

CYBER SECURITY (PS02EMCA37)

Unit-1 : Introduction to Cybercrime

- Cybercrime: Definition And Origins Of The World
- Cybercrime and Information Security
- Who Are Cybercriminals?
- Classifications of Cybercrimes
- Cybercrime: The Legal Perspectives
- Cybercrimes: An Indian Perspectives
- Cybercrime and the Indian ITA-2000
- Cyber Offences: How Criminals Plan the Attack
- Social Engineering
- Cyberstalking
- Botnets

Cybercrime: Definition & Origins of the World

- ❖ The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education.
- ❖ There are two sides to a coin. Internet also has it's own disadvantages is Cyber crime- illegal activity committed on the internet.

Cybercrime: Definition & Origins of the World

- Crime committed using a computer and the internet to steal data or information.
- Malicious programs.



Cybercrime

- The first recorded cybercrime took place in the year 1820.
- In 1820, JosephMarie Jacquard, a textile manufacturer in France, produced the loom.
- Device allowed the repetition of a series of steps in the weaving of special fabrics.
- This resulted in a fear amongst Jacquard's employees that their traditional employment were being in problem.
- They committed acts of sabotage to discourage Jacquard from further use of the new technology.
- **This is the first recorded cyber crime!**

Alternative definitions for computer crime

- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution
- Any traditional crime that has developed a new dimension through the use of a computer, and misuses that have come into being because of computers.
- Any financial dishonesty that takes place in a computer environment.
- Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom

Alternative definitions for computer crime

- “Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that target the security of computer systems and the data processed by them”.
- **Cybercrime** can be called as
 - Computer crime,
 - E-crime,
 - Internet crime,
 - High-tech crime.....

Cybercrime Definitions

- A crime committed using a computer and the Internet
 - To steal a person's identity(identity theft) or
 - Sell illegal goods or
 - Stalk (harass) victims or
 - Disrupt operations with malicious programs.

Cybercrime and information security

- Lack of information security give rise to cybercrime
- **Cybersecurity : Means protecting**
 - Information
 - Devices
 - Computer resources
 - Communication devices &
 - Information stored therein**from unauthorized**
 - Access
 - Disclosure
 - Modification
 - Deletion

Challenges for securing data in business perspective

- Cybercrime occupy an important space in information security due to their power.
- Most organizations do not incorporate the cost of the vast majority of computer security incidents into their budget.
- The difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost.
- Financial losses may not be detected by the victimized organization in case of Insider attacks : such as leaking customer data

Who are Cybercriminals?

- **Are those who conduct acts such as:**
 - Credit card fraud
 - Cyberstalking
 - Defaming another online
 - Gaining unauthorized access to computer systems
 - Ignoring copyrights
 - Software licensing and trademark protection
 - Overriding encryption to make illegal copies
 - Software piracy
 - Child pornography
 - Stealing another's identity to perform criminal acts



Categorization of Cybercriminals

- Type 1: Cybercriminals- hungry for recognition
 - **Hobby hackers**
 - A person who enjoys exploring the limits of what is possible, in a spirit of playful cleverness. May modify hardware/ software
 - **IT professional(social engineering):**
 - Ethical hacker
 - **Politically motivated hackers :**
 - Promotes the objectives of individuals, groups or nations to leaking any organization information.
 - Common targets include Government agencies, multinational corporations.
 - **Terrorist organizations**
 - Cyberterrorism : Use the internet attacks in terrorist activity
 - Large scale disruption of computer networks , personal computers attached to internet.

Categorization of Cybercriminals

- Type 2: Cybercriminals- Not interested in recognition
 - **Psychological perverts**
 - Deviates from normal behavior. Misuse of information like recording , modifying and sharing of illegal videos / photos and text.
 - **Financially motivated hackers**
 - Make money from cyber attacks
 - Attacks may be like phishing, information theft, spam and blackmail.
 - **State-sponsored hacking (national espionage, sabotage)**
 - It's goal is to access the information for long term.
 - Extremely professional groups working for governments
 - Have ability to worm into the networks of the media, major corporations, defense departments

Categorization of Cybercriminals

- Type 3: Cybercriminals- The insiders
 - Dissatisfied or former employees seeking revenge
 - Competing companies using employees to gain economic advantage through damage and/ or theft.

Motives behind cybercrime

- Desire to gain power
- Publicity
- Desire for revenge
- A sense of adventure
- Looking for thrill to access forbidden information
- Destructive mindset
- Desire to sell network security services

Tow Types of Attacks

Techno – vandalism: Passive attack

- Techno Vandalism is a term used to describe a hacker or cracker who breaks into a computer system with the sole **intent of damaging and or destroying its contents.**
- Techno Vandals can set up 'sniffers' on the Internet to locate soft (insecure) targets and then execute a various commands towards a ports.
- The best weapon against such attacks is a firewall which will hide and protect organization's presence on the Internet.

Tow Types of Attacks

Techno- crime : Active attack

- Techno Crime is the term used by law enforcement agencies to denote criminal activity which uses (computer) technology, not as a tool to commit the crime, but as the subject of the crime itself.
- Techno Crime is usually pre-meditated and results in the deletion, corruption, alteration, theft or copying of data on an organization's systems.
- Techno Criminals will usually probe their prey(victim) system for weaknesses and ensure that pseudonym(false name) identity is known.

