# CHAPTER 1

# INTRODUCTION

Cyber Security is indeed an issue of Global Concern in India and all across the Globe. Protecting data and thwarting Cyber Attacks now have ascended alongside dealing with natural catastrophes as the most pressing threats demanding the world's full attention. Data fraud/theft and large-scale Cyber Attacks were each identified among the top five global threats in the latest edition of the World Economic Forum's Global Risks Report. With the increasing proliferation of information and communication technologies (ICTs) and the growing opportunity for real-time borderless exchange, cyber security is a complex transnational issue that requires global cooperation for ensuring a safe Internet. According to a 2011 Norton study, threats to cyberspace have increased dramatically in the past year afflicting 431 million adult victims globally – or 14 adults victims every second, one million cybercrime victims every day. Cybercrime has now become a business which exceeds a trillion dollars a year in online fraud, identity theft, and lost intellectual property, affecting millions of people around the world, as well as countless businesses and the Governments of every nation.

The main aim is to establish a professional understanding and thereby carrying out skill development initiatives, impart knowledge about digital space, develop cyber defence skills and expertise, which in-turn will protect citizens, businesses, critical infrastructures of the state, and e-governance services by establishing a collaborative platform for cyber security to prevent, combat, investigate and mitigate Cyber Crimes in a proactive manner, which in-turn will provide a secure cyber space to the society.

To address the issues and challenges around cyber security and cybercrime, the United Nations Economic and Social Council (ECOSOC) held a Special Event on "Cyber security and Development", organized jointly by the Department of Economic and Social Affairs (DESA) and the International Telecommunication Union (ITU) on 9 December in New York

Cyber security is a fundamental enabler of the digital economy, protecting organizational assets, contributing to business continuity, defending brand names, potentially providing a competitive advantage, and managing liabilities and risk as a whole. The failure of organizations to take sufficient action in protecting themselves and their customers from cyber threats has necessitated increasing regulatory involvement, with 2018 marked by the enforcement of the EU's General Data Protection Regulation (GDPR) and similar policies being crafted in the US and elsewhere; Smith anticipates a large-scale federal privacy law in the US to be enacted within the next year or two.

While new regulation and the development of national cyber security strategies can be helpful, there is not one or two isolated steps that alone can keep us safe. Cyber security requires a holistic approach, taking into account people, process, technology, organizational structures, business strategies and addressing the overall business ecosystem, which nowadays is built through the interfacing of many actors. These actors increasingly work across international borders, meaning the more substantive dialogue that international leaders have,

such as the conversations that took place in Davos, the more opportunity for meaningful collaborations that will drive toward real solutions. This dialogue must be ongoing and include both the public and private sectors, as well as academia and industry professional associations.

These challenges are only going to intensify in the coming years. The evolution of the cyber threat landscape cannot be ignored, especially with the rapid proliferation of new technologies and the corresponding changes to business models. The fact that only 40 percent of respondents to ISACA's 2018 Digital Transformation Barometer express confidence in their organization's ability to assess the security of systems based on AI and machine learning suggest that the challenges will only escalate in the coming years as AI and other fast-developing technologies are deployed more frequently. The global public and private sectors are still far from being prepared for this reality. In particular, there is much work to be done in recognizing the need to take a risk-based approach to understanding organizational cyber security preparedness and in appropriately prioritizing and investing in training resources for security teams.

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

Forensics and Investigation solutions will give you attack context, infrastructure-wide visibility, codified expertise, rich intelligence, and insights gained from front-line experience responding to the world's most impactful threats. So, you'll have everything you need to rapidly detect, triage, investigate, and minimize the impact of attacks.

# CHAPTER 2: LITERATURE REVIEW

R Von Solms, J Van Niekerk 2003 Department of Computer Science and Application, K.M.V., Jalandhar, India.The term cyber security is often used interchangeably with the term information security. This paper argues that, although there is a substantial overlap between cyber security and information security, these two concepts are not totally analogous. Moreover, the paper posits that cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself. In information security, reference to the human factor usually relates to the role(s) of humans in the security process. In cyber security this factor has an additional dimension, namely, the humans as potential targets of cyber attacks or even unknowingly participating in a cyber attack. This additional dimension has ethical implications for society as a whole, since the protection of certain vulnerable groups, for example children, could be seen as a societal responsibility.

W Wang, Z Lu - Computer networks, 2013 – Elsevier. The Smart Grid, generally referred to as the next-generation power system, is considered as a revolutionary and evolutionary regime of existing power grids. More importantly, with the integration of advanced computing and communication technologies, the Smart Grid is expected to greatly enhance efficiency and reliability of future power systems with renewable energy resources, as well as distributed intelligence and demand response. Along with the silent features of the Smart Grid, cyber security emerges to be a critical issue because millions of electronic devices are inter-connected via communication networks throughout critical power facilities, which has an immediate impact on reliability of such a widespread infrastructure. In this paper, we present a comprehensive survey of cyber security issues for the Smart Grid. Specifically, we focus on reviewing and discussing security requirements, network vulnerabilities, attack countermeasures, secure communication protocols and architectures in the Smart Grid. We aim to provide a deep understanding of security vulnerabilities and solutions in the Smart Grid and shed light on future research directions for Smart Grid security

