Cyber Safety Fears and Protection: An Overview

[1]Mayank R. Kothawade, [2]Sachin Lamkane, [3]Dr. Preeti Agarwal

[1,2]Assistant Professor, [3]Director
[1,2]VIIT, [3]G.H. Raisoni

ABSTRACT: **It appears that everything trusts on computers and the internet, now digital communication, entertainment, transportation, online shopping, medical and healthcare, and many more. How much of your daily life relies on computers? How much of your private information is kept on your own computer or on someone else's system? Cyber security comprises protection of that information by stopping, sensing, and responding to attacks. This paper gives the overview of some of the threats concerning to cyber security and measures to avoid these threats.**

KEYWORDS: **Cyber security, Defense, Firewall, IDS, Intrusion detection, Encryption, DOS, DDOS, IP, SMTP.**

INTRODUCTION:

Cyber-security comprises defense of information by stopping, detecting, and replying to attacks. Organized crime is rapid to take the benefit of the openings existing over internet, chiefly the development in e-commerce and online banking. Professional criminal groups target Individuals, small medium and large business networks to steal lots of private information to gain the income from the compromised data available to them.

While rapid technological developments have offered massive areas of new opportunity and potential bases of efficacy for all size organizations, such newer technologies carried extraordinary fears with them. Cyber-security defined as the defense of systems, networks and data in cyber-space is a grave concern for all organizations. Cyber security will become more important as proliferation of devices as well as the internet of things (IOT) developed to connect to the internet[1].

OBJECTIVES

1. To take the overview of different cyber threats.
2. To understand the defense apparatus to handle diverse cybersecurity threats.

CYBER SECURITY THREATS

In this paper researchers have discussed common cyber security threats including; spam, scams, malware or malicious software, identity theft, phishing, pharming, man-in-the-middle attack, (MITM), . Man-In-The-Browser attack, replay attack, denial of service attacks (DoS, DDoS). Cyber threats covered in this paper are classified as threats to consumer and business.

Threats to Consumers

- Phishing: bogus emails requesting for security and personal information or details
- Webcam manager: where criminals takeover your webcam
- File hijacking: in such crimes criminals hijack files and hold them to ransom
- Key logging: where criminals capture the keystrokes you type on your keyboard
- Managing Screenshot : it automatically allows criminals to take screenshots of users computer screen
- Ad clicker: allows a criminal to direct a victim's computer to click a specific link[2]

Threats to Business

- Hacking
- Distributed Denial of Service (DDOS) attacks

These cyber threats and risks left serious impact compare to other crimes. Among these dangers are viruses erasing your entire system, someone cracking your system and modifying files, someone using your computer to attack others, or someone stealing your plastic card information (credit/debit card) and doing illegal purchases. Unfortunately, there's no 100% guarantee that even with the finest safety measures some of these things would not happen to users, but there are steps you can take to minimize the chances.

Defense: -

The first step in protecting yourself is to recognize the risks and be aware with few terminologies associated with them.

- **Hacker, attacker, or intruder**
- **Malicious code**, **Vulnerability**
- **Curtail the access of your information for other people:** You may be able to easily identify people who could legitimately or not getting *physical* access to your computer including your family members, roommates, colleague, cleaning crew members, and may be others. Recognizing the individuals who could getting *remotely* access your computer becomes much more difficult. As long as users have a computer and users are connecting it to a network, they are vulnerable to someone or

something else accessing or corrupting personal or confidential information; though, users can cultivate practices that make it more difficult.

- **Lock your computer when you are away from it.**
- **Disconnect your personal or office computers when you are not using internet.**
- **Evaluate your security settings.**
- **Back up all of your data.**

Here are 5 key countermeasures that can be used to drive cyber-security activities in control systems environments.