Classification of cybercrimes

1. Cybercrime against an individual
2. Cybercrime against property
3. Cybercrime against organization
4. Cybercrime against Society
5. Crimes originating from Usenet newsgroup

1.Cybercrime against an Individual

- Email spoofing
- Phishing
- Spamming
- Cyber defamation
- Cyberstalking and Harassment
- Computer sabotage
- Pornographic offenses
- Password sniffing

2.Cybercrime against property

- Credit card / Debit card frauds
- Intellectual property(IP) crimes
- Internet time theft

3.Cybercrime against organization

- Unauthorized accessing of computer
- Password sniffing
- Denial-of-service attacks
- Virus attack / spreading of viruses
- E-Mail bombing / mail bombs
- Salami attack / Salami technique
- Logic bomb
- Trojan Horse
- Data diddling
- Industrial spying/ industrial espionage
- Computer network intrusions
- Software piracy

4.Cybercrime against Society

- Forgery
- Cyberterrorism
- Web jacking

5.Crimes originating from Usenet newsgroup

- Usenet groups may carry very offensive, harmful, inaccurate material
- Postings that have been mislabeled or are false in another way
- Hence service at your own risk

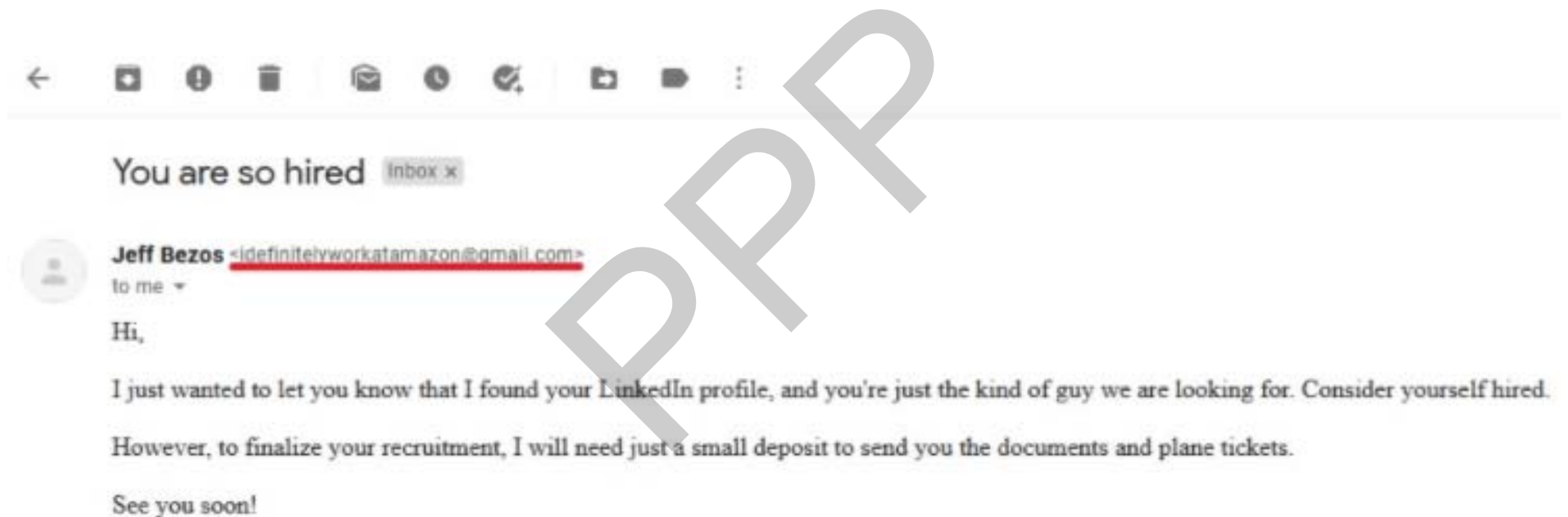
E-Mail Spoofing



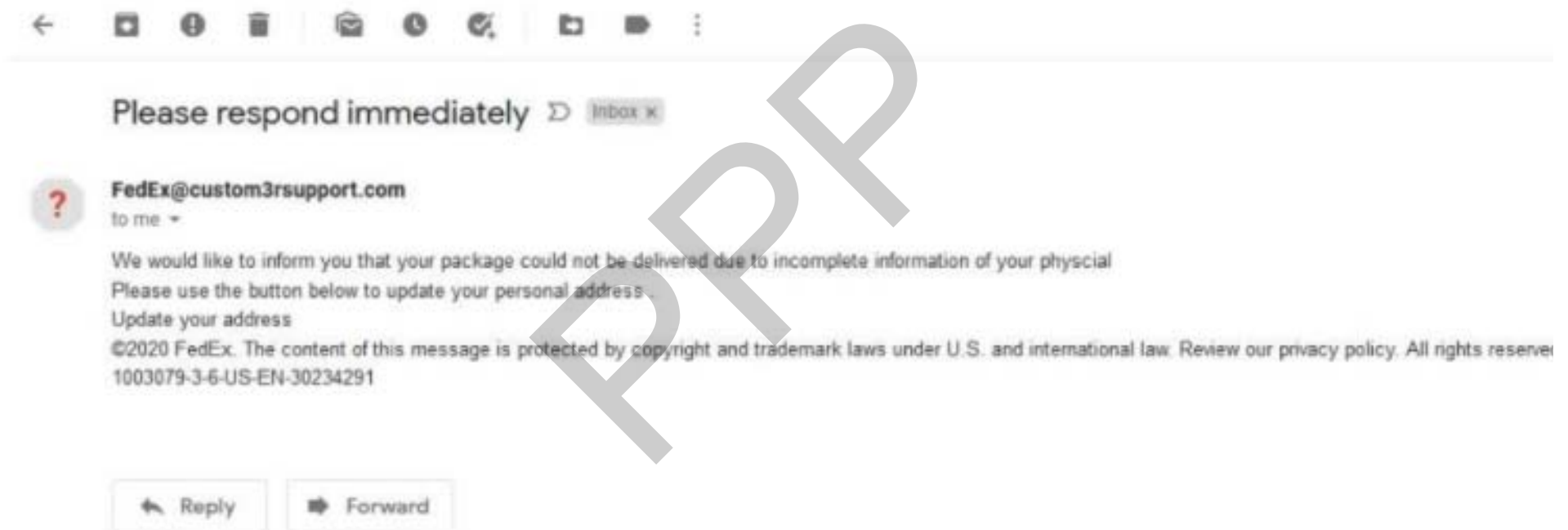
E-Mail Spoofing

- Spoofed email is one that appears to originate from one source but actually has been sent from another source.
- To send spoofed e-mail, senders insert commands in headers that will alter message information.
- Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.
- Spoofed e-mail may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information and which can be used for a criminal purposes.
- E.g. All Seagate employees received emails impersonating their CEO requesting their Wages forms. Most employees believed that it was a genuine internal business email and, unbeknownst to them, leaked their annual wages.

E-Mail Spoofing via Display Name




E-Mail Spoofing via lookalike domain



How to Identify E-Mail Spoofing

- Need to look at the **full email header**.
- It contains all the critical components of every email:
 - **From, To, Date** and **Subject**.
