IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBERCRIME CATEGORIES AND PREVENTION

[1]Manishaben Jaiswal

Abstract: After determining computer system criminal offense within endeavor, experts examine the styles that have been devoted over the last, and the brand new techniques probably to seem down the road. Experts also check the challenge in evaluating and discovering computer system criminal activity, procedures for trying to put on trial or even stop such criminal offenses, and the performance of these solutions. Just a little portion of computer system breather-ins are sensed, as well as, in addition, stats on computer system unlawful act are usually not available. The most usual types of computer system criminal activity mentioned to InterGOV consist of youngster fraudulence, email, and porn spam. Buffers versus computer system illegal activity might happen in the restricting access to the relevant information to be safeguarded, using file encryption to ensure personal privacy and stability, and enlightening the social concerning safety concerns. It provides information on cybercrime and various types and how to prevent the data from the threat.

Keywords: Cybercrime, spam, phising, spoofing, e-mail, DNS, website, pharming, hackers, network security, biometric controls,

1. INTRODUCTION

Internet, technically the group of abundant computers connected to share data. Now, data has increased since the date from which the internet can be thought has inception. This data is of all forms from text to pictures to videos and from various sources, like books to financial data, from images to international treaties. It requires safety at all levels, from the threat of people sitting behind any system, maybe thousands of miles away, to stealing or corrupting information. So, this stealing or hacking is technically termed cybercrime. It's of paramount importance because data is the most precious thing in the world. But cybercrime is most difficult to tackle because of its nature of veil of anonymity, perpetrated in a computer environment, clever criminals with state-of-the-art technology, and the worst Trans-National criminals creating all sorts of jurisdiction issues. Cybercrime is "any crime that is facilitated using a computer, network, or hardware device." United Nations Manual on the Prevention and Control of Computer-Related Crime states that cybercrime is a fraud, forgery, and unauthorized access to the data.

2. CYBERCRIMINALS

Simply put, a cybercriminal is a person committing cybercrime. They can be classified through various ways like

Classification based on age

- Teenagers (age group 9-16)
  This age group commits the crime, and they don't even perceive that they are executing it. They do it sometimes to draw pride from the act.
- Organized Hacktivists
  Hackers with a standard motive conglomerate are Hacktivists. These motives can be political, religious, etc.
- Disgruntled Employees
  They are displeased employees who do harm their employers by sitting behind a computer system. These acts can even damage the organization's whole network that can even be spread across the globe.
- Professional Hackers
  These are hackers that rival companies hire to harm their competitors. This harm can range from stealing sensitive information to pushing the system down.

3. CLASSIFICATION: CYBERCRIME

Cybercrime is determined as a criminal activity where a computer system is a criminal offense or even used as a resource to devote an infraction. A cybercriminal might use a tool to access a customer's private details, personal service details, federal government relevant information, or even turn off a device. It is likewise a cybercrime to offer or even generate the above relevant information online.

Lawbreakers of the World Wide Web make use of web consumers' details for their increase. They also acquire accessibility to categorized authorities' relevant information. The progression of innovation and improving ease of access of wise technicians suggests there is numerous gain access to factors within consumers' houses for cyberpunks to manipulate. While rule administration tries to take on the expanding problem, unlawful varieties increase, taking perk of the privacy of the web.

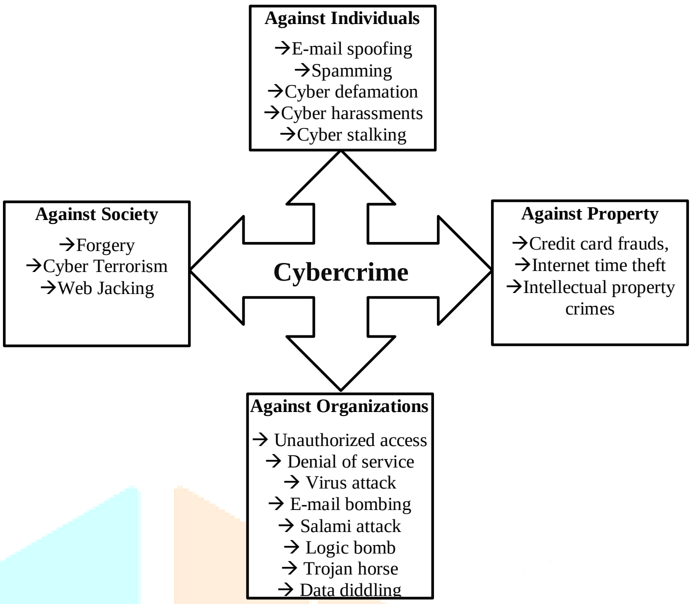


Fig 3.0 Classification of Cybercrime

As shown above, figure

- Against Individuals: These include e-mail spoofing, spamming, cyber defamation, cyber harassment, and cyberstalking
- Against Property: These include credit card frauds, internet time theft, and intellectual property crimes.
- Against Organizations: Unauthorized access, denial Of service, computer contamination or virus attack, e-mail bombing, salami attack, logic bomb, trojan horse, and data diddling.
- Against Society: These include Forgery, Cyber Terrorism, Web Jacking.

4. PHISHING

Phishing is frequently utilized to function in regulatory or business systems as a component of a much larger assault, such as an enhanced relentless hazard occasion. The staff members are weakened to sidestep safety and security boundaries, arrange malware inside a closed-up atmosphere, or even increase lucky accessibility to protected information.

