International Journal of Cyber Security (IJCS)
Volume 2, Issue 1, January-June 2024, pp. 28-33, Article ID: IJCS_02_01_003
Available online at https://iaeme.com/Home/issue/IJCS?Volume=2&Issue=1
Impact Factor (2024): 1.68 (Based on Google Scholar Citation)
Journal ID: 2145-6523

CYBERSECURITY AND ITS ASSOCIATED THREATS

Riyya Hari Iyer
Software Engineer, Brooks Automation, Fremont,
California, United States

ABSTRACT

This study highlights the pressing need for cybersecurity awareness in today's digitally interconnected world. With the pervasive use of electronic devices and smartphones, privacy and security concerns have become paramount. The concept of cybersecurity is introduced as crucial for safeguarding individuals, organizations, and governmental data from cyber threats. Emphasis is placed on the importance of continuous efforts to protect personal and organizational information, with a focus on understanding and combating social engineering techniques. Lastly, the alarming frequency of cybercrimes, occurring every 39 minutes, underscores the urgency for proactive cybersecurity measures.

Keywords: Cybersecurity, Privacy, Electronic Devices, Social Engineering, Cybercrimes

Cite this Article: Riyya Hari Iyer, Cybersecurity and Its Associated Threats, International Journal of Cyber Security (IJCS), 2(1), 2024, 28-33.
https://iaeme.com/Home/issue/IJCS?Volume=2&Issue=1

While the world has benefitted extra-ordinally from the development in computing power, communication explosion and the internet, plenty of unintended, unwanted, but surely unpreventable hindrances, complications, and impediments have also come as side effects of the immense benefits.

In today's world, where one's life is being completely managed by electronic gadgetsand the smart phone having a role to play in controlling one's various day to day activities, privacy isn't completely available, security isn't certain, and threats are round the corner looming everywhere.

One must understand the associated cyber threats and their prevention. Hence one must understand cybersecurity and also what could be done or is being done to protect ourselves from these threats. Cybersecurity, in very simple words, refers to the concept of protecting an individual as well as institutions, organizations and its employees, governmental data and information from cyber threats.[1]

Irrespective of the scale of the business or the number of employees in any organization, there should be continuous efforts to protect employees' data and personal information as well as that of the organization. Organizations must be waryof the crimes that happen in the domain of cyber-security. The term for this is SocialEngineering.

Social engineering refers to all techniques aimed at talking a target into revealingspecific information or performing a specific action for illegitimate reasons.[2]

Cyber-crimes happen frequently. There's a statistic that says there is a cyber-crimehappening every 39 minutes.

There are hackers who constantly trying to hack into the various devices that are being used by everyone today almost on a minute-to-minute basis such as laptops, PCs, mobile phones. They do this using the following methods:

1. **Malware:** Malware refers to malicious software. As the name suggests, it harms or exploits a device and/or network. This causes the devices to slow down, hampers the performance of the device, and gives the hackers access to the users' confidential data. Malware can be introduced in to the devices by means of frequent pop-up ads,or some website links that end up taking the user to websites that they didn'tvisit etc.
2. **Websites and Links: URL:** Phishing refers to the practice of sending fraudulent emails from reputed organizations that prompt the user to click onlinks to obtain their passwords or make them take urgent action that may require financial transactions. One of the ways of doing this is by slightly changing the domain names of the websites. Eg. In www.google.com, googleis the domain name. So, the hackers would make some minute changes to domain names, like replacing a period with a hyphen, or by adding special characters, eg. They may send an email with a link to m@injob instead of mainjob, where the new links are actually malicious links, and the user wouldn't really notice it and click on those links anyway. Phishing refers to sending out emails with malicious attachments to trick the user into opening or downloading them and exposing their data.
3. **Unsecure WiFi connections**: Users often go to local coffee shops and airports and connect their laptops to free WiFi available at these locations in order to work or to browse. These free networks may not be secure; they maypotentially have malware.
4. **Untrustworthy employees**: Although this isn't applicable to all scenarios, there have been proven instances where a few untrustworthy employees of the organizations, who either may be nursing personal grudges against the management, fellow employees, those who may have some vested interests may indulge in leaking company data and create liabilities for the company
5. **Tailgating** – The disgruntled employees may even follow other employees intodesignated areas that may have confidential information

It is important to understand that in certain cases, especially when the hackers are trying to hack into the devices and servers of companies, they will gain information about the victim before they lay out the trap.