- At the bottom of message ... click on **View raw message** or If you go to “**Show Original**”, you can see that **SPF** is indicated as **SOFTFAIL**, and **DMARC** is indicated as **FAIL**. This is enough to call out the email as spoofed.

Original message

Message ID	<20200819071152.A0133270C7@localhost>
Created on:	19 August 2020 at 10:11 (Delivered after 1 second)
From:	Jeff Bezos <jeff.bezos@amazon.com>
To:	justinas.mazura@cybernews.com
Subject:	Job offer
SPF:	SOFTFAIL with  Learn more
DMARC:	'FAIL' Learn more

How to Stop E-Mail Spoofing

- To stop email spoofing by choosing a secure email provider and practicing good cybersecurity hygiene:
 - **Make sure that your email password is strong and is complex enough.** That way, it will be harder for cybercriminals to get into your account and send misleading messages to your contacts.
 - **Inspect the email headers, especially when someone asks to click on a link.** Spoofed emails made by talented attackers can be identical to the genuine ones. They can seem indistinguishable even if you're a long-time user.

Phishing

- An attack in which a targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally information, banking information, credit card / debit card details and passwords.
- Phishing messages look authentic and attempt to get users to reveal their personal information.
- E.g. User finds a message from the bank threatening him/her to close the bank account if he/she does not reply immediately. It is difficult to conclude that it is a fake message / email / call.

Phishing

Identify Your Verification - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Google mailto:syntax

Address http://paypal-supports.com/support/update.html Go Links

PayPal® [Sign Up](#) | [Log Out](#) | [Help](#)

Welcome Send Money Request Money Merchant Tools Auction Tools

Personal Account Identity Verification - Just 1-Page!

Your Profile Information - Enter your name as it appears on your credit card or bank account.

First Name:

Last Name:

Address 1:

Address 2: (optional)

City:

State:

Zip: (5 or 9 digits)

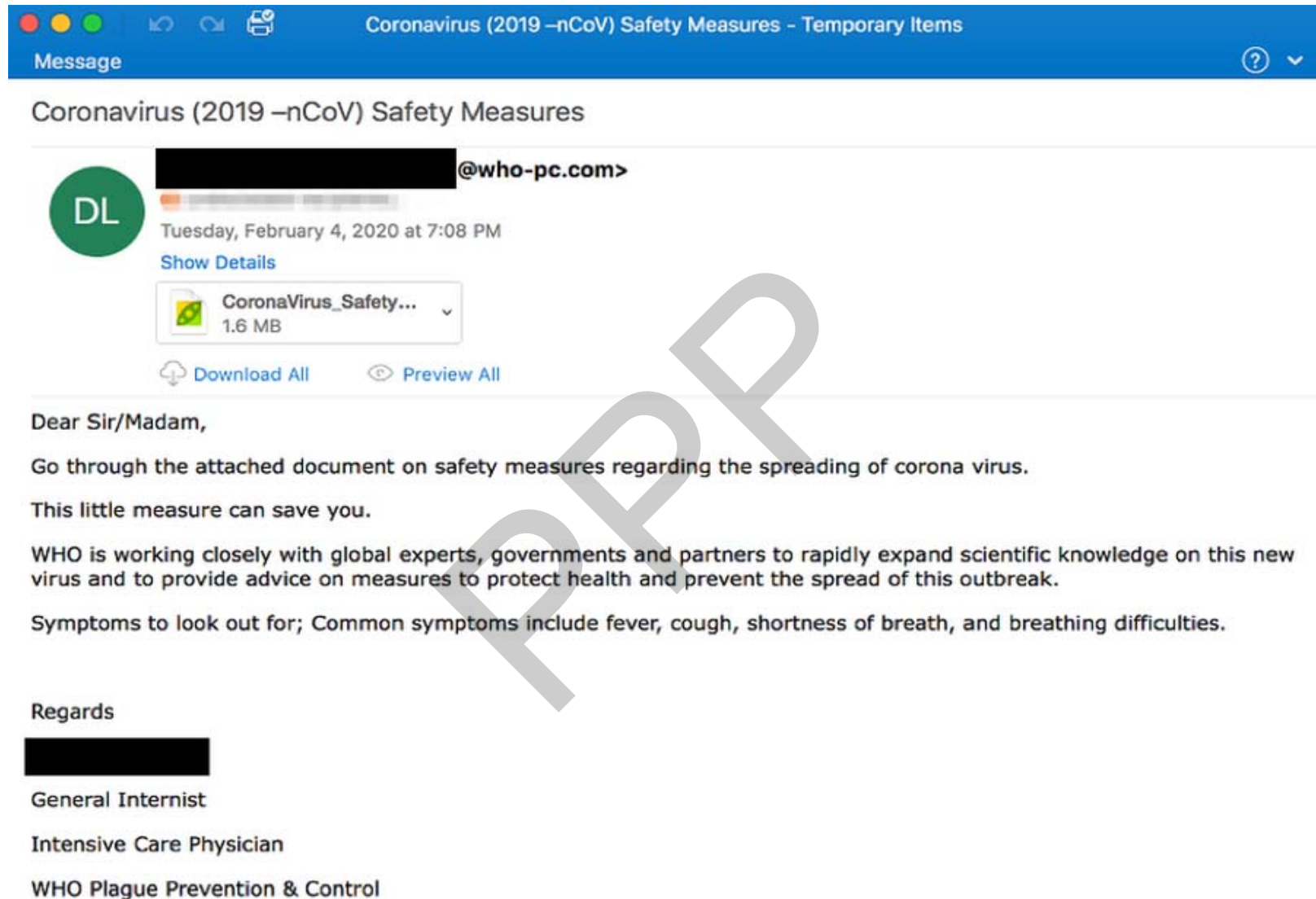
Country:

Home Telephone:

Work Telephone: (optional)

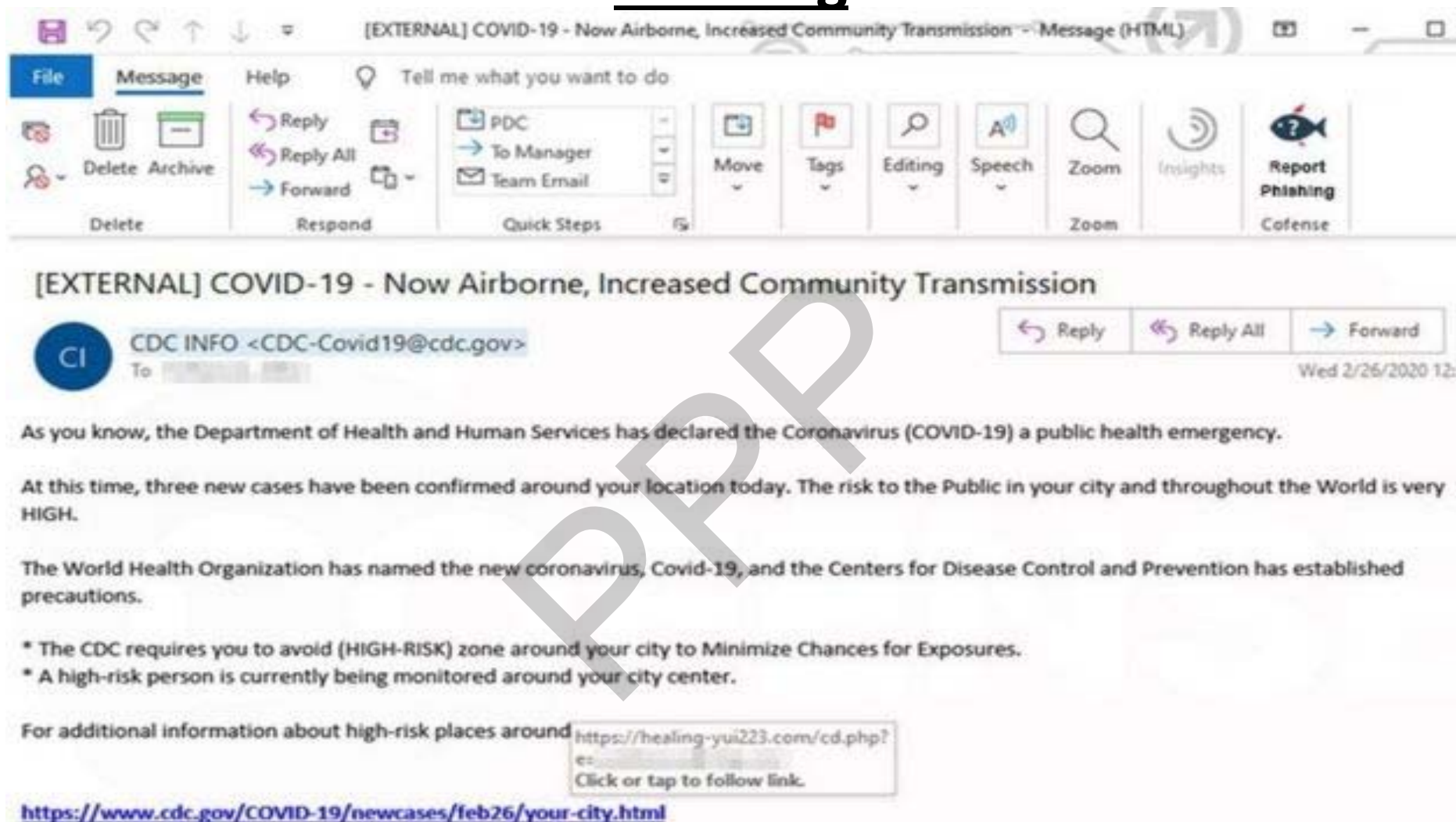
- It is the act of attempting to acquire information such as usernames, passwords, and credit card details by indirect as a trustworthy entity in an electronic communication.