1. Security policies
2. Blocking access to resources and other services
3. Detecting malicious activity
4. Mitigating possible attacks
5. Fixing core problems

1. **SPAM:** Spam is the common term for electronic 'junk mail' unsolicited messages/mails sent to a person's e-mail address. Spam floods the internet with countless replicas of the similar message, in an attempt to force the message on people those are not interested to receive it. There are two main kinds of spam with different impacts on the users of internet. Cancellable Usenet spam is a single message sent to twenty or more Usenet newsgroups. Email spam targets individual users with straight mail messages. Lists of e-mail spam are frequently shaped by scanning Usenet postings, stealing internet mailing lists, or searching the web for addresses.[3]

Zombies: Server and Clients

Figure 1: Source: http://es.masternewmedia.org

Defense:-

- Use Spam filter software
- Don't disclose your email id on unknown sites
- Proper protection of your Computer
- Education and Training of a user
- Detect and block spam mails from reaching the user's mailbox

2. ONLINE FRAUDS OR SCAMS: These scams often arrived through unwanted emails. Most of them are related to the well-recognized Nigerian scams or Loto scams and use similar tactics in one form or another. Apart from these there are many types of such scams as given below;

Figure 2: Source:
a. http://motella.blogspot.in
b. http://www.theregister.co.uk

Online frauds can include; [4, 5]

Account takeover	Bank card and cheque fraud
Advance fee frauds	Business directory fraud
Charity donation fraud	Business opportunity fraud
Click fraud	Clairvoyant or psychic scams
Domain name scams	Government agency scams
Fraud recovery fraud	Vehicle matching scams
Health scams	West African or 419 scam
Holiday fraud	Work from home scams
Identity fraud	Online shopping fraud
Inheritance fraud	Internet dialler scam
Internet auction fraud	Land banking scams
Loan scams	Mass marketing fraud
Lottery scams	Pay-in-Advance Credit Offers
Money muling	Plastic card fraud
Rental fraud	Romance scams
Sweepstakes Scams	Mystery Shopper Scams
Tech Support Scams	Bogus Apartment Rentals
Weight Loss Claims	The "Nigerian" Email Scam
Investment Schemes	Online Dating Scams
Money Transfer Scams	Debt Relief Scams

Defense:

- Do not send money or pay any fee via money transfer to claim prizes.
- Never give personal details to anyone that you have not checked out first from an independent source. Searches on internet sometime providing extra information.
- User Education in the form of Portal, Email newsletters, Customer meet etc.

3. Malware or Malicious Software: In computation of cyber-security, malevolent software is an umbrella term encompassing various types of malware programs including computer viruses, adware, trojans, spyware, keyloggers, ransomware and many other harmful types of software targeted to harming the user and their systems by humiliating, abolishing, or denying access to their files and data, or theft and spying their sensitive information, generally without the user's knowledge or permission. Malware types can be categorized as: worms, viruses,

backdoors, and trojan to infect and spread themselves to create more havoc. Adware and spyware embed themselves to view what the user does and act upon that data. Root kits seek to give full access of your machine to the attacker to do what they want.[6] Software intended to harm computers is malicious software. Malicious software is also referred to as malware.

E.g.: Virus, Worms, Trojan horses, Logic bombs, Backdoors, Spyware, Key-Loggers: Free Key-Logger, Perfect Key-Logger

Figure 3: Malware

Source: a. http://uucyc-xpuctoc.blogspot.in

b. http://www.anvisoft.com/

Defense:

- Install & update good Anti-Virus and Anti Spyware software regularly. (Recommended web & e-mail content filter software)
- Use of Virtual Keypad/Keyboard on the server to prevent Key-Logging
- Awareness & Education in the form of emails, newsletters, SMS, Advertisements etc.
- Do not download software from untrusted and unknown web sites or other sources like torrent and other peer to peer networks
- Do not open any .exe (executable) file formed by somebody else you do unknown
- Assure that software patches are installed on regular basis and up to date
- For backdoor check source code by an independent team
- Anti-spyware software to detect and block spyware

4. Identity Theft: Identity fraud/identity theft is the term used to indicate types of crime in which someone wrongfully obtains and uses others personal data by a specific method that involves fraud or deception, typically for economic gain. Such webpages are planned to describe the need to take precautions to protect yourself from identity theft. Dissimilar to your retina scan, finger or palm impressions, which are distinctive to each individual and cannot be given to someone else for their use, your personal data - especially your Social Security number, your bank account, credit card number, SIM card number, and other valuable identifying data can be used, if they catch by incorrect person, to personally profit at your expense.[7] Identity fraud can be described as the use of that stolen identity to commit some criminal act to get goods or services by deception. Fraudsters can use your identity details to: [8]

- Open bank accounts.
- Obtain credit cards, loans and state benefits.
- Online purchase using victims name.
- Access your existing accounts.
- Getting mobile phone contracts.
- Obtain genuine documents such as passports and driving licenses in your name.
- Theft of individual's identity details does not, on its own, constitute identity fraud.