One of the best ways to gain information about the users is via social media. This isone of the most vulnerable points the users have and the hackers exploit to the hilt. The users' passwords are often their pet names or mother's names. These kinds of pieces of information can easily be available on social media, that the hackers use tohack into their social media as well as their devices. Easy passwords are also the easiest gateways to your information.

Many a times misplaced USB drives have been the prime reason for loss ofconfidential information. These USB drives falling in to wrong hands and unscrupulouselements is surely a recipe to disaster. This may most probably result in the accessedinformation being used against them.

Giving confidential information to a stranger, wittingly or unwittingly puts one at riskof loss of privacy and security.

The consequences of these crimes are far-reaching. Here are a few of them:

1. Data leaking of companies' data gives hackers access to the bank account information of the company, leading to money theft. These kinds of transferscan happen in a matter of seconds and can often be difficult to trace or be blocked
2. Hackers can get access to confidential information about the company, its policies, trade secrets, and the information of its clients. A company can lose its privacy and secrecy over its valuable information. Furthermore, the data leaking can expose the information of its clients and their confidential information to the hackers, causing lawsuits.
3. The above can cause serious damage to the reputation of the organizations. Reputation takes years and, in some cases, even decades to build, and all thiscan be reduced to smithereens in a matter of seconds, due to the leakage of important and confidential information [3]
4. This would result in a loss of customers, and by extension, the business and trade
5. Data leaking can also be that of the personal data of the employees. Their pictures can be morphed, their personal information such as name, address, phone number etc. can end up at the hands of the wrong people, potentially in the dark places of the web, endangering their safety and their lives.
6. The leaking of the credit and banking information of the employees can causeloss of money and funds, their social security information data leakage can beused to commit tax frauds, identity theft, and can potentially land them in legaltrouble

Being vigilant, having an eye for details, and knowing how to spot phishing emails and social engineering, can help you avoid being hacked and getting your data leakedor stolen.

Here are a few ways of exercising caution to prevent oneself from falling for cyber- attacks and exposing data:

1. Review the links in the emails carefully. Check for spelling errors and/or extracharacters added. One good practice is searching for the actual domain on browsers like Google or Bing.
2. Ask the café owners for the exact Wi-Fi name. Don't access financial or work-related information on public Wi-Fi. If one must access that information, use VPN to create a safe internet connection. Also update the device settings not to connect to nearby Wi-Fi sources which may be public.
3. Always use https for links. HTTP stands for Hyper Text Transfer Protocol whileHTTPS stands for Hyper Text Transfer Protocol Secure. As the name suggests,HTTPS is more secure than HTTP, for it conceals any information one types onit, like passwords, credit card information etc.
4. Share less information publicly, especially on social media. Try not to share alot of information about yourself, your family, your school etc.
5. Encrypt all confidential files, whether it's an organization's file or a personal file.
6. Ensure that all devices, organization-related or otherwise have anti-virus software.
7. Documents that contain sensitive information, but need to be discarded, destroyed or trashed, they should be disposed of properly. There are shredders which shred documents into extremely small pieces which makes it difficult toreconstruct them.
8. Always use strict privacy and security settings.
9. Keep in mind, suspicious emails may start with very non-specific greetings, like "Hello", rather name "Hello <your name>" if they're intended to gain access to your confidential data.
10. Phishing emails and social engineering often entail sending out emails that create a sense of urgency in the users. They will urge the users to take immediate action. Things like last minute changes or personal favors, payroll information, bank information, unexpected or urgent requests, are demandedin such emails. Always lookout for these things and take precautions on spotting one.
11. Always check the email address and verify the requests with the sender withother means, such as legitimate phone numbers, or preferably, face to face.
12. Check the domain names of the emails. Hackers will never use proper domainnames, like the domain name of one's company, or that of the company that they're representing in the email. They'll use generic domain names like Gmail,yahoo etc.
13. Check to see if emails have copied or forged logos.
14. Also check the names of the attachments in the files. Check if they have non-standard names or formats.
15. Whenever you're in doubt, call your IT department.