Phishing is a social planning strike usually used to swipe consumer records, including login references and bank card varieties. It occurs when an aggressor, impersonating a count on the body, deceives a target to open up an e-mail, instantaneous notification, or even text. After that, the recipient is fooled right into clicking on a harmful hyperlink. Which easily triggers the setup of malware. The icy of the device as a portion of a ransomware spell, or even the uncovering of delicate info.

An enchantment may possess terrible outcomes. For people, this consists of unwarranted investments, the robbing of funds, or even identification fraud. A company catching such a spell generally maintains intense monetary reductions and decreases market credibility and reputation, allotment, and buyer trust fund. Depending upon the extent, a phishing effort could intensify into a safety event where a company will certainly possess a challenging opportunity bouncing back.

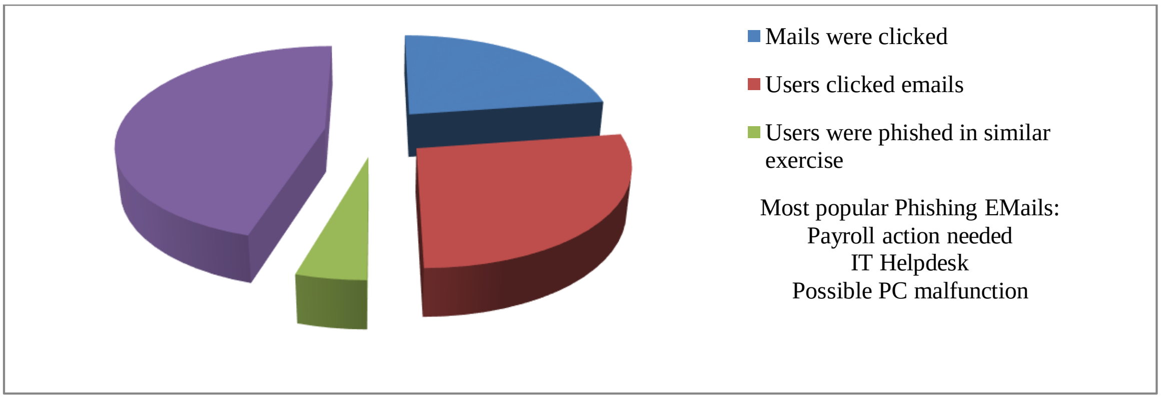


Fig 4.0 Phishing Analysis

The following figure illustrates the most common email subjects that are clicked as bait in phishing.

A severe threat of phishing attacks arose for the health care industry. The employees of this industry are not well versed with phishing baits in the form of emails which brought about severe consequences in the form of breaches. The following figure demonstrated the phishing attacks in the healthcare industry.

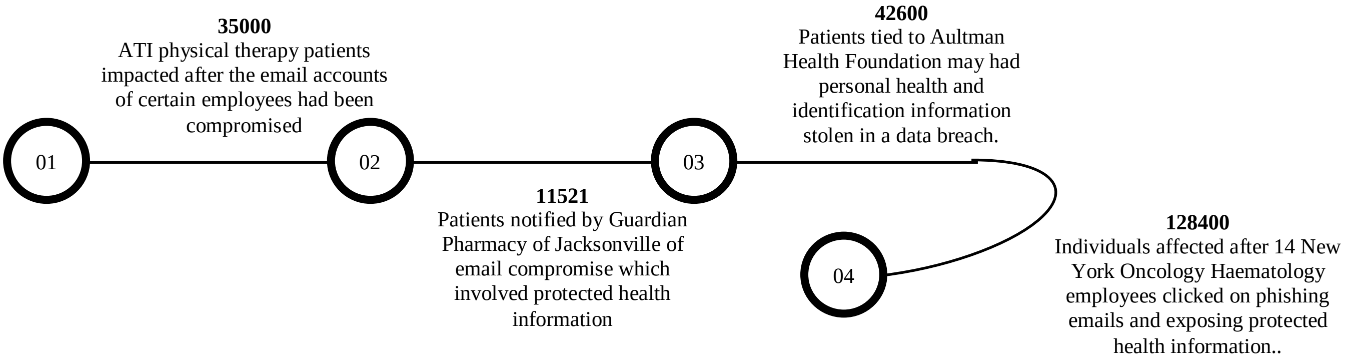

35000
ATI physical therapy patients impacted after the email accounts of certain employees had been compromised
42600
Patients tied to Aultman Health Foundation may had personal health and identification information stolen in a data breach.
01
02
03
11521
Patients notified by Guardian Pharmacy of Jacksonville of email compromise which involved protected health information
04
128400
Individuals affected after 14 New York Oncology Haematology employees clicked on phishing emails and exposing protected health information..

Fig 4.1 Phishing threats in healthcare

4.1 PHISHING ATTACK EXAMPLE:

The sticking emphasizes a usual phishing rip-off effort. A spoofed e-mail seemingly coming from myuniversity.edu is mass-distributed to as numerous professors as achievable. The e-mail states that the consumer's code will run out. Directions are offered to visit myuniversity.edu/renewal to revive their code within twenty-four hrs.

Several points may happen by clicking on the hyperlink. The consumer is rerouted to myuniversity.edurenewal.com, a fraudulent web page that seems precisely like the actual revival web page, where both brand new and existing security passwords are asked for it. The opponent, checking the web page, pirates the initial code to access gotten places on the educational institution system. The customer is sent out to the actual code revival webpage. While being rerouted, a harmful manuscript triggers the history of pirating the customer's treatment biscuit. It causes a demonstrated XSS spell, offering the wrongdoer lucky accessibility to the college system.