Figure 5: Identity Theft

a. https://postalinspectors.uspis.gov

b. http://www.musicrowtech.com

c. http://moneytipcentral.com

Defense:

- Strong Passwords
- SSL
- Clear Screen / Desk Policy
- Good Anti Virus and Anti Spyware
- Awareness

5. Phishing: Phishing attacks/scams are generally fraudster email messages seems to be received from genuine enterprises (e.g., university, Internet service provider, and bank). Such messages typically take you to a spoofed website or else ask you to reveal private information (e.g. credit card details, bank details, other account updates etc.). Perpetrators further use personal information to attack targets. This is a type of phishing attempt is an email message uttering that users are receiving it due to fraudulent activity on their account and asking them to "click here" to verify their information.[9] Criminally fraudulent process of acquiring user's credentials.

Attack vectors:

- URL Obfuscation Attacks: Sending email for asking your username, password details related to banking sites.
- Cyber Squatting: Registration of such domains where users can't differentiate fake and original e.g. http://www.facebook.com[Original website], http://www.facebook1.com, [Fake web site] http://www.facebook.org,[Fake web site] http://www.facebook.in,[Fake web site]
- Cross Site Scripting(CSS): Executed by poor application coding

- Trojans: Named after Greek Story of Trojan horse. Backdoor entry. Most dangerous attack vector.

Figure 6: Phishing
Source: http://www.15minutenews.com

Defense:

- At client side: Anti Virus, Personal Firewall, Anti Spyware, AV, Personal FW, Anti Spyware and User Awareness.
- At server side: Firewall, Network and Host Intrusion Prevention, Secured Code, SSL certificate, Anti-Phishing Service, Two Factor Authentication and Transaction Monitoring

6. Pharming: Pharming is a type of online fraud very similar to phishing rely upon the similarly looking websites and stealing secret information. However, phishing must lure a user to website through the medium like a deceiving email or link, pharming redirects victims to the fake site though the victim has entered correct URL or web address. This is often applied to the websites of banks or e-commerce sites.[10] Variant of Phishing. Redirect User to Bogus Website. Executed by: Changing the hosts file on user's computer, DNS Poisoning.

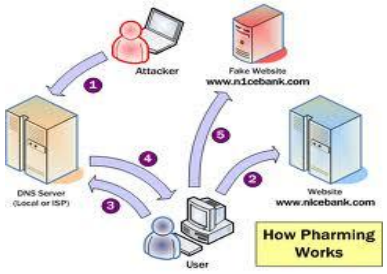

Figure 6: Pharming
Source: a. https://daybreaksdevotions.wordpress.com
b. http://www.massivealliance.com

Defense:

- Receive alert if similar sounding domain is registered (Domain & Brand Monitoring like Mark Monitor, RSA, VeriSign)
- Protection of DNS servers and client PCs.

7. Man-In-The-Middle attack (MITM):
Where a user gets between the sender and the receiver of the information and sniffs any information being sent. In some cases, users may be sending unencrypted data, it shows that the MITM get any unencrypted information. In other cases, a user may be in position to acquire information through attack, but have to decrypt the information earlier it can be read.[11] Old but dangerous attack. Active Eavesdropping, Communication between Client-Server is intercepted and customer is redirected to hacker's proxy server. MITM is accomplished through:

- DNS Cache Poisoning
- Browser Proxy Configuration intrusion

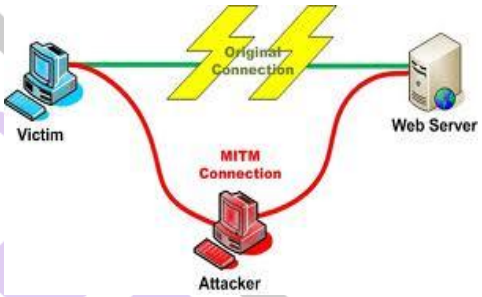

Fig 7: Source: http://www.thewindowsclub.com

Defense: (Best Multi Factor Authentication)

- Mutual Authentication (Client-Server)
- Transaction Monitoring

8. Man-In-The-Browser attack:
Variant of MITM. Trojan is used to infect Internet Browser and has the capability manipulate the transactions. (Ex: Silent banker). [12]

Figure 8:: Man-in-the-browser
Source :http://whythehack.blogspot.in

Defense:

- Virus scans can also detect, quarantine, and delete Trojan horses
- Transaction Verification
- Transaction Monitoring

9. Replay attack:

A replay attack is a form of attack in which a valid data transmission is maliciously or fraudulently repeated or delayed[13]. A replay attack is an attack where an authentication session is replayed by an attacker to fool a computer to allow access. It may be any way or re-transmission of a network data transmission however it is typically used to gain authentication in a falsified manner.

