Introduction to Cyber Crime

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both -- i.e., target computers to infect them with viruses, which are then spread to other machines and, sometimes, entire networks.

A primary impact from cybercrime is financial, and cybercrime can include many different types of profit-driven criminal activity, email and internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may target private personal information, as well as corporate data for theft and resale.

Definition -

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for unfair or malicious purposes.

Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cybercrime may also be referred to as computer crime.

Common types of cybercrime include **online bank information theft, identity theft, online predatory crimes and unauthorized computer access.** More serious crimes like cyber terrorism are also of significant concern.

Email tracking

Email tracking is a method for monitoring the delivery of email messages to the intended recipient. Most tracking technologies use some form of digitally time-stamped record to reveal the exact time and date that an email was received or opened, as well the IP address of the recipient.

Email tracking is useful when the sender wants to know if the intended recipient actually received the email, or if they clicked the links. However, due to the nature of the technology, email tracking cannot be considered an absolutely accurate indicator that a message was opened or read by the recipient.

Most email marketing software provides tracking features, sometimes in aggregate (e.g., click-through rate), and sometimes on an individual basis.

STEPS TO TRACING AN EMAIL:

1. Get instructions for locating a header for your email provider here
2. Open the email you want to trace and find its header
3. Copy the header, then paste it into the Trace Email Analyzer below
4. Press the "Get Source" button
5. Scroll down below the box for the Trace Email results!

You should know that in some instances people send emails with false or "forged" headers, which are common in spam and unwanted or even malicious e-mail. Our Trace Email tool does not and cannot detect forged e-mail. That's why that person forged the header to begin with!

What exactly is email tracking, and how are emails tracked?
Commonly associated with email marketing campaigns, email tracking can provide the email sender with details about if and how a recipient has interacted with the content. There is no 'standard' for email tracking, metrics such as opens and clicks are generally cobbled together from other web tracking technologies such as cookies. Due to these constraints, there is no 100% accurate indicator that a message was opened or read by the recipient.

How Email Tracking Works

There are three ways to track an email:

1. Read receipts (through email software such as Microsoft Outlook and Gmail)
2. Image pixels (tracked images inserted into email content)
3. Trackable Links (tracked links inserted into email content)

Read Receipts
A feature found in Microsoft Outlook and a few other email clients, read receipts are an opt-in way to see if an email has been opened. In order for a notification to be received, the recipient must allow read receipts in their settings, or authorize the sending of a receipt.

This can be a more invasive notification system, and only works if sent from and to the same email client (if you send to a gmail address, it will ignore this request). If you don't know what email client the recipient is using, the notification could end up in a black hole.

Because of this, it is uncommon to use, and not very reliable as a tracking option. On the plus side, if you do receive an email receipt notification, it is because the recipient expressly authorized it.

Pixels or Image Notifications
One of the more common ways to track email opens is known as Web Beacon Trafficking. Small images (also known as tracking pixels) are loaded from a tracking server with a coded filename.

When the email is opened, the image is called from the server and counted as a view or an 'open'. This is how email open rates are calculated in most email tracking services.

Many email clients (Microsoft Outlook, Apple Mail on your iPhone, and Gmail) don't always load images on the email open. There are times when images are not automatically downloaded; instead the recipient is given the option to download images once the email is already opened. In cases like this, the recipient can still read the email contents without registering it as an open.

Underreported opens can occur if you have a higher number of emails being delivered to a spam folder, or are an unrecognized sender. You can limit this by increasing your sender reputation by adhering to email best practices avoiding spam tactics and by getting subscribers and recipients to move your emails to their inbox or adding your email address to their address book, therefore making you a trusted sender.

Trackable Links

The final way to track emails is by using tracking links in your email that link to content stored in a cloud-based content repository. This approach will reliably give email click rates, another key metric commonly associated with email tracking.

By using email tracking software that encodes your links, you will be able to see when and what users clicked on. Not all trackable links are created equal. Tracking software can provide a wide range of data- from returning a number of clicks to actual engagement associated with the links.

The Future of Email Tracking

The standard email metrics of deliveries, opens and clicks will always remain relevant, but today's sales and marketing leaders need to know more about how their prospects and customers are interacting with their emails.

