Internet Threats and Prevention – A Brief Review

Sheenam Bhola
Assistant Professor
SBSSTC, Ferozepur

Sonamdeep Kaur
Assistant Professor
SBSSTC, Ferozepur

Gulshan Kumar
Assistant Professor
SBSSTC, Ferozep

ABSTRACT
Network security is a branch of computer technology whose objective is to protect the information and property from theft, corruption, or threats attack. Now a days, we are mostly dependent on internet for many things such as online shopping, bank transactions, internet surfing etc. However, internet is not fully secure as its users are threatened by many computer viruses, malicious threats and many more attacks. This paper summarize various computer threats and mechanisms used for protecting sensitive information over the internet.

Keywords
Internet Threats, security, prevention

1. INTRODUCTION
Continuallyas the innovation of the computer, the security of computer systems has turn out to be an progressively moresignificantpart of focal point for allassociations. The beginning point of the Internet and Web has supplementary anentireinnovativeaspect to security which we called an Internet Security. Before the use of internet the unauthorised access attact on the system data and misuse the conifidential details. The internet change the whole picture of computer. By using internet anyone can access the data any where in the world.The access of Dial-up releasethe computers upbeat to various threats that did not contain physical access to the computer system[3].

This paper discusses the Internet security distress and the risk of securityallied by the use of Internet which including various threats, risk related to the security and its prevention. all through,the users of internet have practised and they will persist to familiarityprofuseschemesufferers that have a straightcollision on their mainlyvital feature which is their important information and theirsecurity is highestimperative to the users. The exposed attackson the internet increased day by day and and this paper consider thesuggestedthe steps to grip the internet security issues to elucidate before its use [2].

2. THREATS
The internet threats are malicious software programs like spyware, adware, trojan horse, bots, viruses and worms, etc. which are set up on the systemdevoid of our information or we can say without any authorization. These type of programs can make use of the Web forwiden, conceal, update and transmit theft data back to criminals or hackers. This will be better understand by the example- a trojan used to download spyware and a worm is used to contaminate the system with a bot [1].The Technology has turn out to be an predictablecomponent of our lives. But the Internet proffer a accumulationquantity of helpful information and formulatemessage easier and faster than eternally, but it nearbya number of threats as wellbeside the approach. The computer system is a immensedevice to store upimperative information. In convinced cases, the information is extremelyvery importanttotrailing it will damage the system.The Computer system threats can draw closer from numerouscustomsmoreover from human or from natural calamity.illustration, assomebody is burglary your report information from a confidentialstore, this type of threat is well thought-out as a human threat. though, as the computer is drenched in profound rain, then this type is called as natural disaster threat.

Internet has turn out to be a typedevice for industry communication and information contribution. All the Contents of internet we can read, send, and receive bear a risk. The numeral of latent security danger has better than previous to at the similar time that reliance on information technology has fully fledged manufacture the require for a inclusive security program stillextravital.Web threats pretence a broad assortment of risks, with financial indemnity, identity theft, defeat of private information, theft of network property, damaged personal status, and corrosion of customerself-assurance in e-commerce and online banking.specialistdetermineinnovative security vulnerabilities approximatelyeach day[5].The recentlyexposedvulnerabilities might be due to defect in software or they might be due to software constructionfault. Hackers can make use of these vulnerabilities to achieve access to network resources. overseerhave touse up a set of point and forceimmediatelyhang aboutknowledgeableconcerning and trade with new-fangled vulnerabilities. frequently the effect is that they are not capable to obtain the instance to observe and edifyemployees. Enforcement of security strategymight be missing or rely on the honor structure. stoppage to protecttouching the solution threats to information and systemresources can effect in disaster [11].

The system threats aresomething that show the way to defeat or bribery of data and bodilyharm to the hardware andcommunications. significantly how to recognizeprotection threats which is the first step in defensive the systems. The internet threats possibly will be deliberate, unintentional and cause due to natural disasters[12].