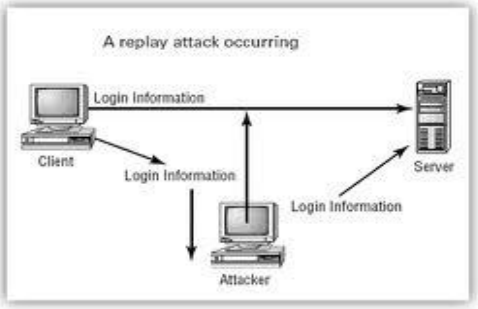

Figure 9 Source: http://infosecaffairs.blogspot.in

Defense:

Session Tokens (Password is valid only for that session)

10. Denial of Service Attacks (DoS, DDoS):

To block legitimate users from receiving services they are getting generally through servers

- Denial of service (DoS)-launched through a single computer
- Distributed Denial of service (DDoS)-launched through a group of computers

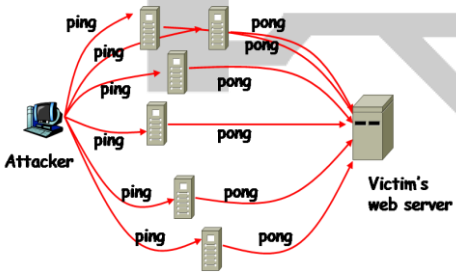

Figure 10. DoS/DDoS Attacks

Defense:

Encrypt IP headers. But an IP (Internet Protocol) packet with an encrypted IP header can't route to destination. Therefore, network gateways are needed.

Follow R.U.N.S.A.F.E. guidelines[14]:

- **R**efuse to run unknown programs;
- **U**pdate our computers regularly;
- **N**ullify unneeded risks;
- **S**afeguard our identity and password;
- **A**ssure sufficient resources for proper system care;
- **F**ace insecurity;
- **E**verybody needs to do their part

GLOBAL SECURITY MEASURES AND INITIATIVES:

Cybercrimes are not only varying in nature moreover they are committed from any part of the world irrespective to geographical locations. Under these circumstance agencies like INTEPOL are playing an important role towards minimizing the impact of such crimes. Main initiatives taken by INTERPOL are[15];

- Operational and investigative support
- Cyber intelligence and analysis
- Digital forensics
- Innovation and research
- Capacity building
- National Cyber Reviews.

CONCLUSION:

It is not possible to avoid all the threats or risk while using internet or online services, as such crimes are committed from any part of the world. However, the impact of such attacks may be lessen by taking proper care and defense mechanisms as discussed above. As attacks are varying in nature each attack can be handled in a different way. Training and education to common man is equally important along with government and corporate officials. Promotional activities through regulatory authority towards awareness of diversified attacks will be the effective solution.

REFERENCES:

[1] Cyber Security Management: What is Cyber security? http://www.bankpara.com/cyber-security management/

[2] Cybercrime,http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime

[3] What is spam?, http://spam.abuse.net/overview/whatisspam.shtml

[4] Common Online Scams, https://www.onguardonline.gov/articles/0002-ommon-online-scams

[5] Malicious Software - Definition & Threats, http://usa.kaspersky.com/internet-security-center/threats/malicious-software

[6] Online fraud, http://www.actionfraud.police.uk/fraud-az-online-fraud

[7] Identity Theft, https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

[8] Identity Fraud, http://www.actionfraud.police.uk/fraud_protection/identity_fraud

[9] Phishing Explained, https://kb.iu.edu/d/arsf

[10] Online fraud: pharming, http://us.norton.com/cybercrime-pharming

[11] Man-in-the-middle attack, http://www.computerhope.com/jargon/m/mitma.htm
[12] Man-in-the-browser attack, https://www.owasp.org/index.php/Man-in-the-browser_attack
[13] Session Replay Attack, http://infosecaffairs.blogspot.in/2015/07/session-replay-attack.html?m=1
[14] R.U.N.S.A.F.E., http://www.jmu.edu/computing/runsafe/
[15] Cybercrimes, http://www.interpol.int/Crime-areas/Cybercrime