No discourse on securing your information and devices will be complete, without emphasizing and undermining the need for a strong password. The concept of strongpasswords goes a long way in shielding one's devices from hackers. Here are a few ways in which one can create strong passwords:

1. Strong passwords have around 16-20 characters
2. Passwords should be a combination of alphabets – both upper-lower caseletters and lower-case letters, numbers, and special characters.
3. Incorporate silly phrases in your passwords, that only you can think off.
4. Never reuse passwords for different accounts or places.
5. Use an organization approved password manager to create and storepasswords
6. Don't reveal your passwords to anyone, not even the Technical Support team.
7. Refrain from using simple dictionary words, people's names, birthdays etc.
8. If possible, create a passphrase, not a password. E.g. 9&inmygreAtwoRLdS

Other forms of security include Internet of Things (IoT) Security, which means security for IoT devices. While IoT provides a lot of advantages and helps to achieveincreased productivity, it is susceptible to threat due to its wireless nature.

These devices are secured as per classification of the connected devices, auto- segmentation to control network activities, and using IPS as a virtual patch to preventexploits against vulnerable IoT devices. Sometimes, the firmware of the device is alsoaugmented with small agents to prevent exploits and runtime attacks.[4]

For end-point security, which is about securing the end-user devices, such as desktops and laptops, the zero-trust security model is the best way to achieve it, which prescribes creating micro-segments around data wherever it may be. With endpoint security, companies can secure desktops and laptops with data and networksecurity controls, advanced threat prevention such as anti-phishing and anti- ransomware, and technologies that provide forensics such as endpoint detection andresponse (EDR) solutions.[4]

Cloud security can be achieved through by third-party solutions, while network security can be achieved via well designed Firewall.

Here, I would also like to recall a project in cybersecurity, which I undertook as partof my curriculum during my Masters. This was about a mobile phone app, which wouldbe connected to a smartwatch as well as wireless earphones that can store data by means of an IMU sensor. The main objective of the project was to ensure that the theft of the earpiece or the watch could be detected before the weakening of Bluetooth signal, that is before the breaking of the connection between the devices. The initial authentication was designed like this: The mobile phone application wouldask for an OTP which would only be heard on the earpiece. And then the password would have to be typed from the smartwatch. Only then the app would be started and would start storing the data safely from the watch and the earpiece. The analysison that data as well as the algorithms designed in the project used were carried outto ascertain whether all three pieces remained with the same person or not. Many such projects are being carried out to ensure and maintain privacy and security.

One must ever keep in mind and always be cautious that it is possible to fall victim to scams and malicious attacks by hackers at all times when we are using devices such as our smart phone. However, by taking necessary precautions such as exercising caution and always checking emails before opening the attachments and links, could help prevent one from being a victim to such attacks. This is the only wayone can shield oneself, family and the associated organization from cyber-attacks.

REFERENCES

[1] https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/

[2] https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social- engineering

[3] https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach

[4] https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/

Citation: Riyya Hari Iyer, Cybersecurity and Its Associated Threats, International Journal of Cyber Security (IJCS), 2(1), 2024, 28-33.

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCS/VOLUME_2_ISSUE_1/IJCS_02_01_003.pdf

Abstract Link:
https://iaeme.com/Home/article_id/IJCS_02_01_003

✉ **editor@iaeme.com**