Phishing



- Attachment file does not contains any useful advice. It is keylogger software to records keystroke.

Phishing



- The message provides a link for information regarding high risk places around you. It diverts to fake website and ask for Microsoft login and password & then redirect to original website of Centers for Disease Control and Prevention (CDC) website.

Phishing



#1 IN INDIA

Jio

#2 IN THE WORLD

JIO अपने सभी यूजर को दे रहा है

399 RECHARGE FREE

आप सभी को मिलेगा 399 रिचार्ज पैक फ्री और डेली 2GB फ्री

पूरे 3 महीनो के लिए फ्री

जल्द रिचार्ज करे ऑफर सीमित समय के लिए है

आपका नाम:

यहाँ अपना नाम लिखिए....

आपका Jio नंबर:

मोबाइल नंबर लिखिए...

How to Stop Phishing

- In a doubtful email, do not click on any links listed in the email message, and do not open any attachments contained
- Do not enter personal information in a pop-up screen. Legitimate companies, agencies, and organizations don't ask for personal information via pop-up screens.
- Rotate passwords regularly
- Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker.
- Browser add-ons and extensions can be enabled on browsers that prevent users from clicking on malicious links.
- Use an SSL Certificate to secure all traffic to and from your website. This protects the information being sent between your web server and your customers' browser

Spamming

- **Spam** is misuse of electronic messaging systems to send unwanted bulk messages broadly.
- People who create electronic spam : **spammers**
- Spamming may be
 - E-Mail Spam
 - Instant messaging spam
 - Usenet group spam
 - Web search engine spam
 - Spam in blogs, wiki spam
 - Online classified ads spam
 - Mobile phone messaging spam
 - Internet forum spam
 - Social networking spam
 -

Spamming

- Spamming is difficult to control because
 - Advertisers have no operating costs beyond the management of their mailing lists.
 - It is difficult to hold senders accountable for their mass mailings

Search engine spamming

- Alteration or creation of a document with the intent to mislead an electronic catalog or a filing system
- Some web authors use “destructive techniques” to ensure that their site appears more frequently or higher number in returned search results.
- **Solution:** Those who continuously Spam the search engines permanently exclude them from the search index

Avoid web publishing techniques

- Repeating keywords
- Use of keywords that do not relate to the content on the site
- Use of fast meta refresh
 - change to the new page in few seconds.
- Redirection
- IP cloaking:
 - When a person hides their **IP** address.
 - People want to avoid being tracked and monitored. This is achieved by accessing the internet through a second computer called a proxy server.
- Use of colored text on the same color background
- Tiny text usage : Text is not visible by human eye.
- Duplication of pages with different URLs
- Hidden links

Cyberdefamation

- **Cyber defamation** occurs when a computer connected to the internet is used as a tool, or a medium to **defame** a person or an entity.
- **E.g.** if a customer blamed the restaurant owner of food poisoning even though it was not actually the restaurant's food that caused them to be ill. If the customer shared the false information with other customers, the owner could have grounds for a **defamation** lawsuit.
- **There are two types of defamation**
 - **libel** : It is published defamation
 - **E.g.** when someone publishes in the newspaper that a person is a thief, even though this is false. The person can sue in an admiralty court.
 - **Slander** : It is fleeting, mostly verbal.
 - **E.g.** Claiming a Manager of organization harass the employees, when it is false, in an attempt to harm his or her reputation.



Cyberdefamation

PPR

Cyberdefamation cases

- In first case of cyber defamation in India (14 dec 2009),
 - Employee of a corporate defamed its reputation was sending offensive and defamatory emails against the company and its managing director.
 - In this case the Court (Delhi court) had controlled the criminal from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails.
- **Other defamation cases:**
 - A malicious customer review by a competitor could destroy a small business.
 - A false claim of dishonesty on a social networking site could destroy a marriage.



Cyberdefamation cases

- The case involves content in the form of videos about the book on Swami Ramdev (popularly known as Baba Ramdev) titled “Godman to Tycoon – The Untold Story of Baba Ramdev” by Priyanka Pathak Narain.
- Such book had been previously controlled from being published by the Delhi High Court which held that it contained prima-facie defamatory content on Baba Ramdev.
- The petitioners, Baba Ramdev and Patanjali Ayurved Ltd., asked the court to issue a global take down order for the defamatory content in question to Facebook, Google, YouTube, Twitter and other Internet intermediaries.
- The Internet platforms removed the content from their India-specific domains, but refused to remove it globally.
- Judge ruled that as long as either the content is uploaded from India or the information/data is located in India on a computer resource, Indian courts would have jurisdiction to pass global bans.

Internet Time Theft



- Occurs when an unauthorized person uses the Internet hours paid for by another person
- The person get access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means
- And uses the internet without the other person's knowledge
- This theft can be identified when Internet time is recharged often or may be used on off days and times.