Y Yan, Y Qian, H Sharif, D Tipper -Communications Surveys 2012. A smart grid is a new form of electricity network with high fidelity power-flow control, self-healing, and energy reliability and energy security using digital communications and control technology. To upgrade an existing power grid into a smart grid, it requires significant dependence on intelligent and secure communication infrastructures. It requires security frameworks for distributed communications, pervasive computing and sensing technologies in smart grid. However, as many of the communication technologies currently recommended to use by a smart grid is vulnerable in cyber security, it could lead to unreliable

system operations, causing unnecessary expenditure, even consequential disaster to both utilities and consumers. In this paper, we summarize the cyber security requirements and the possible vulnerabilities in smart grid communications and survey the current solutions on cyber security for smart grid communications.

L Hansen, H Nissenbaum - International studies quarterly, 2009 This article is devoted to an analysis of cyber security, a concept that arrived on the post-Cold War agenda in response to a mixture of technological innovations and changing geopolitical conditions. Adopting the framework of securitization theory, the article theorizes cyber security as a distinct sector with a particular constellation of threats and referent objects. It is held that "network security" and "individual security" are significant referent objects, but that their political importance arises from connections to the collective referent objects of "the state, society, the nation," and "the economy." These referent objects are articulated as threatened through three distinct forms of securitizations: hyper securitization, everyday security practices, and technifications. The applicability of the theoretical framework is then shown through a case-study of what has been labelled the first war in cyber space against Estonian public and commercial institutions in 2007.

J Liu, Y Xiao, S Li, W Liang Surveys & Tutorials, 2012. Smart grid is a promising power delivery infrastructure integrated with communication and information technologies. Its bi-directional communication and electricity flow enable both utilities and customers to monitor, predict, and manage energy usage. It also advances energy and environmental sustainability through the integration of vast distributed energy resources. Deploying such a green electric system has enormous and far-reaching economic and social benefits. Nevertheless, increased interconnection and integration also introduce cyber-vulnerabilities into the grid. Failure to address these problems will hinder the modernization of the existing power system. In order to build a reliable smart grid, an overview of relevant cyber security and privacy issues is presented. Based on current literatures, several potential research fields are discussed at the end of this paper.

CW Ten, G Manimaran, CC Liu - IEEE Transactions on 2010. Disruption of electric power operations can be catastrophic on national security and the economy. Due to the complexity of widely dispersed assets and the interdependences among computer, communication, and power infrastructures, the requirement to meet security and quality compliance on operations is a challenging issue. In recent years, the North American Electric Reliability Corporation (NERC) established a cyber security standard that requires utilities' compliance on cyber security of control systems. This standard identifies several cyber-related vulnerabilities that exist in control systems and recommends several remedial actions (e.g., best practices). In this paper, a comprehensive survey on cyber security of critical infrastructures is reported. A supervisory control and data acquisition security framework with the following four major components is

proposed: (1) real-time monitoring ; (2) anomaly detection ; (3) impact analysis ; and (4) mitigation strategies . In addition, an attack-tree-based methodology for impact analysis is developed. The attack-tree formulation based on power system control networks is used to evaluate system -, scenario -, and leaf -level vulnerabilities by identifying the system's adversary objectives. The leaf vulnerability is fundamental to the methodology that involves port auditing or password strength evaluation. The measure of vulnerabilities in the power system control framework is determined based on existing cyber security conditions, and then, the vulnerability indices are evaluated.

MD Cavelty – 2007. Myriam Dunn Cavelty posits that cyber-threats are definable by their unsubstantiated nature. Despite this, they have been propelled to the forefront of the political agenda. Using an innovative theoretical approach, this book examines how, under what conditions, by whom, for what reasons, and with what impact cyber-threats have been moved on to the political agenda. In particular, it analyses how governments have used threat frames, specific interpretive schemata about what counts as a threat or risk and how to respond to this threat. By approaching this subject from a security studies angle, this book closes a gap between practical and theoretical academic approaches. It also contributes to the more general debate about changing practices of national security and their implications for the international community.

AS Elmaghraby, MM Losavio - Journal of advanced research, 2014. The world is experiencing an evolution of Smart Cities. These emerge from innovations in information technology that, while they create new economic and social opportunities, pose challenges to our security and expectations of privacy. Humans are already interconnected via smart phones and gadgets. Smart energy meters, security devices and smart appliances are being used in many cities. Homes, cars, public venues and other social systems are now on their path to the full connectivity known as the “Internet of Things.” Standards are evolving for all of these potentially connected systems. They will lead to unprecedented improvements in the quality of life. To benefit from them, city infrastructures and services are changing with new interconnected systems for monitoring, control and automation. Intelligent transportation, public and private, will access a web of interconnected data from GPS location to weather and traffic updates. Integrated systems will aid public safety, emergency responders and in disaster recovery. We examine two important and entangled challenges: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go hand-in-hand with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live.

# CHAPTER 3: AIM & OBJECTIVES

## AIM:

Countermeasure of Cyber Security.