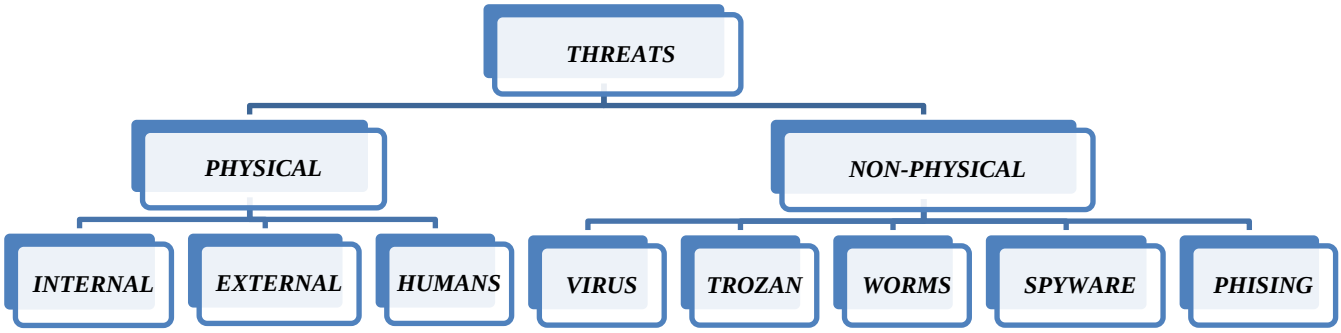

Figure 1: Category of Web Threats

2.1 PHYSICAL THREATS

Thelatentsource of an occurrence which causemay possiblyeffect in the loss and physical harm of the systems is known as physical threat.

There are three types of physical threat:

- **Internal threats**- these type of threats include fire, unbalanced power contribute, dampness in the rooms,accommodation the hardware etc.
- **External threats**- these threats include the floods, earthquakes etc.
- **Human threats**- these include theft, destruction of the communications and hardware, disturbance, unintentional or deliberate errors [4].

2.2 NON-PHYSICAL THREATS

The latent source of an occurrence which cause may cause:

- Loss or fraud of system data
- interrupttradeprocedure that rely on the systems
- Loss of responsive information
- illegitimateobserve of actions on thesystems

These types of threats are also known as the logical threats. The following list is the common types of non-physical threats :

Table 1: Summary of Internet threats and their Impact

THREATS	DEFINITION	RECENT ATTACKS	IMPACT
MALWARE	A software program which is clandestinely located on the computer system that perfom unpredicted and unauthorized attempts, that are malicious activities.	On 14th Oct 2014, Spike in Malware Attacks on Aging ATMs [13]	Loss of about USD $1 million
		On 8th Oct 2014, Malware Attacks Drain Russian ATMs [14]	Millions of Dollars
VIRUS	A program which can make copy of its own like real-life viruses and extend rapidly. they are premeditated to harm the computer system and put on show unforeseen messages and images. It also destroy the important files and slow down the system.	On 15 August 2012,The cyber attact on Saudi on Saudi Aramco by Shamoon Virus [15]	Infected 30,000 of its Windows-based machines
WORM	A self-reliant program which broaden copy of itself to other systems throughout network links, email regard, messages and work as malware. They can block you from accessing various web sites and also pilfer the licenses for various applications that we had installed on our computer system.	On 14th Feb 2013, Bizarre attack infects Linksys routers with self-replicating malware [16]	1000 devices have been hit by worm
TROZEN HORSE	It is a program which act upon a malicious act except cannot imitate itself. This type of program might turn up as a undamaging file and we can say an appliance with concealed malicious signs. During its execution, we might practice unnecessary system trouble and may every so often misplace information from the system.	On 25th Oct 2011, Japanese government hit by Chinese Trojan horse attack [17]	A cyber-attack mounted from a server in China apparently stole user ID codes and passwords of Lower House members and their secretaries who use the chamber's computer network. It gave the hackers access to e-mails and documents possessed by the chamber's 480