Salami attack/ salami technique

- Are used for committing financial crimes.
- The alterations made are so insignificant that in a single case it would go completely unnoticed.
- Example: A bank employee inserts a program, into the bank's serve, that deduces a small amount from the account of every customer every month.
- The unauthorised debit goes unnoticed by the customers, but the employee will make a sizable amount every month.

Salami attack: real life examples

- Bank employee write a malicious program into bank server

Solution:

- The banking system should initiate both SMS and email message to alert their customers on any transaction that occurs and also advise the customers to immediately report any unaware money reduction no matter how small it is, so the bank can update their security system

Cyber Attacks : Data Diddling



- It is a practice of changing of data before or during entry into the computer system.
- E.g. Account executives can change the employee time sheet information of employees before entering to the HR payroll application.
- E.g. DA is changed during pay calculation. Once salary transferred to his account, salary field is replaced by actual salary in the report.

To Stop Data Diddling

- To deal with this type of crime, a company must implement policies and internal controls.
- This may include performing regular audits, using software with built-in features to combat such problems, and supervising employees.

Forgery

- The act of forging something, especially the unlawful act of counterfeiting a document or object for the purposes of fraud or deception.
- Something that has been forged, especially a document that has been copied or remade to look like the original.
- Counterfeit
 - currency notes,
 - postage,
 - revenue stamps,
 - marksheets, etc.,using sophisticated computers, printers and scanners.

Web jacking



- This term is derived from the term hi jacking.
- In these kinds of offences the hacker gains access and control over the web site of another.
- He / She may even change the information on the site.
- The first stage of this crime involves “password sniffing”.
- The actual owner of the website does not have any more control over what appears on that website.
- This may be done for fulfilling political objectives or for money

How to stop Web jacking



- **Protect the Browser**

- Install browser plugins, which prompt users to apply javascript actions on sites they visit, as well as specify trusted domains.

- **Firewall**

- It will prevent someone from interjecting your site and inputting code

Industrial spying/ Industrial Espionage

- Industrial espionage is the hidden and illegal practice of investigating competitors to gain a business advantage.
- The target of investigation might be a trade secret such as a
 - Proprietary product specification or formula, or
 - Information about business plans.
- In many cases, industrial spies are simply seeking any data that their organization can exploit to its advantage.

Hacking

Every act committed toward breaking into a computer and/ or network is hacking and it is an offense.

Purpose

- Greed
- Power
- Publicity
- Revenge
- Adventure
- Desire to access forbidden information
- Destructive mindset

Hacking

- M.I.T. engineers in the 1950s and 1960s first popularized the term and concept of hacking.
- "hacks" effected by these hackers were intended to be harmless technical experiments and fun learning activities.
- Later, outside of M.I.T., others began applying the term to less honorable pursuits.
- E.g. Some hackers in the U.S. experimented with methods to modify telephones for making free long-distance calls over the phone network illegally.
- As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hackers and hacking.

Hacking

- Hackers write or use ready-made computer programs to attack the target computer.
- They possess the desire to destruct and they get enjoyment out of such destruction.
- Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

Cracking vs. Phrackers

- Malicious attacks on computer networks are officially known as *cracking* ,
- When someone targeting phones for malicious activity are known as Phrackers.

Types of hackers

- **Black Hats:** Criminal Hackers.
 - Possess desire to destruction
 - Hack for personal monetary gains : Stealing credit card information, transferring money from various bank accounts to their own account, force money from corporate giant by threatening.
- **White Hats:** Ethical Hackers.
 - Network Security Specialist.
 - Identify the security weaknesses in websites and networks.
 - Provide the proper guidelines and solutions for protection of hardware and software resources.

Real life case: Dec 2009

NASA site hacked via SQL Injection

- Two NASA sites were hacked by an individual wanting to demonstrate that the sites are vulnerable to [SQL injection](#).
- The researcher, using the alias "c0de.breaker," used [SQL injection](#) to hijack the sites.
- SQL injection is an attack process where a hacker adds additional SQL code commands to a page request and the web server then tries to execute those commands within the backend database
- The NASA hack yielded the credentials of some 25 administrator accounts.
- The researcher also gained access to a web portal used for managing and editing those websites.
- In this particular case, the researcher found the vulnerabilities, made NASA aware of them, then published findings after the websites had been fixed

Online frauds



- Fraud that is committed using the internet is “online fraud.” Online fraud can involve financial fraud and identity theft.
- Online fraud comes in many forms.
 - **Viruses** that attack computers with the goal of retrieving personal information, to email schemes that attraction victims into wiring money to fraudulent sources,
 - “**phishing**” emails that purport to be from official entities (such as banks or the Internal Revenue Service) that solicit personal information from victims to be used to commit identity theft

Online frauds



- Online fraud comes in many forms.
 - **To fraud on online** auction sites (such as Ebay) where perpetrators sell fictional goods.
 - **E-Mail spoofing** to make the user to enter the personal information : financial fraud
 - **Illegal intrusion:** log-in to a computer illegally by having previously obtained actual password. Creates a new identity fooling the computer that the hacker is the genuine operator. Hacker commits innumerable number of frauds.
 - **Lottery frauds** are letters or E-mails that inform the recipient that he/she has won a prize in lottery. To get the money, the recipient provide credential details and it should be used for frauds and scams.

Online frauds



- To safe from online frauds.
 - Install Antivirus like McAfee, Sophos, Symantec, Quick Heal etc.
 - To be alert and careful about email containing an embedded link, with a request for you to enter secret details.
 - Do not provide sensitive information like bank details, credit card or debit card details, without confirming to the authority person or organization.