5. SPOOFING

Spoofing is an extensive condition for the kind of actions that entails a cybercriminal impersonating a count on the facility or unit to receive you to carry out one thing good for the cyberpunk and harmful to you. Whenever an online fraudster conceals their identification as another thing, it is spoofing.

In cybersecurity, 'spoofing' is when cheaters become a person or even something to gain an individual's count. The inspiration is normal to access devices, take records, swipe cash, or even spread malware. Spoofing may relate to a series of interaction stations and may entail various degrees of technical complication. Spoofing strikes typically involve an aspect of social planning, where fraudsters emotionally manipulate their sufferers through using individual susceptibilities like concern, piggishness, or even the absence of technology.

5.1 HOW DOES SPOOFING WORK?

There are various forms of spoofing assaults. The much more uncomplicated ones connect to e-mails, websites, and telephone calls. The additional structure of technological assaults entails internet protocol handles, Address Resolution Protocol (ARP), and Domain Name System (DNS) web servers. Experts discover one of the most usual spoofing instances listed below.

Spoofing commonly depends on pair of aspects. Spoof on its own, including a forged e-mail or even site, and after that, the social planning element pokes targets to act. Spoofers might send out an e-mail that shows up to come from a relied on an elderly colleague or even supervisor, inquiring you to move some cash online and giving a prodding reasoning for the demand. Spoofers usually understand what cords to draw to adjust a prey right into taking the preferred activity within this instance, licensing a deceptive cord move without elevating uncertainty.

A prosperous spoofing assault may possess severe outcomes featuring swiping individual or even firm relevant information. Collecting references for usage in more strikes, dispersing malware, getting unapproved system access, or even bypassing access to commands. For services, spoofing assaults can easily result in ransomware strikes or even expensive and detrimental information violations.

5.2 TYPES OF SPOOFING:

5.2.1 E-mail spoofing:

Amongst one of the most widely-used assaults, e-mail spoofing occurs when the email sender creates e-mail headers to that customer software application presents the deceptive email-sender handle, which most customers trust. Unless they examine the title carefully, e-mail receivers take up the built email sender who has sent the notification. They are most likely to trust it if it is a title they recognize.

Spoofed e-mails typically ask for a loan move or even consent to access a unit. Also, they can easily often include add-ons that put up malware, including Trojans or even infections when opened up. In most cases, the malware is developed to prevent corrupting your personal computer and infecting your whole system.

Email spoofing depends intensely on social planning. The capacity to encourage an individual customer to feel that what they are finding is legit, triggering all of them to react and open up an accessory, transmit the amount of money, and more.

5.2.2 IP Spoofing

Internet protocol spoofing includes an assailant attempting to acquire unapproved accessibility to a unit through sending out notifications along with a spoofed. Or else even phony Internet protocol deal with to create it appear like the information happened to come from a dependent resource, such as one on the same inner personal computer system. Whereas e-mail spoofing pays attention to the individual, internet protocol spoofing is mostly targeted at a system.

Cybercriminals obtain it by taking a good multitude's internet protocol handle and changing the package headers sent out coming from their body to make all of them seem coming from the initial, counted on a personal computer. Capturing internet protocol spoofing strikes at the beginning is vital. They frequently happen as an aspect of DDoS (Distributed Denial of Service) strikes, which may take a whole system offline.

5.2.3 Website spoofing

Site spoofing also understood as URL spoofing, is when fraudsters create a deceptive site similar to a valid one. Usually, site spoofing takes location in combination along with e-mail spoofing. For instance, fraudsters could deliver you an e-mail consisting of a hyperlink to the artificial website.

5.2.4 DNS Spoofing

DNS spoofing is sometimes referred to as DNS store poisoning, is an assault through which transformed DNS files are used to reroute the internet web traffic to a phony site that resembles its own planned location. Spoofers accomplish it by substituting the internet protocol deals with saved in the DNS web server and the cyberpunks would like to utilize.

How to prevent spoofing:

Typically, clinging to these on the internet, safety and security pointers are going to aid to lessen the visibility to spoofing assaults:

- Steer clear of using the same code throughout the panel and also alter your security password regularly. If users utilize social making contacts web sites, be mindful that you attach along with and know how to use your privacy and surveillance environments to guarantee you keep secure. If you identify questionable actions, have hit on Spam, or even have been scammed on the internet, take measures to safeguard your profile and be certain to mention it.
- Stay clear of clicking hyperlinks or even opening up add-ons coming from strange resources. It might have malware or even infections that will corrupt your tool. , if in uncertainty consistently prevent.
- Do not respond to e-mails or even telephone calls coming from unacknowledged email senders. Any kind of interaction along with a fraudster brings prospective threats and also welcomes additional unnecessary notifications.
- Feasible put together two-factor verification. It incorporates an additional level of safety and security to the verification method and makes it harder for aggressors to access your tools or even online profiles. Stay away from utilizing the same security password around the panel and alter your security password consistently.
- A security password supervisor device is an outstanding technique to handle the codes.
- Assessment of your online personal privacy environments. Be mindful that data hook up and find out exactly how to utilize your privacy and protection environments to guarantee you remain secure if users use social making contacts web sites. If you acknowledge questionable actions, have clicked Spam, or even have been scammed online, take measures to safeguard your profile as well as make sure to disclose it.
- Do not offer private details online. Please avoid revealing exclusive and personal info online unless you are 100% certain it is a dependent resource.
- Maintain the system as well as software application around the day. Software application updates consist of safety spots, infection remedies, and brand-new functions, which reduce the danger of malware disease and safety violations.
- Keep an eye out for internet sites, e-mails, or even information along with bad punctuation or sentence structure and every other component that appears improper, including company logos, colors, or even skipping web content. It may be an indication of spoofing. Just go to sites along with an authentic safety certification.