			lawmakers and other personnel for at least one month
SPAM	The message which is transmit by email and instant message that is not requested by us and intended to formulate funds for the sender.	In Jan. 2014,Fridge sends spam emails as attack hits smart gadgets [18]	100,000 devices used as part of the spam attack
PHISHING	the attempts which are made by our phones, emails, messages and fax for getting our private information by stealing our identity. mainly phishing stab appear like they are intended for a lawful intention, but in short they are in fact planned to be worn for illegal action.	In April 2013, an AP journalist journalist clicked on a spear phishing email disguised as a Twitter email.[19]	Erasing $136.5 billion of value
PHARMING	The action of capture lawful websites addresses for redirecting us to a fake website whick appear as original. The spoofed website clandestinely gather our private information when ever weenter it, and can be used for any numeral of illegal activities.	In March 2014, Criminals hack 300,000 home routers as part of mystery 'pharming' attack[20]	Compromised 300,000 consumer and small office routers
SPYWARE	Software which are installed on our system without our knowledge and observe, tracks and rumour our electronic actions to the spyware instigator. They are frequently installed on system throughout Trojans and from justifiable software which are prefer for downloading and installation.	On 9th Jan 2011, 'SPYWARE' INCIDENT SPOOKS JIHADI FORUM [21]	System compromised
ADWARE	A software which distribute advertisements like pop-ups and Web links for us without our permission. They are typically installed surreptitiously in the course of Trojans and through legitimate software which we prefer for downloading and installation. It can exhibit highly targeted advertisements based on the data composed by spyware which is previously on our system and track the Internet surfing.	Nov 2014,Web Attack:PUP/Adware/Fake Application Download[22]	Affected Windows
BOTS BOTNETS	They are very small programs which are located clandestinely on system throughout a Trojan. A botmaster might manage numerous bots from a innermost position and carry out phishing and perform a denial of service attack which carry down a website so it cannot be accessed. They are normally used to deal out spam and phishing attacks.	On 9th Dec 2009, Amazon EC2 cloud service hit by botnet, outage [23]	Infected client computers after hackers were able to compromise a site on EC2 and use it as their own C&C (command and control) operation.
RANSOMWARE	The Software which encrypts the files for the intention of extortion. Files are held payment awaiting wounded pay money for a decryption key by distribution payment throughout a third-party	On 28th Jan 2015, One million rooms for Marriott Hotels, book earlier, Ransomware on the rise, Hot Hotels doing well [24]	Ransomware works by infecting your hard drive, freezing your computer and demanding a ransom.

3. PREVENTIVE MEASURES

Below are some Internet security tips to keep your computer and your family safe from web threats:

Avoiding Malware

Ensure that your Internet security software is restructuredrepeatedly and routinely, but don't take it for grantedthat it will protect you from attacks, and don't be dependententirely on antivirus software. Numerous threats requiremultifacetedshield like a full-blown security group.The risks from "zero-day" attacks could be eliminated by keeping

updated. Be alert that PDF's, image files and Office documents sometimes obscurenasty surprises and be apprehensive of program

records and Web links from any unexpected and unauthorized source. Also observe for anyforged anti-malware packages that identify the invented spyware and viruses [6].

Anti-Social Networks

Avoid compressed URLs like bit.ly, tr.im and tinyURL.comthat are very generally used to disguise nasty Web sites with different links to fake login window or to malware. Pleasure very undersized URLs with doubt. You can put an alternative on TinyURL's page in your own web browser that does the same thing. "Web 2.0" sites are generally fun based sites but are not secure as they focus to worm attacks like spam and denial of service attacks. Be cautious while postingresponsivedelicate information on social network sites like Facebook and LinkedIn as such

social websites are getting worse as you can't even imagine what damage the bad guys can do with your private data. So better to Take a birthday, your home address and your identity from these social networking sites [7].

Maintaining a Healthy System
Make use of Windows bring up to date and related mechanisms for regular updating, wheneverpromising. In short, keep your applications and system reorganized and updated.a Lots of existing malware reaches to teh sites via Office documents, PDFs and so on as there are enumorous number of malicious sites. So, Office up-to-date, Adobe Reader and system updates are needed to keep the different applications and system safe [9]. For day-to-day work and play puposes avoid using an administrative account so that if an attacker or malware access your system then it will restrict the amount of damage as the profile doesnot have any administrative privileges.

Protecting Your Passwords
Frequently change your passwords and also try to use different passwords for your different accounts so that unauthorized user can never guess and hack it anyways. If any of your password leaked out then having different passwords for different accounts will lead the attacker can't access to everything you owns.Always try to use very strong passwords which make use of combination of uppercase and lowercase characters,special characters and numbers [10]. Avoid using easy guessable passwords and don't make silly mistakes like writing down passwords where they can be found easily.

(Don't Be) Burned on a Wire
Don't connect to Web sites that engagewith the transfer of sensitive information, such as online banking and create a specific user profile without administrator rights for surfing from public hotspots. Use HTTPSwhile accessing Websites. Wireless networks areinherently less protected [8]. Avoid sharing of files and weak passwords for Internet usage.

Backups Not Crackups
Keep your private and necessary information "off-site" as the professional system administrators do. Always keep your laptops along with you so that to keep backing up as if anyone stole your data then you won't have loose all the important information.Try using system passwords so that unauthorized user can't access your systems [7].

4. CONCLUSION

To develop policies and structures to bump into such threats is a big challenge of Internet security. As the US' Iowa state develop the laboratories in order to simulate the investigation process of Internet attacks so they could work the same way. The usage of Internet facilities are becoming more and more familiar and should be described to the internet users that how these are to be used and protect their information from disclosure.

