International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 2, Mar-Apr-2020, ISSN (Online): 2395-566X

Cyber-Security for Digital Well-Being

Assistant Professor Kumkum Saxena, Manav Vikas Bahl (S.E, I.T, Student)
Department of Information Technology,
Thadomal Shahani Engineering College, Bandra, Maharashtra, India.
kumkum@saxena.ind.in, manav.vbahl@gmail.com

***Abstract* – With the advancement in technology, there has been an increasing urgency and need for security with the rising practices taking place unethically. The technology works as a boon only when users are up-to-date with the updates and the people who lack this quality are often a target to various attacks in the cyber world leading to misuse of data and financial scams. Cyber-security takes the limelight in such cases to avoid these unfortunate events which lead to damage over individuals, business and the world at large. This review paper addresses the various cyber-attacks that exist and go unnoticed to a daily user. It also throws light over the procedures of execution of such malpractices and conveys precautionary and effective ways to avoid these cyber attacks.**

***Keywords* – Cybersecurity, Cyberthreat, Cyberdefense, Cyberattack, Spoofing etc.**

I. INTRODUCTION

The data that we send, receive and back up has a digital existence and is linked to the internet through various means. With the ability to store data with enormous space over virtual drives, cloud storage, the security of data takes the highest priority. Various developments on the internet such as e-wallets, internet banking and promotions via advertisements over the web have attracted attackers to perform unethical means to steal the data, credentials and misuse them. As a result, attacks like phishing, malware distribution, a man in the middle, mal advertising, password attacks and rouge software attacks are used to cause harm over unaware users. These attacks make it essential to create awareness about practices which harm internet safety and also to throw light on how to avoid such attacks. Cyber-security in the field of Information Technology protects as a method to prevent unauthorized breach into data without the users' permission.

It also helps to prevent intruders in accessing information which could be confidential and when exposed, could harm an individual.

II. MALWARE ATTACK

Malware, also known as Malicious Software is the process of using software or program to conduct unethical activities without the user's consent. With technological advancement, various spoof applications are created and distributed over the internet which allows permissions and rights to access data. Malicious software installs themselves into devices without the user's permission and creates multiple folders to prevent any antivirus software to recognize its existence.

1. **Malware attacks include:**

- Advertising software (Adware) that bombs the application with unwanted advertisements.
- Spying software (Spyware) which makes a note of the activities taken place on the system and
- A virus which prevents the machine from performing any functionality resulting in corrupting the software.

The most dangerous attack by Malware is Trojan which is installed into the system by pretending to be something useful and once accepted, transfers financial data and is used to inject a virus into the devices.
Malware attacks can be recognized when the device does not perform at the ideal pace, various substitute toolbars, plug-ins and search engines take place without prior setting and pop-ups of bogus ads frequently occur while using the internet.

III. PHISHING ATTACK

Phishing is a technique which attackers use to mask themselves as a trustworthy entity to gain access to private information like login, bank account details. Individuals are tricked into clicking on unauthorized links of fake websites which are structured to appear like authentic websites which install various malware into the device.
The most effective scam that includes phishing is:

1. **Email phishing**

Email phishing functions on sending emails in bulk to various individuals in which the attacker bluffs about having information and implies to cause damage until a certain denomination in currency is transferred. Some mails also create a sense of emergency by claiming that the login credentials will be expiring and force the individual to update the data, which is linked to a spoof

website to gain those details.
These malicious phishing activities can be recognized by checking the website URL for https:// (Hypertext Transfer Protocol Secure) functionality which authenticates the website and to activate Two-Step Verification, also known as Multi-factor authentication (MFA) on the passwords to avoid uninvited attackers from accessing personal and professional information.

IV. PASSWORD ATTACKS

Password is often known as verification criteria to obtain access to encrypted information, accounts and websites. When a user enters a username and password, the details are saved into the database of the website where the username is stored as it is presented but on the other hand, the passwords are hashed using various encryption languages to avoid theft.
Since usernames are commonly present all over the internet, password serves as an effective wall to keep the intruders away from personal data. As a result, having a secure and unique password becomes the highest priority.
Various ways to obtain access through password attacks are:

1. Brute force

The attacker on the backhand of the machine uses various automated software which carries out permutation and combination of words to predict passwords. This method serves effectively to common/weak passwords.

2. Key-Logger attack

A malicious email is first sent with a link to the victim with urgency to address it. Once clicked it allows the intruder to record activity, including everything typed on that device as a result, gaining access to passwords. This is the most dangerous method which leads to losing personal data.
Password attacks cannot be recognized and as a precaution, one must include one capital, one numeric and special character into their passwords and change their passwords regularly to avoid attacks.

V. MAL ADVERTISING

Mal Advertising is known as malicious advertising refers to the usage of ad space to spread malware to different systems. Every website witnesses a wide spread of interactions and comes across large numbers of ads submitted for promotions.
Due to entries coming in a bunk, the quality for the deep check for authenticity is compromised. This makes it easier for the attackers to succeed with their motive. The attackers use legitimate advertisements and replace the backhand code of such advertisements to avoid getting detected by the software.
This method is generally used to install malware and also to conduct Trojan attacks.
Since these attacks appear legitimate, it is suggested to keep the software of the browsers up-to-date, avoid pop-ups from websites and to set the settings which ask for permission to use the j-frame, flash plug-ins.