## OBJECTIVES:

- Security countermeasures are the controls used to protect the confidentiality, integrity, and availability of data.
- To prevent or mitigate the effects of a cyber attack against a victim, computer, server, network or associated device.
- Identify Fundamental Concepts Of Computer Security.
- Harden Internal Systems &Services.
- Establish Security Best Practices for Creating & Running Web-Based Applications.
- Identify Security Threats.
- To provide innovating countermeasures and ideas about the attacks.
- To provide well clean proper awareness.
- Manage Security Incidents.
- Monitor the Security Infrastructure.
- Enforce Organizational Security Policies.
- Secure Network Communications.

# CHAPTER 4: MATERIALS & METHODOLOGY

## MATERIALS

Computer, Cyber Attacks, Images, Case Studies etc.

## METHODOLOGY

### 1:- SCAM MESSAGES / SPAM MESSAGES

SCAM Messages or SPAM Messages also called as Phishing Attack. The main aim of the hackers is to get the confidential and secret credentials of other users worldwide, in order to gain financial benefits or many more. These guys are named as Scammers.

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful. The FBI's Internet Crime Complaint Centre reported that people lost $30 million to phishing schemes in one year. But there are several things you can do to protect yourself against phishing attacks. Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message. Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may:-

- Say they've noticed some suspicious activity or log-in attempts.
- Claim there's a problem with your account or your payment information.
- Say you must confirm some personal information.
- Include a fake invoice.
- Want you to click on a link to make a payment.
- Say you're eligible to register for a government refund.
- Offer a coupon for free stuffs
- Eligible for bank loan.
- Admit card is released.

- Gift from Microsoft.
- Flash online sale offering a massive discount.
- Messages from college, universities etc.
- Scholarship's offering and many more…..


Figure 1.0

We will receive messages that offers prices and discounts and many more to convince the peoples to click the fake links in order to get credentials. In the underground something weird is happening, we are automatically redirected to a fake websites which exactly looks like the original one.

Scams are based on communication made via email or on social networks. In many cases, cyber criminals will send users messages/emails by trying to trick them into providing them valuable and sensitive data (login credentials from bank account, social network, work account, cloud storage) that can prove to be valuable for them.

Moreover, these emails will seem to come from an official source (like bank institutions or any other financial authority, legitime companies or social networks representatives for users.) This way, they'll use social engineering techniques by convincing you to click on a specific (and) malicious link and access a website that looks legit, but it's actually controlled by them. You will be redirect to a fake login access page that resembles the real website. If you're not paying attention, you might end up giving your login credentials and other personal information.

We've seen many spam email campaigns in which phishing were the main attack vector for malicious criminals used to spread financial and data stealing malware.

In order for their success rate to grow, scammers create a sense of urgency. They'll tell you a frightening story of how your bank account is under threat and how you really need to access as soon as possible a site where you must insert your credentials in order to confirm your identity or your account.

After you fill in your online banking credentials, cyber criminals use them to breach your real bank account or to sell them on the dark web to other interested parties.

If you open such an email and click on the card, you usually end up with malicious software that is being downloaded and installed on your operating system. The malware may be an annoying program that will launch pop-ups with ads, unexpected windows all over the screen.