Pornographic offenses: Child pornography

Means any visual description includes :

1. Any photograph that can be considered obscene and/ or unsuitable for the age of child viewer.
2. Obscene Film ,video & picture
3. Obscene Computer generated image or picture

Software piracy

- Theft of software through the illegal copying of genuine programs or the forging and distribution of products intended to pass for the original.
- Illegal downloads from internet
- Those who buy pirated software have a lot to lose:
 - Getting untested software that may have been copied thousands of times over
 - May potentially contain hard-drive-infecting viruses
 - No technical support in the case of software failure
 - No warranty protection,
 - No legal right to use the product, etc.



Computer sabotage



- Computer sabotage involves deliberate attacks intended to disable computers or networks for the purpose of disrupting commerce, education and recreation for personal gain, committing espionage, or facilitating criminal plans.
- **Through** viruses, worms, logic bombs
- Chernobyl virus
 - **The Chernobyl virus is a computer virus with a potentially devastating payload that destroys all computer data when an infected file is executed.,**
- Y2K virus

Computer sabotage



- **Chernobyl virus**
 - The Chernobyl virus is a computer virus with a potentially devastating payload that destroys all computer data when an infected file is executed.
- **Y2K virus**
 - Y2K bug, also called Year 2000 bug or Millennium Bug, a problem in the coding of computerized systems that was projected to create havoc in computers and computer networks around the world at the beginning of the year 2000



E-mail bombing/mail bombs

- Sending a large number of E-mails to the victim to crash victim's E-mail account or to make victim's mail servers crash.
- Computer program can be written to instruct a computer to do such tasks on a repeated basis.
- It Can overwhelm the recipient's personal account and potentially shut down the entire system.



Usenet Newsgroup as the Source of Cybercrimes

- Usenet is a popular means of sharing and distributing information on the Web with respect to specific topic or subjects.
- It is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics.
- It may be used for
 - obscene materials
 - Selling of pirated softwares
 - Distribution of hacking software.

Computer network intrusions



- An intrusion to computer network from any where in the world and steal data, plant viruses, create backdoors, insert trojan horse or change passwords and user names.
- An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
- The practice of strong password

Password sniffing

- Password sniffers are programs that monitor and record the name and password of network users as they login, exposing security at a site.
- Through sniffers installed, anyone can impersonate an authorized user and login to access restricted documents.



Credit card frauds



- **Credit card fraud** is a wide-ranging term for [theft](#) and [fraud](#) committed using or involving a [payment card](#), such as a [credit card](#) or [debit card](#), as a fraudulent source of funds in a transaction.
- The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.
- Payment Card Industry Data Security Standard (PCI – DSS) is a set of regulations developed jointly by the leading card schemes to prevent cardholder data theft and to help against credit card fraud.

Identity theft

- Identity theft is a fraud involving another person's identity for an illegal purpose.
- The criminal uses someone else's identity for his/ her own illegal purposes.
- Phishing and identity theft are related offenses
- Examples:
 - Fraudulently obtaining credit
 - Stealing money from victim's bank account
 - Using victim's credit card number
 - Establishing accounts with utility companies
 - Renting an apartment
 - Filing bankruptcy using the victim's name



Cybercrime: The Legal Perspectives

- **Computer-related crime** was defined in the broader meaning as: any illegal act for which knowledge of computer technology is essential for a successful prosecution.

Cybercrime:

- Outcome of “globalization.”
- Globalized information systems accommodate an increasing number of transnational offenses (International offenses).

This problem can be resolved in two ways:

1. Divide information systems into segments bordered by state boundaries. (Cross border flow of information)
 2. Incorporate the legal system into an integrated entity eliminating these state boundaries
- Apparently the first way is unrealistic.

Cybercrimes: An Indian Perspective

- India has the fourth highest number of internet users in the world. (In 2006)
 - 45 million internet users in India
 - 37% - in cybercafes
 - 57% are between 18 and 35 years
- Majority of offenders were under 30 years.
 - About 46% cybercrime cases were related to incidents of cyber pornography
 - In over 60% of cases, offenders were between 18 and 30 years.
- In 2006, 142 cases were registered under IT Act
- In 2007, 217 cases were registered under IT Act
- Increase of 52.8% in 2007 over 2006.
 - 22.3% cases (49 out of 217 cases) from Maharashtra
 - 18.4% cases (40 out of 217 cases) from Karnataka ,
 - 17.5% cases (38 out of 217 cases) from Kerala and
 - 7.4% cases (16 out of 217 cases) from Andhra Pradesh and Rajasthan

Hacking and the Indian Law(s)

- Cyber crimes are punishable under two categories
 - ITA 2000 (**Information Technology Act, 2000**)
 - IPC (**Indian Penal Code**)
- **In 2006**, 142 cases of cybercrime were registered under the IT Act & 311 cases were recorded under the IPC.
- **In 2007**, 207 cases of cybercrime were registered under the IT Act & 339 cases were recorded under the IPC.

Cybercrime & Indian ITA 2000

- The first step toward the Law relating to E-Commerce at international level to regulate an alternative form of commerce and to give legal status in the area of E-Commerce.

Section	Crime	Punishment
Sec. 43	Damage to computer system etc.	Compensation for Rs. 1 crore.
Sec. 66	Hacking (with intent or knowledge)	Fine of Rs. 2 Lacs & imprisonment for 3 Yrs.
Sec. 67	Publication of obscene material in electronic form.	Fine of Rs. 1 Lacs & imprisonment for 5 Yrs & double on second offence.
Sec. 68	Not complying with directions of controller	Fine of Rs. 2 Lacs & imprisonment for 3 Yrs.

