT ALL YOUR DEVICES

We utilize a same password across various portals; we use passwords that are simple for others to make sense of – and simply trust in the best. Passwords are as important as we use to verify anyone identity – like driving license, Social Cards, Passports and other valid identities. A strong password can help you to prevent unauthorized access from your personal profiles and information database.

Figure 5: Passwords strength

Your computing devices, whether they are PCs, laptops, tablets, or smart phones, should be password protected to prevent unauthorized access. The stored information should be encrypted, especially for sensitive or confidential data. For mobile devices, only store necessary information, in case these devices are stolen or lost when you are away from your home. If any one of your devices is compromised, the criminals may have access to all your data through your cloud-storage service provider, such as iCloud, Google drive or Dropbox. IoT devices pose an even greater risk than your other computing devices. While desktop, laptop and mobile platforms receive frequent software updates, most of the IoT devices still have their original firmware. To reach the Internet, most IoT devices manufacturers rely on the customer's local network. The result is that IoT devices are very likely to be comprised and when they are, they allow access to the customer's local network and data. The best way to protect you from this scenario is to have IoT devices using an isolated network, sharing it only with other IoT devices.

7. WIRELESS NETWORKS SAFELY

Wireless networks allow Wi-Fi enabled devices, such as laptops, tablets, smart phones, to connect to the network by way of the network identifier, known as the Service Set Identifier (SSID). To prevent hackers from entering your home wireless network, the pre-set SSID and default password for the browser-based administrative interface should be changed. Intruders will be aware of this kind of default access information. Optionally, the wireless router can also be configured to not broadcast the SSID, which adds an additional barrier to discovering the network. However, this should not be considered adequate security for a wireless network. Furthermore, you should encrypt wireless communication by enabling wireless security and the WPA2 which is the strongest authentication feature on the wireless router. Even with WPA2 encryption enabled, the wireless network can still be vulnerable. In October 2017, a security flaw in the WPA2 protocol was discovered. This flaw allows an intruder to break the encryption between the wireless router and the wireless client, and allow the intruder to access and manipulate the network traffic.

Figure 6: Wireless network safety

For laptops or other devices with wired NIC, a wired connection could mitigate this vulnerability. Furthermore, you can also use a trusted VPN service to prevent the unauthorized access to your data while you are using the wireless network. When you are away from home, a public Wi-Fi hot spot allows you to access your online information and surf the Internet. However, it is best to not access or sends any sensitive personal information over a public wireless network.

8. USING VPN SERVICE

The VPN service provides you secure access to the Internet, with an encrypted connection between your computer and the VPN service provider's VPN server. With an encrypted VPN tunnel, even if a data transmission is intercepted, it is not decipherable. Many mobile devices, such as smart phones and tablets, come with the Bluetooth wireless protocol. This capability allows Bluetooth-enabled devices to connect to each other and share information. Unfortunately, Bluetooth can be exploited by hackers to eavesdrop on some devices, establish remote access controls, distribute malware, and drain batteries. To avoid these issues, keep Bluetooth turned off always when you are not using.

Do not share much information on your social media particularly. This platform is the first choice for intruders; you should never share any personal information in a web which is not relevant for your purpose. If you order something from any site that must be delivered, the supplier asks your credit card details or bank account number to check payment status. You can ask them why they need it if you already made the transactions online! If you suspect anything from the caller's side, then it's advisable not to share anything without re-confirm the order yourself. Thousands of cases like this every day happening surrounding us. We have to keep your eyes on stop mouths before share anything over the phone without justifying.

9. REFERENCES

[1] Ashish Patel, J. T. (2020). A malicious activity monitoring mechanism to detect and prevent ransomware. *Computer Fraud & Security* , https://www.sciencedirect.com/science/article/pii/S1361372320300099.

[2] Besemer, L. (n.d.). Retrieved June 10, 2020, from https://www.exin.com/data-protection/why-is-data-protection-so-important/

[3] Elizalde, D. (n.d.). Retrieved June 20, 2020, from https://danielelizalde.com/iot-security-hacks-worst-case-scenario/

[4] European Commission. (n.d.). *Data protection*. Retrieved June 23, 2020, from https://ec.europa.eu/info/law/law-topic/data-protection_en

[5] Fielding, J. (2020). The people problem: how cyber security's weakest link can become a formidable asset. *Computer Fraud & Security* , 6-9.

[6] *Intersoft Consulting*. (n.d.). Retrieved June 22, 2020, from https://gdpr-info.eu/issues/personal-data/

[7] Jenkins, S. (n.d.). Retrieved June 20, 2020, from https://www.techsafety.org/passwordincreasesecurity

[8] Jony, T. M. (n.d.). Retrieved June 22, 2020, from https://www.booktopia.com.au/cybersecurity-basics-md-tapon-mahamud-jony/ebook/9781794801967.html

[9] Norton. (n.d.). Retrieved June 23, 2020, from https://us.norton.com/internetsecurity-iot-smart-home-security-core.html

[10] Rouse, M. (n.d.). Retrieved June 23, 2020, from https://searchdatabackup.techtarget.com/definition/data-protection

[11] Wikipedia. (n.d.). Retrieved June 23, 2020, from https://en.wikipedia.org/wiki/Antivirus_software

[12] Wikipedia. (n.d.). Retrieved June 10, 2020, from https://en.wikipedia.org/wiki/Antivirus_software