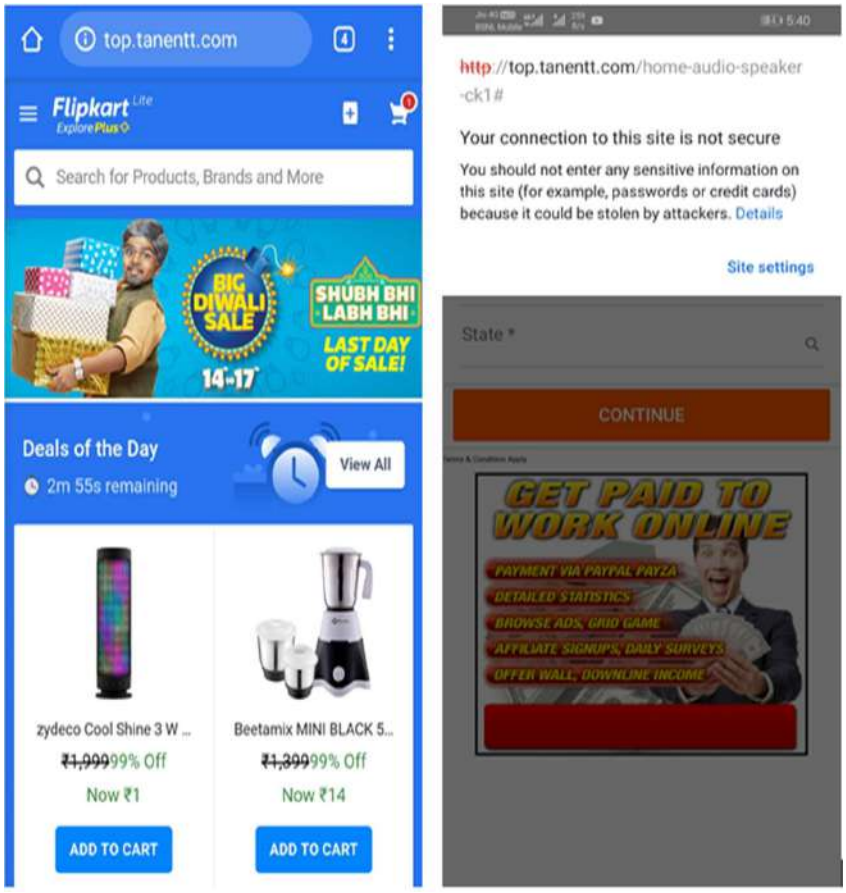


Figure 1.1

The attackers are well advanced and consider all the top rated user applications and websites for this Phishing process. Some of the applications like GOOGLE PAY, FLIPKART, AMAZON, BANK WEBSITES, ONLINE DATA ENTRY WEBSITES, GMAIL, YAHOO, HOTMAIL, REDIFF, INDIA TIMES and many more.

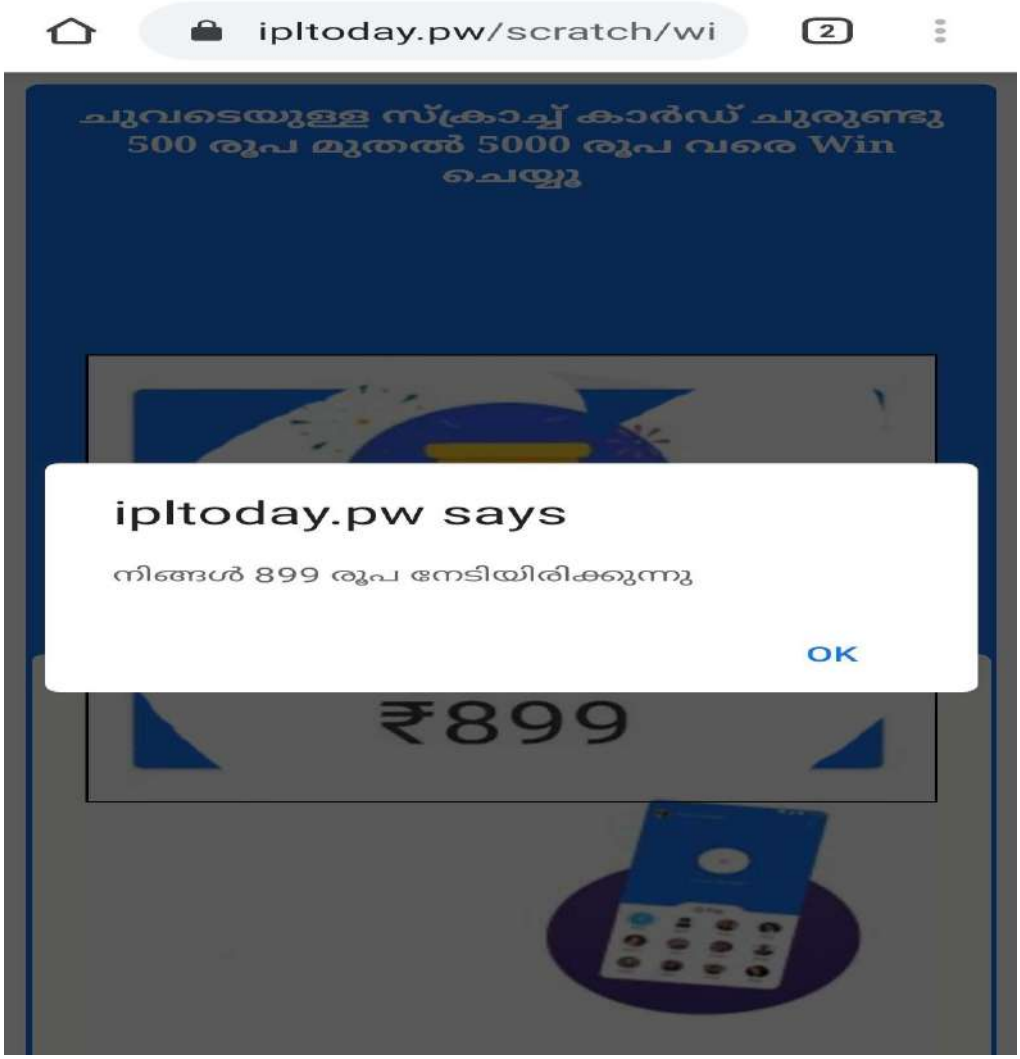


Figure 1.2

Spam has been growing rapidly over the years. According to some estimates, 64% of the total Internet mail in the year 2004 was spam, while other estimates put the figure at 77% and some others even put estimates at 88%. In a survey, Message labs identified 9.2 billion or about 73% of total Internet mail traffic as spam. A quarter of this spam in personal email accounts is considered to be pornographic in nature.

Spam has both direct and indirect costs. Direct costs are in the way of financial losses due to scams. However, they affect indirectly by reducing employee

efficiency, consuming network resources, causing annoyance, and in the spreading of viruses/ worms and other scams like phishing. Spam also adds a cost to the service provider and the end user in the form of filtering software, added bandwidth and storage. These costs, direct and indirect when combined, make spam a growing issue for companies and have a significant negative effect on business.