6. SPAM

Observe the past spam segment listed below, which intrigued me by the beginnings of Spam in a more significant particular.

Spam is any type of undesirable, unrequested data that acquires sent wholesale. Commonly Spam is delivered using e-mail. However, it may likewise be circulated utilizing text, telephone calls, or even social networks. Spam is certainly not a phrase for a pc hazard, although some have been proposed (dumb unproductive bothersome malware, for example). The motivation for using the condition "spam" to illustrate undesirable mass information is a Monty Python act. The stars state that everybody needs to consume the meals Spam, whether they desire it or otherwise. Everybody along with an e-mail handle must, regrettably, be troubled through spam information, whether any corporation likes it or even certainly not.

6.1 TYPES OF SPAM

Spammers utilize numerous kinds of interaction to bulk send their undesirable notifications. A few of these are industry notifications marketing unrequested products. Various other types of spam notifications may disperse malware, the technique you right into revealing private info, or even shock you right into presuming you need to have to pay for to leave issue.

Email spam filters record much of these kinds of information, and phone service providers are usually alert of a "spam danger" coming from unfamiliar customers. Whether using e-mail, message, phone, or even social networking sites, some spam notifications perform to make it through and intend to have the ability to acknowledge all of them and prevent these dangers. Below are many kinds of Spam to keep an eye out for it.

6.2 REPORTING OF SPAM

Coverage spam can easily assist e-mail service providers or phone company feel better at discovering Spam. Suppose genuine e-mails obtain delivered spam filters. In that case, users can easily state that they must certainly not be denoted as Spam, which additionally supplies valuable details about what needs to certainly not be filtering the system. One more valuable measure is incorporating email senders intend to learn through calls checklist.

Email suppliers have acquired respectable at straining Spam, yet when information is utilized in the inbox. It can easily report all of them. It is real for spam rings and content notifications, as numerous service providers provide the capacity to mention Spam. Likewise, it can choose to shut out the email sender, typically in the same measure as saying the information.

6.3 USE TWO-FACTOR AUTHENTICATION (2FA)

Along with two-factor or even multi-factor verification, regardless of whether username and code are jeopardized through a phishing assault, cybercriminals will not have the capacity to navigate the different authorization needs connected to the profile. Additional verification variables feature top secret inquiries or even proof codes delivered to the phone through text.

6.4 INSTALL CYBERSECURITY

They hit a negative weblink or even install malware delivered by Spam. An excellent cybersecurity software program will identify the malware and close it down before damaging the body or even the system. Malwarebytes has received it dealt with everywhere modern technology takes it, along with items for residence and company.

How to prevent Spam

If a brand-new kind of phishing strike happens out, an expert might certainly not quickly identify it. To guard on own, find out to inspect for Some crucial indications that a piece of spam information isn't merely irritating; it is a phishing try:

- An overlooking private welcoming alone isn't sufficient to locate a phishing e-mail. However, it is one factor to appear for, particularly in notifications that claim they are coming from a provider along with whom you carry out the company. Suppose you receive a piece of information coming from a business along with those who possess a profile. In that case, it is smart to log in to your profile to find if there is a piece of information there certainly instead of simply hitting the web link in the report without confirming. You can easily consult with the business to inquire if a doubtful notification is legit or even certainly not.
- Email sender's e-mail handle: If an e-mail coming from a business is legit, the email sender's e-mail handle needs to match the domain name for the company they state to stand for. Often these are noticeable, like example@abkljzr09348.biz. However, various other opportunities the improvements are much less detectable, like example@paypa1.com as opposed to paypal.com.
- Skipping individual details: If you are a consumer, the firm needs to possess the attributes and likely resolve them through the initial title. A missing out on personal welcoming alone isn't sufficient to locate a phishing e-mail. Yet, it is one trait to search for, particularly in notifications that state they are coming from a business along with whom you perform service.
- Syntactical mistakes: A business sending genuine notifications may not possess many spelling mistakes, bad sentence structure, and punctuation blunders. It may be yet another warning to show that e-mail can be problematic.

- Too-good-to-be-true deals: Many phishing information claims to become coming from huge, popular businesses, wanting to trap visitors that take place to perform organization along with the company. Various other phishing tries to deliver one thing free of charges like cash or even a preferable reward. The claiming is frequently accurate that if one thing appears extremely excellent to become real, it is actually. Also, this could be a caution that spam information is making an effort to obtain one thing coming from the user instead of providing you with one thing.
- Accessories: Unless you are anticipating an e-mail along with add-ons, regularly beware just before opening up or even installing all of them. Making use of anti-malware software applications can easily aid through checking reports that establish malware.

7. PHARMING

Pharming is an extrapolation of a phishing attack. It infects the user's computer and installs the malicious code on the user account that redirects it to the imitated website. In this case, the attacker has not had to wait for the user to click the bait. Instead, the malicious code redirects itself to the attacker’s website and hence removes the extra step of the need of the user to click on the malicious website link. So, the basic difference between phishing and pharming is that the attacker sends an email that looks like the original website in the case of phishing. Through it, the attacker tries to capture sensitive information. In the case of pharming, the malicious code directs the other infection process.

The following figure illustrates the basic functioning of a pharming attack.