There are in short the following security issues to be taken into concern:

- Security software should be keep up-to-date and working always. Especially when you use a laptop in cafes airports and other locations as they are unprotected networks.
- Make use of Web reputation which is the latest technology,which can determine the reliability and security of a Website before you visit it. Use this technology collectively with contented scanning technologies and active URL filtering.
- Install safety patches and use the most up-to-date Web browser version whenever available. Make use a no-script plug-in web browser.
- Verify your Internet Service Provider to check what kind of fortification is presented by their network.
- Permit the "Automatic Update" feature while using Microsoft Windows operating system and pertainlatest updates as soon as they are obtainable.
- Install, renew, and sustain firewalls and intrusion revealing software that offer spyware/ malware protection.
- Be careful of Web pages or web links that involveinstallation of software. Try to examine all programs downloaded from the Internet with an advancedsafety measures solution.
- Always examine the End User License Agreement and terminate the installation method if any other "programs" are going to be installed in addition to the desired program.
- Avoid giving the personal information to unwantedrequirements for the information.

Also when you accept connections ensure that people are who they say they are, and whether or not you really want them as a connection. At the end make sure that you are using a protected connection for your safekeeping.

5. REFERENCES

[1] The basic of Web Threats, http://la.trendmicro.com/media/br/the-basic-of-web-threats-brochure-en.pdf

[2] Anthony Bisong and Syed (Shawon) M. Rahman , AN OVERVIEW OF THE SECURITY CONCERNS IN ENTERPRISE CLOUD COMPUTING, http://airccse.org/journal/nsa/0111jnsa03.pdf

[3] RandyBrown, WEB SECURITY ISSUES: HOW HAS RESEARCH ADDRESSED THE GROWING NUMBER OF THREATS? http://www.swdsi.org/swdsi08/paper/SWDSI%20Proceedings%20Paper%20S301.pdf

[4] Potential security threats to your computer system, http://www.guru99.com/potential-security-threats-to-your-computer-systems.html

[5] David Harley BA CISSP FBCS CITP , Staying Safe on the Internethttp://www.eset.com/us/resources/white-papers/StaySafeOnTheInternet.pdf

[6] Saeed S. Basamh, Hani A. Qudaih, Jamaludin Bin Ibrahim, An Overview on Cyber Security Awareness in Muslim Countries, http://esjournals.org/journaloftechnology/archive/vol4no1/vol4no1_4.pdf

[7] Trends for 2014 The Challenge of Internet Privacy, http://www.welivesecurity.com/wp-content/uploads/2013/12/Trends-for-2014.pdf

[8] EMERGING CYBER THREATS REPORT 2014, https://www.gtisc.gatech.edu/pdf/Threats_Report_2014.pdf

[9] Mark Johnson, Overview of Cyber Security & Risk, http://www.int-comp.org/attachments/Overview-Cyber-Security-Risk.pdf

[10] Dennis Rand, CSIS Security Research and Intelligence, http://www.csis.dk/downloads/LinkedIn.pdf

[11] Top 10 Internet Threats, http://www.norman.com/home_and_small_office/security_center/internet_security_tips/internet_security_tips_top_10_internet_threats

[12] Lujo Bauer, Alessandro Acquisti, Nicolas Christin, Lorrie Cranor, Anupam Datta, Efforts to promote online privacy via research and education at Carnegie Mellon, http://p2.zdassets.com/hc/theme_assets/512007/20004350 0/CMU_Proposal_Updated.pdf

[13] http://krebsonsecurity.com/2014/10/spike-in-malware-attacks-on-aging-atms/

[14] http://www.bankinfosecurity.com/russian-malware-attacks-drain-atms-a-7412/op-1

[15] https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272

[16] http://arstechnica.com/security/2014/02/bizarre-attack-infects-linksys-routers-with-self-replicating-malware/

[17] http://ajw.asahi.com/article/behind_news/social_affairs/AJ2011102515710

[18] http://www.bbc.com/news/technology-25780908

[19] http://blog.returnpath.com/blog/tori-funkhouser/top-7-phishing-scams-of-2013

[20] http://www.techworld.com/news/security/criminals-hack-300000-home-routers-as-part-of-mystery-pharming-attack-3505049/

[21] http://www.wired.com/2011/09/jihadi-spyware/

[22] http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=27222

[23] http://www.cnet.com/news/amazon-ec2-cloud-service-hit-by-botnet-outage/

[24] http://www.irishtimes.com/business/transport-and-tourism/one-million-rooms-for-marriott-hotels-book-earlier-ransomware-on-the-rise-hot-hotels-doing-well-1.208246.