The worldwide cost of spam is rising enormously. According to a study by Radicati Group and Message Labs, the estimated worldwide cost to businesses due to spam is US$ 20.5 billion. In fact, spam could be costing an average company US$ 4.1 million a year in lost productivity, according to a report published by IDC. Another study by Forrester Research, 2003, found spam to be responsible for nearly US$20 billion in lost time and expenses worldwide

## COUNTERMEASURES FOR SCAM MESSAGES / SPAM MESSAGES

- Should not relay unauthorized mails (Should not be an Open Relay).
- Get updated the system and mobile devices.
- Don't visit unwanted websites and pages.
- Reject NULL sender identity.
  (Spammers sometimes try to send mail with no sender information. The Mail Server should be so configured that it rejects mails with NULL sender identity.)
- Define maximum number of recipients per message.
  (A single email message can be addressed to a number of recipients. A limit on the maximum number of recipients that may be addressed by a single message should be enforced, to prevent misuse by spammers.)
- Disguise e-mail addresses posted in a public electronic place.
  (Email addresses posted in a public web should be disguised through simple means to avoid being harvested by manual or automatic crawlers. They can be disguised by simple means such as replacing the symbol @ in the email id with some other symbol. Thus, "example@domain.com" could be written as "example [at] domain dot com". The email-id can be also be published on the web page as an image. In addition, the 'MAIL TO:' tag in source of the HTML pages should not be used so as to avoid the email address from being harvested by manual and automatic crawlers.)
- Users should be extremely careful while giving out their e-mail addresses to unknown commercial sites.
- Avoid using the same email-id for different purpose like business, personal, etc. Users should consider creating multiple e-mail addresses or accounts.
- Opt for Disposable email address which is available in the internet for free of cost.
- Using a filter and Enable spam filtering options in the email clients.

- Not use short e-mail addresses.
  (Short email addresses are easy to guess, and susceptible to brute-force attacks. Studies have shown that shorter email ids receive more spam. In fact, some free email address providers no longer accept short email addresses. Users should therefore use long email ids.)
- Don't access to uncertified websites link and so on.
- Enable SCAM OR SPAM identifier.

**2:- RANSOMWARE ATTACK**

Ransomware is a type of malware that has become a significant threat globally. Most of the current ransomware variants encrypt files on the infected system/network (crypto ransomware), although a few variants are known to erase files or block access to the system using other methods (locker ransomware). Once access to the system is blocked, the ransomware demands a ransom in order to unlock the files, frequently $200 - $3,000 in bitcoins, though other currencies and gift cards are occasionally reported. Ransomware variants almost always opportunistically target victims, infecting an array of devices from computers to smartphones. Victims are at risk of losing their files, but may also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for employees/customers.

The majority of ransomware is propagated through user-initiated actions such as clicking on a malicious link in a spam e-mail or visiting a malicious or compromised website. In other instances, malware is disseminated through malvertising and drive-by downloads, which do not require user engagement for the infection to be successful.

While almost all ransomware infections are opportunistic, disseminated through indiscriminate infection vectors such as those discussed above, in a few very rare instances cyber threat actors specifically target a victim. This may occur after the actors realize that a sensitive entity has been infected or because of specific infection attempts. The Federal Bureau of Investigation (FBI) refers to these instances as extortion, rather than ransomware, as there is almost always a higher ransom amount that coincides with the strategic targeting. This was the case in spring 2016, when several hospitals infected with strategically

targeted ransomware made the news. In the past year, ransomware variants features have expanded to include data exfiltration, participation in distributed denial of service (DDoS) attacks, and anti-detection components. Ransomware attack looks like below:-


Figure 1.3

## COUNTERMEASURES FOR RANSOMWARE ATTACK

- Have an incident response plan that includes what to do during a ransomware event.
- Keep all systems patched, including all hardware, including mobile devices, operating systems, software, and applications, including cloud locations and content management systems (CMS), patched and up-to-date.
- Restrict Internet access. Use a proxy server for Internet access and consider ad-blocking software. Restrict access to common ransomware entry points, such as personal email accounts and social networking websites.
- Software's and system must be up to date.
- Use firewall system and try to enable it, in order to fight against attacks. (ANTIVIRUS SOFTWARES ARE ALSO AVAILABE. Don't try to use CRACKED or PIRATED VERSION of its. In the underground hacking community antivirus software's themselves create viruses and worms and sell across the world, so we must opt for a genuine one)

- Participate in cyber security information sharing programs and organizations.
- Implement an anti-spam solution to stop phishing emails from reaching the network. Consider adding a warning banner to all emails from external sources that reminds users of the dangers of clicking on links and opening attachments.
- Backup's files are critical.
  (Use a backup system that allows multiple iterations of the backups to be saved, in case a copy of the backups includes encrypted or infected files. Routinely test backups for data integrity and to ensure it is operational.)
- Close the browser when it is not in use.
- Don't use multiple tabs at a time. It will leads to TAB NAPPING attack.
- Restrict administrative and system access.
  (Some strains of ransomware are designed to use a system administrator account to perform their operations. With this type of ransomware, decreasing user accounts and terminating all default system administrator accounts can create an extra roadblock.)
- Robust filtering fewer emails that contain spam or potentially malicious attacks.\
- Reviewing permission-related practices. Not give permission to all websites.
- Don't rely on ads popup.
- Close all open ports and use bitlocker encryptions for the drives.
- Use genuine version of OPERATING SYSTREM.
- Don't post our personal information's like mobile number, email address, card details and to unknown websites and applications.
- Don't reply to unsolicited phone calls, text messages or instant messages.
- Restoration of your files from a backup is the fastest way to regain access to your data. So backup is the more secure way to protect our file.
- Do not pay the ransom. It only encourages and funds these attackers. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.
- Poor protection practice is the main loop hole that will help the hackers to get access.