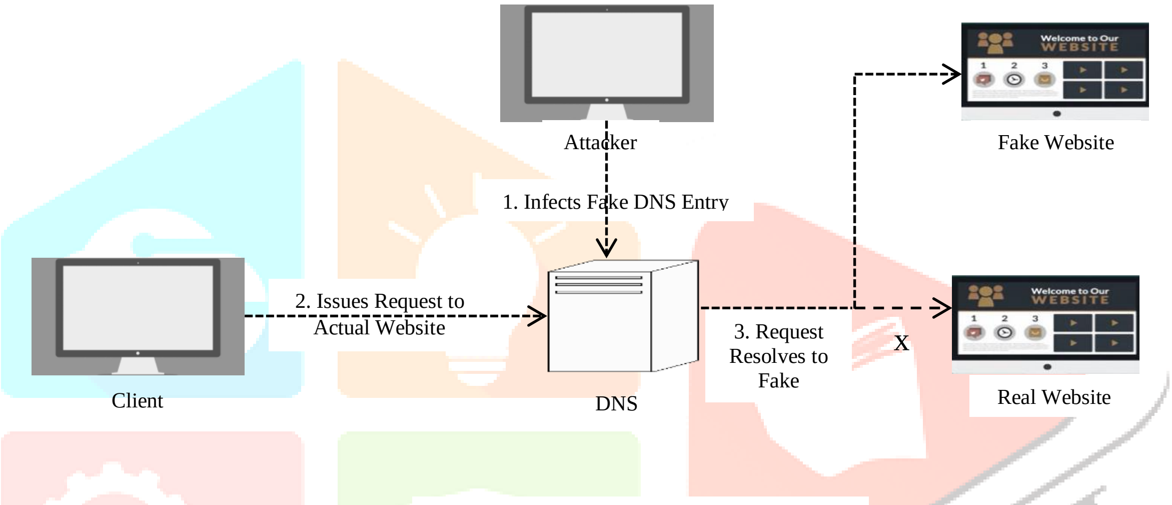

Attacker
Fake Website
Welcome to Our WEBSITE
1. Infects Fake DNS Entry
2. Issues Request to Actual Website
Client
DNS
3. Request Resolves to Fake
X
Real Website
Welcome to Our WEBSITE

Fig 7.0 working of pharming attack

The phishing attacks of 2006 had a pretty devastating effect on the software of Microsoft Corporation. In this case, attackers stuffed the website with malicious code. In addition to this, they installed a bot, which provided the attackers the remote of users' PC.

8. MALICIOUS HACKING

Technically hacking is nothing but malicious use of digital devices to have damage, corrupt systems, steal information, or disrupt normal activity. Hacking is highly skilled programmers that have increased sophistication for breaching the security of the victim. Hacking is now an industry with comprehended techniques and high success rates.

8.1 DRIVERS OF HACKERS

Following are the few drivers that motivate hackers:

- The direct gain in terms of money through stealing information of credit details or by defrauding financial services.
- Gain through corporate spying
- Gain popularity or notoriety for so-called hacking talent
- Government-aided hacking to steal information for national intelligence.
- Public attention is yet another motive for leaking sensitive information.

8.2 TYPES OF HACKING

- Black Hat Hackers

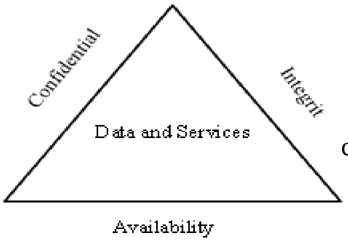
  They can be considered as black souls of the hacking industry. They perform hacking for all the drivers stated above.

- White Hat Hackers

  They are hackers that stand in the path of black hat hackers and prevent their success through proactive hacking. They enter the system to measure network security; this is technically termed ethical hacking. Companies hire these hackers to detect a potential breach in their systems proactively.

- Grey Hat Hackers
  They exist between black and white hackers. They enter into the system not to harm it or gain financial, but they do it publicly.

9. NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS



When a system gets connected to the internet, incident traffic is immeasurable, creating vulnerabilities. Network security augments network security by evading downtimes by continuously monitoring suspected malicious transactions that sabotage the systems.

Fig 9.0 Network security essentials

According to NIST Computer Security Handbook, computer network security is the protection offered to an automated information system to accomplish the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources, including hardware, software, firmware, information, and telecommunication.

A new approach for implementing distributed security solutions in a controlled collaborative manner, called grid of security, in which community of devices ensures that a device is trustworthy and communications between devices can be performed under control of the system policies."

Keeping in view the above definition following terms need to be expanded. They form the major security objectives.

- Confidentiality
  It includes data confidentiality and privacy. Here data confidentiality means the sensitive information is not available for unauthorized access. Privacy means to control which related information can be collected, seen, or stored to whom.
- Integrity
  It also includes two terms of data and system integrity. Data form of integrity assures that information can be altered through authorized access. System integrity has that the system is not changed through unauthorized deliberate ways.
- Availability
  It prompts that system works as expected and services are not denied to authorized users.

9.1 CHALLENGES OF COMPUTER SECURITY

- Security requirements are simple, i.e., they should include confidentiality, authentication, non-repudiation, and integrity. But the process to implement these requirements is quite complex.
- There can be an unexpected weakness in the system.
- It is difficult to implement a security mechanism against potential unexpected threats.
- After designing the mechanism, the next issue for crops is to decide where to implement physical and logical security mechanisms.
- Security mechanism also involves the exchange of secret information for the algorithm.
- The designer and administrator of the security mechanism need to find and fill all weaknesses in the system. In contrast, the attacker has to find out a single flaw in the system.
- Companies don't want to invest in security systems until a system failure occurs.
- Mechanism of security requires constant monitoring that gets difficult in the busy environment.