VI. ROGUE SOFTWARE ATTACKS

Rogue software stands out as a security threat as it notices the user with bogus pop-ups about a security breach in the machine and forces them to pay/install software to get rid of these viruses. The pretend software installs malware and in the process transfers personal information and details like passwords, financial details.
Downloading freeware software from the internet often comes along with a threat of malware. As a result, this scenario can be avoided by using built-in antivirus software by the system.

VII. MAN IN THE MIDDLE ATTACK

Man in the middle attack functions when an unauthorized attacker places his system between the regular data flow of the client and the server. As a result of this, the attacker usually eavesdrops or impersonates as an inbuilt function and steals data. This attack is usually targeted over E-commerce companies where the base of the company relies upon the internet.
The new connection implemented with the attacker in the middle is always displayed secure but various caches and data packets from the browser come into their hands resulting in unethical hacking and spoofing of identity.
Implementation of 'Man in the middle' is easy as users often connect their devices to open wifi networks which easily help the attacker to put themselves in the middle of the data flow.

VIII. DENIAL OF SERVICE ATTACK

Denial of service (DoS) attack is a cyber-attack which intends to make a particular service unavailable for the users by sending multiple requests by I.P addresses. In DoS attack, the attacker floods the server with numerous entries from the same I.P address which occupies the entire capacity of the server, making it unavailable or extremely slow to respond.
The attack is often ineffective as the security on the backhand of the server detects the abnormality and hence blocks the I.P making an unethical entry.
As a result, Distributed denial of service (DDoS) attack is preferable over DoS attack as every registered entry on the server holds a unique address. This attack makes it impossible to detect false entries blocking the server.
The motive of these attacks is to disrupt the normal functioning and to overload the capacity of the server. DDoS attacks are initiated to affect clients from accessing their financial-based websites and also to block competitors in business.

IX. DRIVE-BY ATTACK

A drive-by attack targets the users through their internet browsers and installs malicious software in their devices. These attacks are also known as drive-by download attacks as they are initiated on their own as a user visits an insecure webpage or redirected to a fake web page.
The drive-by attack takes advantage of the browser and uses it as a medium to infect the device with viruses which harm the user. The most common method is to replace the HTTP and PHP files with malicious scripts which cause unnoticed downloads or redirects the user to unauthentic websites. Using an ad blocker and visiting only authentic sites.

X. CONCLUSION

In the most competitive market, advancing with new technology daily, the implementation of these destructive attacks get better day by day and to safely work in this environment comes across as a challenge. As a result, to safeguard ourselves we must:

1. Ensure to download applications, software only from verified in-built stores as their authenticity is stated.
2. Prevent clicking on pop up advertisements which show on the sidebar of browsers because they are linked to spoof web pages which might gain access to the user's device information without their permission.
3. Never put in passwords, OTP or any confidential data over sites that do not have encryption because those websites could be unauthorized.
4. Avoid paying attention to bogus, spam emails pretending to have personal information about the user as the attackers usually bluff and the unaware users fall into such traps
5. Check the URL for a secure connection i.e. https:// when dealing with financial, data exchange.
6. Keep a strong password with one capital, one number and a special character and if any suspicious activity is detected, the password must be changed immediately.
7. Use an ad blocker as it keeps the users away from being redirected to unauthorized websites.
8. Switch to two-factor authentication over general login and password in ensure high-level security.
9. Use antivirus which is provided by the system as other freeware software often infect the computer with virus, additional junk and end up coping cache which is used to keep an eye over browsing history.
10. Delete unwanted applications and keep all the software up to date as they contain security patches which make it impossible for the attacker to gain any access.
11. Avoid logging in multiple devices and seize the use of public, open wifi networks.

This is how we can transform the technologically advanced environment and ensure digital well-being.

REFERENCES

[1]. Nate Lord on "What is Cyber Security?" https://digitalguardian.com/blog/what-cyber-security
[2]. Search Security on "Malware" https://digitalguardian.com/blog/what-cyber-security
[3]. Imperva on "What is a phishing attack?"https://www.imperva.com/learn/application-security/phishing-attack- scam/
[4]. One login on "6 types of password attacks" https://www.onelogin.com/learn/6-types-password-attacks
[5]. Authanvil on "3 types of password attack and how to avoid them." https://authanvil.com/blog/3-types-of-password-security-attacks-and- how-to-avoid-them
[6]. Ben Canner on "The top 7 password attack methods" https://solutionsreview.com/identity-management/the-top-7-password- attack-methods-and-how-to-prevent-them/
[7]. Bekah Rhea on "What is mal advertising and how can you avoid it" https://salesintel.io/blog/what-is-maladvertising-and-how-can-you- avoid-it/
[8]. Wikipedia on "Rogue software attack" https://en.wikipedia.org/wiki/Rogue_security_software
[9]. Norton on "What is man-in-the-middle attack" https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle- attack.html
[10]. Veracode on "MITM attack" https://www.veracode.com/security/man-middle-attack
[11]. Kaspersky IT Encyclopedia on "Drive-by attack" https://encyclopedia.kaspersky.com/glossary/drive-by-attack/
[12]. Cloudflare on " What is a DDoS attack?" https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-attack/