**3:- TROJAN HORSE ATTACK**

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network. A Trojan acts like a bona fide application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designed for.

You might think you've received an email from someone you know and click on what looks like a legitimate attachment. But you've been fooled. The email is from a cybercriminal, and the file you clicked on and

downloaded and opened has gone on to install malware on your device. When you execute the program, the malware can spread to other files and damage your computer. In a Trojan horse attack, a criminal disguises malware as a legitimate piece of software (like a program or app) or even a harmless document (like a spreadsheet) to trick users into willingly installing it on their computer.

Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include:

- Deleting data.
- Blocking data.
- Modifying data.
- Copying data.
- Disrupting the performance of computers or computer networks.

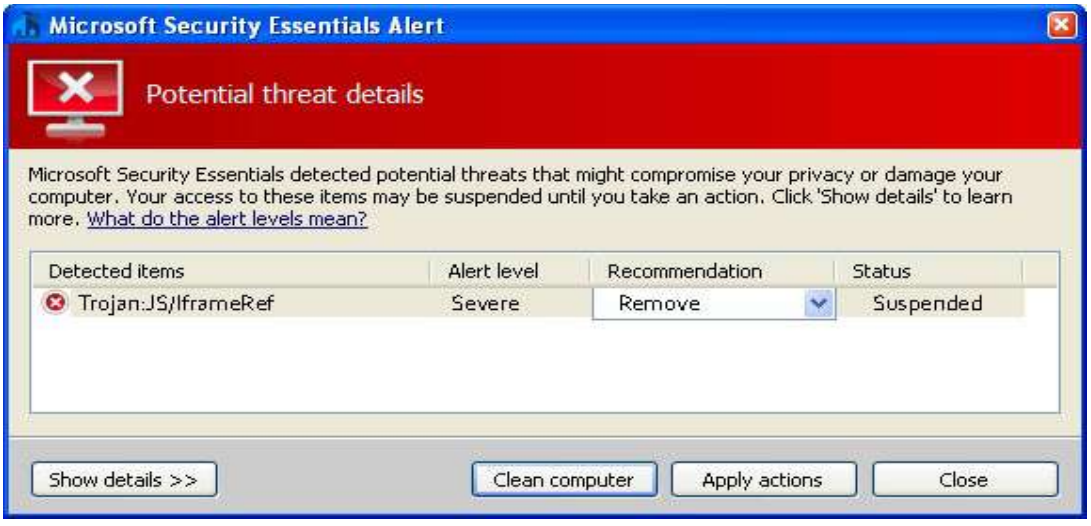


Figure 1.4

## COUNTERMEASURES FOR TROJAN HORSE ATTACK

- Installing the right endpoint protection software is critical and it would help users to stay ahead of Trojan attacks.
- Unparalleled antivirus, robust firewall, anti-spyware, application control featuring host intrusion prevention techniques.
- Encrypting your email helps protect you in many ways.

- Make sure all of your programs are up to date.
  (These updates patch any weaknesses that have been detected in a particular software. Even infrequently used programs are important to update as these are some of the weak areas used for intrusion.)
- Make sure your ISP has proper and effective security measures in place.
- Use Linux operating system.
  (Because it's less popular, there are hardly any viruses targeting Linux, meaning you are significantly less likely to be affected by malware.)
- Use Firefox or Opera web browsers.
  (These don't allow ActiveX controls, unlike Internet Explorer, which is one of the ways Trojans can infect your system.)
- Back up all of your data.
  (If your computer is infected with a Trojan, often times the process of removing them can result in file damage and loss of data. Always back up your hard drive in the event that your data is damaged by a Trojan or in the process of removing one.)
- Make sure your firewall is up and running.
  (Firewalls prevent unknown traffic from entering your computer, therefore blocking a potential Trojan. If your computer is already infected, an outbound-blocking firewall prevents any unauthorized programs from connecting to the Internet.)
- You must observe caution when opening email attachments, clicking on unfamiliar links, downloading and installing certain programs from publishers that you don't trust and visiting strange websites as some of these attachments, links, programs or websites could be Trojans that contain viruses.
- Update your security patches for your operating system.
- Use genuine operating system.
- Don’t Forget to Avoid Auto run.
  (Inserted a Pen drive or a hard disk to your computer. Well, you need to be sure that the Auto run option is disabled and first scan the drive properly. Not doing so, your computer may get affected. Infected external drives with viruses are one of the most common ways to infect your computer.)
- Avoid the Third Party Downloads.
  (Do not go to websites by clicking on shortened URLs. Type the website address in the address bar.)
- Do not download software from publishers you aren’t sure of.