9.2 STANDARDS OF NETWORK SECURITY

Many organizations are involved in designing the standards like:

- **National Institute of Standards and Technology (NIST)**
  It is a federal agency that includes measurement science, standards, and technology relating to the US government. But these have a worldwide utility.

- **Internet Society**
  It is a society that has members of both types, including organizations and individuals. It deals with the future of the internet, internet infrastructure, with the internet engineering task force.

The following security controls are required to be implemented.

- **Currently deployed Network devices**: If the device now used does not fulfill the standards, that needs to be looked after.
- **Purchase and installation of new Network Devices**: All new devices purchased should comply with the standards. They should be configured following all requirements of the standards.
  - ✓ Physical security: All physical devices should be in an area with physical access control. All controlled devices should be installed in an area that is secured with an alarm system. All machines should be maintained with UPS and power backup
  - ✓ Authentication and access lists: Every access to the network devices should be validated by access lists that allow only authorized personnel. All external attempts of access should be blocked through access lists. Strong passwords should be allowed for non-interactive purposes.
  - ✓ Network management: Text protocols should be avoided in network management. All device management interfaces should be on the management network
  - ✓ Intrusion Detection System: The link connecting the owned system with the external system should have an IDS installed. Blocked systems will not be allowed access until the cause of detection is understood and treated well.
  - ✓ Anti ARP-spoofing: DHCP support should be enabled.
  - ✓ Change control: A strong change control should be implemented so that any change involving risks should cross through the change control process.
  - ✓ Logging and monitoring: All devices should log in to Network Management System to be monitored regularly.
  - ✓ Passwords: Passwords should be strong enough to guess and should be changed regularly according to standards.
  - ✓ Configuration backups: All configurations should be backed up regularly. An audit of network configurations should be done.
  - ✓ VPN: All VPNs that are deployed for organizations should be configured to get unified access with security review
  - ✓ Wireless Security: All wireless devices should have ISO encryption methods.

9.3 WAYS OF NETWORK SECURITY

- A strong firewall and proxy should be used to avoid unwanted people.
- A complete package of internet security software should be used with a large spectrum antivirus software package.
- A strong password should be used; it should be updated biweekly or monthly to maintain high authenticity.
- Network analyzer should be used whenever required.
- Physical security plays a vital role in network security. So CCTV with MICS is also very important.

9.4 NETWORK BUSINESS SECURITY MODEL

The information security model comprises three constituents: data security, network system security, and network business security. Now, when communicating data is most important henceforth, network security control is of paramount importance. It can be achieved through application gateways, packet filtering, or with some hybrid system.

- **Application Gateways**

  It is one form of the first firewall which runs at the application layer of the ISO/OSI Reference Model. Here the clients need to be prioritized or categorized as it does not hold anything as default before starting the traffic.
- **Packet Filtering**

  In this case, the routers contain the Access Control Lists, so only defined users can pass through the network. It is also present at the lower ISO/OSI layer, making it less complex than an application gateway.
- **Hybrid Systems**

  It is a system having the speed of packet filtering and security features of the application gateway. So packet filters check that only original packets traverse through the system, whereas the rest is checked at the session layer.

9.5 ORGANIZATIONAL STEPS FOR NETWORK SECURITY

In terms of expanse, the organizations also need to expand network security with business growth. As it can be neglected until a security threat arises, it also requires proper planning and implementation. Nowadays, the dangers are focused on the application layer rather than the network layer. So, the following are among the possible solutions for the same:

- Secure office and remote connection with controlled internet access.
- Protection for network, services, and applications in the office network.
- Network division, desktop-server-data center protection.
- Easy deployment of security solutions with integrated access control.

9.5.1 Technology Options

Vendors extend security at both hardware and software levels to take care of the entire network. SSL and IP-VPN are the need of the hour for accommodating the risks in communicating data over the network. Intrusion Detection Prevention Systems also form an integral part of security that manages the network access control points. It is the intelligence of the network by sniffing the attacks.

9.5.2 Security

The current era is of even satellite offices, which means we are talking of vastly scattered computers connected to communicate; henceforth, security is obviously of paramount importance. Various ways can be employed for the same logical network security system.

9.5.3 Biometric controls:

A biometric control uses special sensors to examine fingerprints, retina scans, voice patterns, or other physical or behavioral characteristics. These systems can be used as the sole control method or integrated with other security controls dependent on keys or passwords. The technology is simple to operate and easy to install. It is mainly based on performance, cost, reliability, ease of use, and maintenance.

The biometric control measures are used for access control and authentication, including:

- Verifying the identity of an individual. It includes comparing the biometric data from the face, eyes, and fingerprints of the individual.
- Assessing the authenticity of an individual. It includes verifying that the biometric data from the individual's face, eyes, and fingerprints are genuine.
- Perform the authentication of a person from a biometric control system.
- The company can use both systems to detect the illegal use of a password. However, the retina patterns detection system has a higher detection rate than the voice detection system. Because eye movements and voice are not the same, each person has a different speed, speed, and length of eye movements. Moreover, eye movements and voice are various, and so the detection rate is different. For the same reason, the human eye detection system is the easiest to be detected. It has two ways of detection.
- It allows access to different types of information and documents of mechanisms (e.g., fingerprint, voice, and retina) but is generally characterized by identifying individuals based on physical characteristics or behavioral attributes. It is easy to operate and easy to install. It offers some significant advantages over key-based access controls.
- Biometric access is highly reliable and accurate. The system is self-verifying, and there is no need for a key and lock to be available for a user to access a building or room. Biometric controls are a cost-effective, environmentally friendly alternative to other conventional controls. It offers a low cost and a high level of security.
- Biometric controls are increasingly popular in the automotive industry. In particular, the automotive industry has begun to promote a more systematic approach to using biometrics to prevent potential risks and reduce fraud.