Cybercrime & Indian ITA 2000

Section	Crime	Punishment
Sec. 70	Attempting or securing access to computer of another person without his/her knowledge.	imprisonment for 10 Yrs.
Sec. 72	Attempting or securing access to computer for breaking confidentiality of the information of computer.	Fine of Rs. 1 Lacs & imprisonment for 2 Yrs
Sec. 73	Publishing false digital signature, false in certain particulars.	Fine of Rs. 1 Lacs & imprisonment for 2 Yrs

Cybercrime & Indian ITA 2000

Section	Crime	Punishment
Sec. 74	Publication of Digital Signatures for fraudulent purpose	Fine of Rs. 1 Lacs & imprisonment for 2 Yrs

How Criminals Plan the Attacks

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

Reconnaissance

“Reconnaissance” is an act of reconnoitering – explore, often with the goal of finding something or somebody (especially to gain information about an enemy or potential enemy).

Reconnaissance begins with *“Footprinting”* – this is the preparation toward pre-attack phase

- Involves accumulating data about the target’s environment and computer architecture to find ways to intrude into that environment.

How Criminals Plan the Attacks

Attacker gather the information in two phases : Active & Passive Attacks

Passive Attacks

- A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge.
- It is usually done using Internet searches or by Googling an individual or company to gain information.

E.g.

- Google or Yahoo Search : To locate information about employee
 - Google Earth, WHOIS, Traceroute, Website Watcher
- Surfing online community group like Orkut/ Facebook /Instagram / Whatsapp to gain information about individual.
- Organization's website provide the Name, Email & Contact info.
- Blogs , newsgroups, press releases provide company or individual info.
- Network sniffing : IP address ranges, Hidden servers or networks, What time critical data are transfer and where the traffic is going

How Criminals Plan the Attacks

Active Attacks

- An active attack involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase.
- It involves the risk of detection and is also called “*Rattling the doorknobs*” or “*Active reconnaissance*.”
- Active reconnaissance can provide confirmation to an attacker about security measures in place.
- Tools used for active attacks are
 - PING : To check the availability of a node in network.
 - Nmap : Port scanning and OS service / version identifier
 - TCPCDump: Protocol packet capture

How Criminals Plan the Attacks

Scanning and Scrutinizing Gathered Information

The objectives of scanning are:

- 1. Port scanning:** Identify open/close ports and services.
FTP : Port 20 & 21 for uploading and downloading
SMTP : Port 25 for sending and receiving email
TELNET : Port 23 for remote access device.
HTTP : Port 80 to access the web pages
- 2. Network scanning:** Understand IP Addresses and related information about the computer network systems.
- 3. Vulnerability scanning:** Understand the existing weaknesses in the system.

How Criminals Plan the Attacks

Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password;
2. Exploit the privileges;
3. Execute the malicious commands/applications;
4. Hide the files;
5. Cover the tracks – delete the access logs, so that there is no track illegal activity.

Social Engineering

- It is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- The sign of truly successful social engineers is that they receive information without any doubt.
- **E.g.**
 - Service Desk / Technical Support
 - Shoulder surfing : Look around your desk when you enter credential information.

Social Engineering

Classification of Social Engineering

1. Human-Based Social Engineering

Human-based social engineering refers to person-to-person interaction to get the required/desired information.

- Copying an employee or valid user:
- Posing as an important user: CEO , Project Manager of Company
- Using a third person : Communicate in absenteeism of someone
- Calling technical support:
- Shoulder surfing:
- Dumpster Diving: Looking in the trash for hand written or printing pages or devices (like discarded hdd, fdd, cd, Dvd) Information might be like SSN , PAN, Credit card / Debit card details.

2.

Social Engineering

2. Computer-Based Social Engineering

Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.

E.g.

Fake Email:

Email Attachment : Malicious program like virus, Trojans, keyloggers

Pop-up Window

Solution to social engineering attacks:

- Continuous training / awareness session about such attacks.
- Strict organization policies for employees.

Cyberstalking

- It is defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- It involves harassing or threatening behavior that an individual will conduct repeatedly.
- As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

Cyberstalking

Types of Stalkers

There are primarily two types of stalkers as listed below:

- 1. Online stalkers:** They aim to start the interaction with the victim directly with the help of the Internet.
E.g. Email, Chat room, Social groups etc.
- 2. Offline stalkers:** The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.
E.g. Personal website, Company website, Newsgroups etc.

How Stalking Works? Cyberstalking

1. Personal information gathering about the victim
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.
5. The stalker may post the victim's personal information on any website related to illegal services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details
6. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
7. Whosoever comes across the information, start calling the victim on the given contact details asking for bad services or relationships.
8. Some stalkers subscribe/register the E-Mail account of the victim to innumerable illegal websites, because of which victim will start receiving such kind of unsolicited E-Mails.

Botnets: The Fuel for Cybercrime

- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- Your computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.

Botnets: The Fuel for Cybercrime

One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date.
2. Set the OS to download and install security patches automatically.
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet.
4. Disconnect from the Internet when you are away from your computer.
5. Downloading the freeware only from websites that are known and trustworthy
6. Check regularly the folders in the mail box – “sent items” or “outgoing” – for those messages you did not send.
7. Take an immediate action if your system is infected.