Protecting Your Devices Against Malicious Attacks.

Mohammed. I. Mohammed

Abstract—The increasing reliance on digital devices in our daily lives, has brought about the heightened risk of cyber-attacks on our personal devices. This article highlight various strategies and method individuals can employ in their daily lives, to protect their devices against cyber attackers.

By examining some common method and techniques used by cyber attackers to target vulnerable devices and exploit security weaknesses, this article discusses on how to identify malicious links and approach to differentiate between authentic and malicious website links, it also highlights the tips to follow to protect your device from cyber-attacks.

This article will provide and equip individuals with requisite knowledge on how to protect your devices, and safeguard your sensitive information stored on the device from being compromised.

***Index Terms*—Vulnerability assessment, cybercrime, malware, social engineering.**

I. Introduction

In this era, dominated by technology, the threat of cyber-attacks keeps increasing every day, posing a significant risk to individuals and organizations. With the rise of advanced hacking tools and techniques, protecting our devices from cyber threats is necessary.

According to cyber security ventures, cybercrime was estimated to have cost the global community $6 trillion each year by 2021, Doubling from $3 trillion in 2015. In a report titled “2017 Crime Report,” Opaluwa (2016)

Stated that cybercrime in Nigeria resulted in a loss of $9.3 billion for the country.

This article seeks to highlight various techniques and strategies to explore and identify malicious links and tips to protect our devices. By examining the rise of sending and receiving website links, it is crucial to identify legitimate website links, this article aims to discuss on tips to follow to protect your devices.

fostering a culture of digital awareness is crucial at this digital era, it can help individuals to understand and avoid cyber-attacks and protect their devices from falling into the hands of cyber attackers, there is a popular saying that protection is better than cure.

Let define some useful terms related to the topic.

Protection is the mechanisms and techniques put in place to safeguard devices from unauthorized access by malicious users.

Vulnerabilities: are loopholes or weakness in a device that could potentially be exploited by an attacker to gain unauthorized access to a device.

Malicious attackers are also referred to as black hackers; are individuals that attack computer devices with a malicious intent in order to exploit vulnerabilities to have unauthorized access to that device. After getting unauthorized access to a device, they steal valuable information such as password or bank information, or cause harm to that device by decrypting a particular sensitive information and request for a ransom money to decrypt the information.

Malicious hackers they hack devices and get valuable information, they do this because of Money, political reasons.

White hackers differ from malicious hackers, White hackers penetrate through a device in order to identify its various vulnerabilities and to find a solution to that.

Protecting your device against malicious attackers: refers to the mechanisms and techniques put in place by a user in order to safeguard the device from harm or unauthorized access by malicious hackers to avoid compromising sensitive information.

Is protecting your device expensive? If so, try not protecting the device and compare the cost.

II. Tips to identify malicious links

- Always ensure that the link is secure – before clicking a link, always ensure that the application layer protocol is secure(https).
  Click in the search box address of a web browser and check the web address, if “s” is present at the end of http (that is, https), then the site you want to reach is secure, and the information will be encrypted using any of the encrypted algorithm.

- Hover over the link before clicking – before you click any link, hover over the link and look at the bottom left side of your device you will see the actual destination that the link will forward you to, then compare the link inside the search box with the one at the bottom side, if they are the same then the link is safe and secure. Otherwise, it is a malicious link.

- Copy and paste the link in a website that identify malicious links – website that identify malicious links for example *Virus Total*, *Virus Total* is a website that analyzes files and URLs for suspicious activities and potential malware threats. It verifies the legitimacy of a link; *Virus Total* will provide you with a detailed report on the link safety, it will rate it in terms of percentage.
- Delete any suspicious email – deleting emails that indicate any sign of suspicion especially those that contain suspicious links or attachment.
- Avoid clicking a link from unknown sender – before you click a link Always make sure that you verify the legitimacy of that link by subjecting it to the above steps.

III. Tips to Protect Your device

- Update Your Applications regularly- updating your application regularly is crucial, it helps to protect you against malicious hackers that are looking for loopholes or vulnerabilities to exploit.

  Application developers are always looking for loopholes in their applications to fixed it, so they update their applications regularly to keep it secure, you have to update your application regularly as to have the latest version on your phone to avoid those vulnerabilities that hackers use to exploit to gain unauthorized access or damage to a device.

- Be cautious of pop-up alert – pop-up alert usually comes up while surfing the net, they usually request for you agreement to accept, if you give them permission, they will have access to your device.

- Install antivirus software – are software that are specifically designed to prevent your device from malware (malicious software), it typically runs in the background to protect your device from harm by malicious software.

- Protect your device with a strong password or biometric – password is any form of code that a user has to enter to have access to his device. The password has to be combination of letters, alphabets and characters, in order to have a strong password and to reduce the probability of guessing that password. Hackers usually use robot now a days to crack the password by trying different combination of code, they usually do this with a sophisticated software.

- Be careful of pop-up alert, calls or emails that request your personal information in a sense of urgency: The suspicious Email or text message is usually an offer that seems too good to be true, be careful of such offers.

IV. Conclusion

In this era of digitization, protecting your device is not optional, but mandatory to preserving your personal identity. You have to be vigilant all the time, as we discussed in the above bulletin, it gives you an insight on how to take proactive measures to protect your device from malicious hackers. Never underestimate the importance of keeping your device secure from hackers. It only takes one breach to cause irreparable damage, don’t make it easy for them to access your sensitive information.

Remember, hackers are always looking for vulnerabilities to exploit, by putting these preventive measures into practice, it will keep your device safe and secure.

In this digital era, security of devices is a measure concern by many individuals and organizations. Many organizations suffer from different form of hacking, which are now in great need of cybersecurity expert.

Thank you for reading, stay safe and secure.

V. REFERENCES

- Johansen A. G. (2020, August 2015). “11 Ways to help protect yourself against cybercrime”. https://us.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-from-cybercrime
- “Protect your PC from ransomware” by Microsoft: https://support.microsoft.com/en-us/windows/protect-your-pc-from-ransomeware-08ed68a7-939f-726c-7e84-a72ba92c01c3

VI. BIOGRAPHY

Mohammed Ibrahim Mohammed is a 400-level student from Computer and Communication Engineering.

He hails from Gombe State, He attended Hammadaji International School for his primary education, his Junior Secondary School at Modibbo Tukur College of Arabic and International studies and then transition to Ilimi international for only a term, after his First term he transition to Pen Resource Academy.

He wrote his WAEC and Jamb in 2018, and secured admission into ATBU Bauchi.

He was an Academic tutor in Computer and Communication engineering and doubles as his departments Auditor General.

He participated in international youth math challenge and was honored with a certificate of participation.

He is dedicated and proactive undergraduate student who excels in professional and Academic roles both within and outside campus.