10. CONCLUSION

Record participates in an essential duty in the percentage of many cybercrimes and a weakness to cybercrime. Especially, information assortment, storing, study, and discussing both allow several cybercrimes and the substantial selection, storage space, use, and circulation of records without individuals' educated authorization and selection and essential lawful and protection defenses. The concern is that there is no trusted data on the complication; it is difficult to validate the raised electrical powers that the Regulation of Investigatory Powers Act has provided to the authorizations. These electrical powers will certainly likewise be unproductive in handling along with the complication of computer systems. Therefore, the worldwide negotiations attracted to work along with it are hazy that they are unproductive in handling along with difficulty. In addition, attacks, including viruses, worms, etc., hamper the system's productivity; thereby, machines work slowly. Also, a major portion of revenue is lost because of a lack of trust, confidentiality, and hesitation. The expanse of financial loss can be well understood because share trading is also done through the internet; a small theft can shock a whole economy. Nowadays, most firms rely on their information systems for their overall functionality. If the IS of a company is spoofed, the trust and value that the company enjoys would be lost. Henceforth a detailed assessment for the security of IS should be done for identifying threats to security and evaluating their severity. When a web page or website is hacked, the hacked may have changed its logic, affecting the user's confidence and discouraging it from using it in the long term. Concluding can say that cybercrime is a serious repercussion of networking is unavoidable when we talk about the whole world as a marketplace. When we say that cybercrime is a serious threat to the company, a chill runs down; now imagine when we talk about national security. So the need of the hour is to have an effective and efficient system that saves the most important resource and data. Usually, businesses take Cybersecurity as an overhead until cyber-loss occurs. It is a need to have a complete solution to cyber threats.

11. REFERENCES

[1] Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202-209.

[2] Underground: Are You Policing Computer Crimes?, Sloan Management Review (Summer 1989): 35-43 [

[3] Sprecher, R., and M. Pertl, 1988, Intra-Industry Effects of the MGM Grand Fire, Quarterly Journal of Business and Economics, 27: 96-16.

[4] Jaishankar, K. (2007). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 7-9.

[5] Sinrod, E. J., & Reilly, W. P. (2000). Cyber-crimes: A practical approach to the application of federal computer crime laws. Santa Clara Computer & High Tech. LJ, 16, 177.

[6] Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552.

[7] Bitter, D.A. Elizondo, T. Watson, (2010) "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection", IEEE World Congress on Computational Intelligence (WCCI 2010), pp. 949 – 954.

[8] Y. Chen, (2008) "NeuroNet: Towards an Intelligent Internet Infrastructure", 5th IEEE Consumer Communications and Networking Conference (CCNC 2008), pp. 543 547.

[9] L. Ondrej, T. Vollmer, M. Manic, (2009) "Neural Network Based Intrusion Detection System for Critical Infrastructures", Proceedings of International Joint Conference on Neural Networks, pp. 1827 1834.

[10] F. Barika, K. Hadjar, N. El-Kadhi, (2009) "Artificial neural network for mobile IDS solution", Security and Management, pp. 271–277.

[11] Iftikhar, B.A. Azween, A. S. Alghamdi, (2009) "Application of artificial neural network in detection of dos attacks," Proceedings of the 2nd ACM international conference on Security of information and networks, pp. 229–234.

[12] H. Wu, (2009) "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Systems with Applications, Vol. 36, Issue. 3, Part: 1, pp. 4321–4330.

[13] P. Salvador, A. Nogueira, U. Franca, R. Valadas, (2009) "Framework for Zombie Detection using Neural Networks", Fourth International Conference on Internet Monitoring and Protection (ICIMP '09), pp.14 – 20.

[14] S. T. F. Al-Janabi, H. A. Saeed, (2011) "A Neural Network Based Anomaly Intrusion Detection System", Developments in E-systems Engineering (DeSE), pp. 221 – 226.

[15] K. Barman, G. Khataniar, (2012) "Design Of Intrusion Detection System Based On Artificial Neural Network And Application Of Rough Set", International Journal of Computer Science and Communication Networks, Vol. 2, No. 4, pp. 548-552. [

[16] N. C. Rowe, "Counterplanning Deceptions To Foil Cyber-Attack Plans", Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, Information Assurance Workshop, pp. 203 210.

[17] X. Gou, W. Jin, D. Zhao, (2006) "Multi-agent system for worm detection and containment in metropolitan area networks", Journal of Electronics, Vol. 23, No. 2, pp. 259-265.

[18] L. Phillips, H. Link, R. Smith, L. Weiland, (2006) Agent-Based Control of Distributed Infrastructure Resources, U.S. Department of Energy, Sandia National Laboratories, USA.

[19] I. Kotenko, A. Ulanov, (2007) "Multi-Agent Framework fo Simulation of Adaptive Cooperative Defense Against Internet Attacks", International Workshop on Autonomous Intelligent Systems: Agents and Data Mining (AIS-ADM 2007), Springer-Verlag, Berlin Heidelberg, vol. 4476, pp. 212228.

[20] Herrero, M. Corchado, A. Pellicer, A. Abraham, (2007) "Hybrid multi agent-neural network intrusion detection with mobile visualization", Innovations in Hybrid Intelligent Systems, Vol. 44, pp. 320 328.