## 4:- TAB NAPPING ATTACK

Tab nabbing is a computer exploit and phishing attack, which persuades users to submit their login details and passwords to popular websites by impersonating those sites and convincing the user that the site is genuine. The attack takes advantage of user trust and inattention to detail in regard to tabs, and the ability of browsers to navigate across a page's origin in inactive tabs a long time after the page is loaded. Tab nabbing is different from most phishing attacks in that the user no longer remembers that a certain tab was the result of a link unrelated to the login page, because the fake login page is loaded in one of the long-lived open tabs in their browser.

Tab nabbing is a form of cyber-attack which enables a hacker to take the advantage of the idle tabs in the browser and use them for carrying out the phishing attacks. The attack can be carried out even if the JavaScript is disabled, using the HTML attribute or a "meta refresh" meta element which are used for page redirection that causes a reload of a specified new page after a period of time. Also, the attack causes the browser to navigate to the spoofed page after the page has been left idle for some time.

**Procedure for the Attack:-**

1:- The hacker first creates a malicious website which have malicious script running in the background of website which are capable of detecting all the other tabs open in the current browser, and check if it those tabs are idle and inactive.

2:- When a user opens that malicious website, the script starts to execute. If any other tab is found idle and inactive, then the malicious script executes itself and rewrites the whole webpage in the tab where the malicious site was opened.

3:- To evade any type of detection, the malicious script even changes the title of the webpage along with favicon of the site. When the user comes back, he sees the malicious webpage as a genuine page (for example, a Gmail login page) asking for credentials. If the user provides his credentials, the information is sent directly to the hacker.

Figure 1.5

Tab napping attack occurs when we use multiple tabs at a time, here end user is surfing by opening multiple tabs within a browser such as BANKING WEBSITES, EMAIL ACCOUNT, SOCIAL MEDIA ACCOUNTS, NEWS, ARTICLES, and many more… in the underground something terrible is going on while we are using many tabs at a time.

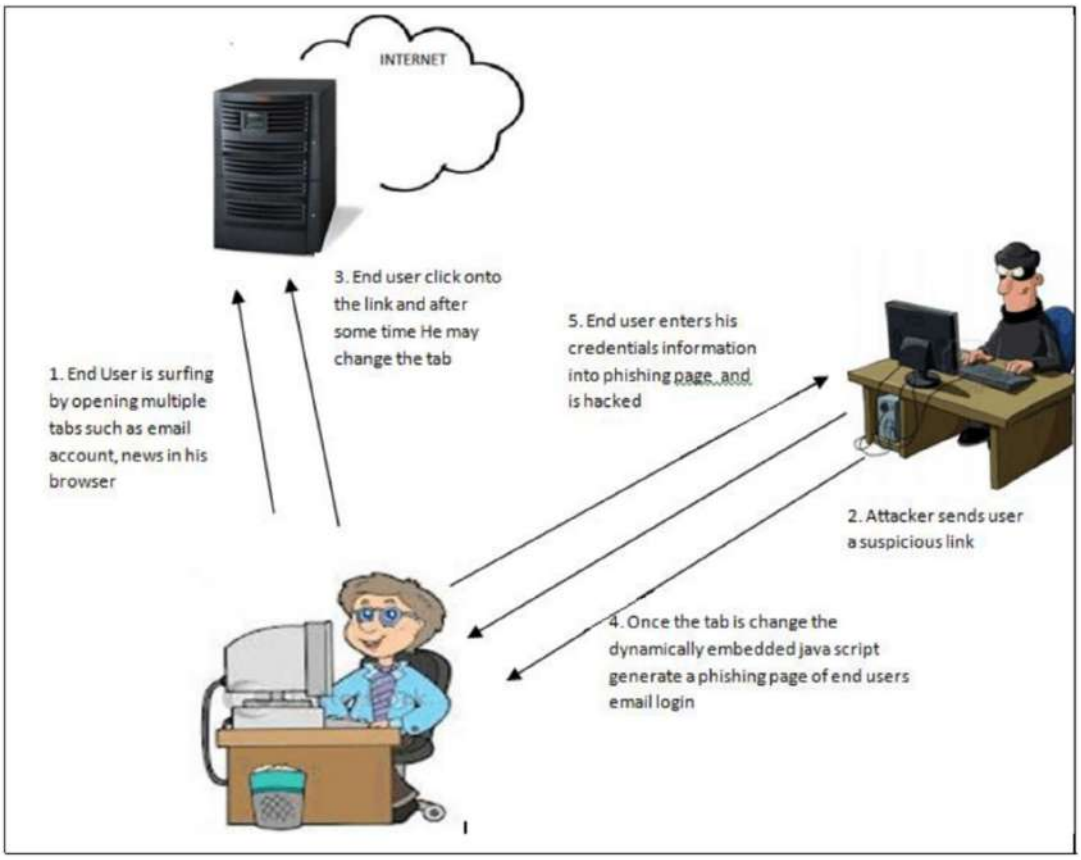


Figure 1.6

## COUNTERMEASURES FOR TAB NAPPING

- Be aware of Tab nabbing and know that tab icons and contents can be changed when you aren't looking.
- Always check the address bar for https:// and a legitimate/trusted domain name before entering a password into a web screen.
- Use firewall system and try to enable it, in order to fight against attacks.
  (ANTIVIRUS SOFTWARES ARE ALSO AVAILABE. Don't try to use CRACKED or PIRATED VERSION of its. In the underground hacking community antivirus software's themselves create viruses and worms and sell across the world, so we must opt for a genuine one)
- Prefer to use mobile apps over mobile web interfaces. Sites like Gmail, Ebay, Amazon, Office365, PayPal, and mobile banking sites are prime targets for this type of Tab nabbing attack.