[21] H. Fu, X. Yuan, K. Zhang, X. Zhang, Q. Xie, (2007) "Investigating Novel Immune-Inspired MultiAgent Systems for Anomaly Detection", The 2nd IEEE Asia-Pacific Service Computing Conference, pp. 466 472.

[22] Edwards, S. Simmons, N. Wilde, (2007) "Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture", IEEE International Conference on System of Systems Engineering (SoSE '07), pp. 1 – 6.

[23] Kotenko, A. Konovalov, A.Shorov, (2010) "Agent-Based modeling and Simulation of Botnets and Botnet Defence", Proceeding of Conference on Cyber Conflict (CCD COE).

[24] X. Ye, J. Li, (2010) "A Security Architecture Based on Immune Agents for MANET", International Conference on Wireless Communication and Sensor Computing (ICWCSC 2010), pp. 1 5.

[25] D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, (2010) "An Integrated Security System of Protecting Smart Grid against Cyber Attacks", Innovative Smart Grid Technologies (ISGT), pp. 1 7.

[26] Doelitzscher, C. Reich, M. Knahl, N. Clarke, (2011) "An Autonomous Agent Based Incident Detection System for Cloud Environments," IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), pp.197-204.

[27] F. Shosha, P. Gladyshev, W. Shinn-Shyan, L. Chen-Ching, (2011) "Detecting cyber intrusions in SCADA networks using multi-agent collaboration," 16th International Conference on Intelligent System Application to Power Systems (ISAP), pp.1-7.

[28] Ionita, L. Ionita, (2013) "An agent-based approach for building an intrusion detection system," 12th International Conference on Networking in Education and Research (RoEduNet), pp.1-6. 36 International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015

[29] Williams, M. L., & Levi, M. (2017). Cybercrime prevention. Handbook of crime prevention and community safety, 454.

[30] Alazab, M., & Broadhurst, R. (2017). An analysis of the nature of spam as cybercrime. In Cyber-Physical Security (pp. 251-266). Springer, Cham.

[31] Wall, D. S. (2004). Digital realism and the governance of spam as cybercrime. European journal on criminal policy and research, 10(4), 309-335.

[32] Alazab, M., & Broadhurst, R. (2016). Spam and criminal activity. Trends and issues in crime and criminal justice, (526), 1-20.

[33] Alazab, M., & Broadhurst, R. (2015). The role of spam in cybercrime: data from the Australian cybercrime pilot observatory. In Cybercrime Risks and Responses (pp. 103-120). Palgrave Macmillan, London.

[34] Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 149-164). Syngress.

[35] Clayton, R., Moore, T., & Christin, N. (2015, June). Concentrating Correctly on Cybercrime Concentration. In WEIS.

[36] Alazab, M., Layton, R., Broadhurst, R., & Bouhours, B. (2013, November). Malicious spam emails developments and authorship attribution. In 2013 fourth cybercrime and trustworthy computing workshop (pp. 58-68). IEEE.

[37] Trefan, L., Harris, C., Evans, S., Nuttall, D., Maguire, S., & Kemp, A. M. (2018). A comparison of four different imaging modalities–Conventional, cross polarized, infra-red and ultra-violet in the assessment of childhood bruising. Journal of forensic and legal medicine, 59, 30-35.

[38] Tiago, M. T. P. M. B., & Verissimo, J. M. C. (2014). Digital marketing and social media: Why bother?. Business horizons, 57(6), 703-708.

[39] Vieira, K., Schulter, A., Westphall, C., & Westphall, C. (2010). Intrusion detection for grid and cloud computing. IT Professional, 12(4), 38-43.

[40] Welsh, B. C., & Farrington, D. P. (2004). Surveillance for crime prevention in public space: Results and policy choices in Britain and America. Criminology & Public Policy, 3(3), 497-526.

[41] Williams, F. P. (2009). Statistical concepts for criminal justice and criminology. Upper Saddle River, NJ: Pearson Prentice Hall.

[42] Willison, R. (2000). Understanding and addressing criminal opportunity: the application of situational crime prevention to IS security. Journal of Financial Crime, 7(3), 201-210.

[43] Willison, R. (2006). Understanding the perpetration of employee computer crime in the organizational context. Information and Organization, 16(4), 304-324.

[44] Wilsem, J. V. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. Journal of Contemporary Criminal Justice, 29(4), 437-453.

[45] Wortley, R. (2001). Classification of techniques for controlling situational precipitators of crime. Security Journal, 14(4), 63-82.

[46] Wright, M. F., & Li, Y. (2013). The association between cyber victimization and subsequent cyber aggression: The moderating effect of peer rejection. Journal of Youth and Adolescence, 42(5), 662- 674.

[47] Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280.

[48] Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. Center for Strategic and International Studies.

[49] Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. Deviant Behavior, 31(5), 381-410.

[50] Pogarsky, G. (2002). Identifying "deterrable" offenders: Implications for research on deterrence. Justice Quarterly, 19(3), 431-452.

[51] Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. Crime Prevention and Community Safety, 12(2), 99-118.

[52] Schneider, S. (2014). Crime prevention: Theory and practice. Boca Raton, FL: CRC Press.

[53] Shariati, A., & Guerette, R. T. (2017). Situational Crime Prevention. In B. Teasdale & M.S. Bradley (Eds.) Preventing Crime and Violence pp. 261-268.

[54] Skopik, F., Bleier, T., & Fiedler, R. (2012). Information management and sharing for national cyber situational awareness. In H. Reimer, N. Pohlmann, & W. Schneider (Eds.) ISSE 2012 Securing Electronic Business Processes pp. 217-227