# CHAPTER 5: OBSERVATION

## 1:- SCAM MESSAGES / SPAM MESSAGES

- Contents in the scam messages will be mostly related to business or financial platform.
- Source Email id not be genuine.
- Scam messages will offer fake promises.
- Scam messages will ask our personal data's like (Account number, Card number, CVV, Internet banking password etc.
- Mainly we can see SCAM messages in social Medias and email platforms.

## 2:- RANSOMWARE ATTACK

- Mainly the attack will encrypt our personal data's and ask for ransom.
- Ransom attack is caused by downloading unknown files from unauthorized sites.
- Victims themselves cannot decrypt the data which are encrypted by the attacker.
- Mainly ransome attack is focused on corporates, MLM, IT sectors.

## 3:- TROJAN HORSE ATTACK

- Trojan create backdoor for attackers by creating vulnerabilities in our system.
- Through Trojan we can remotely access a targeted system.
- Trojan can either manipulate our personal data or it can corrupt the data.
- It is difficult to find out Trojan using free ware antiviruses.

## 4:- TAB NAPPING ATTACK

- This occurs when we are handling with multiple tabs in a single browser.
- Its quiet easy to run some kind of java scripts to active the attack.
- Attackers will get our credentials and other details.
- Tab napping is a common attack which we can see everywhere.
- It's an issue for common users in India and globally.

# CHAPTER 6: RESULTS & CONCLUSION

**RESULT:-**

By the analysis of various types of attacks, I have found the countermeasures.

**1:- SCAM MESSAGES / SPAM MESSAGES**

• Should not relay unauthorized mails (Should not be an Open Relay).

• Get updated the system and mobile devices.

• Don't visit unwanted websites and pages.

• Reject NULL sender identity. (Spammers sometimes try to send mail with no sender information. The Mail Server should be so configured that it rejects mails with NULL sender identity.)

• Define maximum number of recipients per message.

**2:- RANSOMWARE ATTACK**

• Have an incident response plan that includes what to do during a ransomware event.

• Keep all systems patched, including all hardware, including mobile devices, operating systems, software, and applications, including cloud locations and content management systems (CMS), patched and up-to-date.

• Restrict Internet access. Use a proxy server for Internet access and consider ad-blocking software. Restrict access to common ransomware entry points, such as personal email accounts and social networking websites.

• Software's and system must be up to date.

**3:- TROJAN HORSE ATTACK**

• Installing the right endpoint protection software is critical and it would help users to stay ahead of Trojan attacks.

• Unparalleled antivirus, robust firewall, anti-spyware, application control featuring host intrusion prevention techniques.

• Encrypting your email helps protect you in many ways.

• Make sure all of your programs are up to date.

**4:- TAB NAPPING ATTACK**

• Be aware of Tab nabbing and know that tab icons and contents can be changed when you aren't looking.

## CONCLUSION

Mounting a good defence requires understanding the offense. This article has reviewed the 10 most common cyber-security attacks that hackers use to disrupt and compromise information systems. As you can see, attackers have many options, such as DDoS assaults, malware infection, man-in-the-middle interception, and brute-force password guessing, to trying to gain unauthorized access to critical infrastructures and sensitive data.

Measures to mitigate these threats vary, but security basics stay the same: Keep your systems and anti-virus databases up to date, train your employees, configure your firewall to whitelist only the specific ports and hosts you need, keep your passwords strong, use a least-privilege model in your IT environment, make regular backups, and continuously audit your IT systems for suspicious activity.

# REFERENCE

[1] G. M. Koien and V. A. Oleshchuk, Aspects of Personal Privacy in Communications-Problems, Technology and Solutions. River Publishers, 2013.

[2] N. R. Prasad, "Threat model framework and methodology for personal networks (pns)," in Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on. IEEE, 2007, pp. 1–6.

[3] Assis F., OSBF-Lua -- A Text Classification Module for Lua. The Importance of the Training Method, The Fifteenth Text REtrieval Conference Proceedings (TREC), Nov, 2006.

[4] Mimoso, Michael (28 March 2016). "Petya Ransomware Master File Table Encryption". threatpost.com. Retrieved 28 July 2016.

[5] "Trojan Horse: [coined By MIT-hacker-turned-NSA-spook Dan Edwards] N." Retrieved April 5, 2012.

[6] Claburn, Thomas (2010-05-25). "Tabnapping attack makes phishing easy". Information Week. Retrieved 2012-02-19.