What is email spoofing?

Email spoofing refers to a sender address that is fake to make it look as if it came from someone else.

This is a common technique used by phishing attacks, spam, and malware to make their emails appear to be coming from legal sources, such as governmental authorities, insurance companies, and banks. They will frequently contain requests for confidential information, such as social security numbers or banking details, and requests to reset passwords.

Email spoofing is a fraudulent email activity hiding email origins. The act of e-mail spoofing occurs when imposters are able to deliver emails by altering emails' sender information. Although this is usually done by spammers and through phishing emails for advertising purposes, email spoofing can have malicious motives such as virus spreading or attempts to gain personal banking information. Simple Mail Transfer

Protocol (SMTP) does not provide any type of authentication process for persons sending emails. Yet, it is the primary email system for most people, facilitating email spoofing. Now a days, most email servers can provide further security. Also many digital software vendors have created products remedying this problem.

Email spoofing is the creation of email messages with a fake sender address.

Because the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such spoofing to mislead.

When an SMTP email is sent, the initial connection provides two pieces of address information:

- **From:** Joe Q Doe <joeqdoe@example.com> - the address visible to the recipient; but again, by default no checks are done that the sending system is authorized to send on behalf of that address.
- **Reply-to:** Jane Roe <Jane.Roe@example.mil> - similarly not checked

and sometimes:

- **Sender:** Jin Jo <jin.jo@example.jp> - also not checked

The result is that the email recipient sees the email as having come from the address in the *From:* header; they may sometimes be able to find the *MAIL FROM* address; and if they reply to the email it will go to either the address presented in the *From:* or *Reply-to:* header - but none of these addresses are typically reliable, so automated bounce messages may generate backscatter.

How email spoofing works

Email spoofing can be easily achieved with a working Simple Mail Transfer Protocol (SMTP) server and mailing software like Outlook or Gmail. Once an email message is composed, the scammer can fake fields found within the message header such as the FROM, REPLY-TO and RETURN-PATH addresses. After the email is sent, it will appear in the recipient's mailbox that appears to come from the address that was entered.

This is possible to execute because the SMTP does not provide a mechanism for addressing authentication. Although email sender authentication protocols and mechanisms have been developed to combat email spoofing, adoption of those mechanisms has been slow.

If a spoofed email does not appear to be suspicious to the user, it is likely it will go undetected. However, if the user does sense something is wrong, they can open and inspect the email source code. Here, the recipient can find the originating IP address of the email and trace it back to the real sender.

Introduction to Hacking Mobile Devices

The mobile device has become an inseparable part of life today. The attackers are easily able to compromise the mobile network because of various vulnerabilities; the majority of the attacks are because of the untrusted apps. SMS is another way the attackers are gaining access to the mobile devices by sending phishing messages/spam messages to users. The main operating systems used are:

- Android
- IOS
- Windows
- Blackberry

Phone hacking is the practice of manipulating or gaining unauthorized access to mobile phones, such as by intercepting telephone calls or accessing voicemail messages. When the unauthorized access is to the phone user's conversation, it is more commonly referred to as phone tapping.

Phone/Mobile Hacking is the practice of manipulating or gaining unauthorized access to mobile phones, for the malicious purpose.

There are two types of attack used in the mobile sector and these are:

- SMS forwarding
- Bluetooth hacking
- Malicious Website clicking
- Malicious apps

All of these provide a huge HACK value to an attacker when he/she exploits a mobile system for gaining access partially.

SMS forwarders + malicious apps = paying for premium rate numbers

Data Recovery - A Brief Introduction

Data Recovery is the process of retrieval of inaccessible or corrupt data from digital media that has become damaged in some way. Data Recovery can be used to recover data from devices as varied as Hard Disk Drives, Memory Cards, Tapes, Mobile Phones, Personal Digital Assistants, Floppy Disk's, CD's, DVD's, Data Cartridges, Xbox's and many more items.

Data Recovery may be needed for reasons as diverse as hardware failure, (the tape has been 'chewed' up, the hard disk drive has failed, the user has maliciously damaged the computer or digital device, or it could have suffered fire or flood damage). All of these instances will require the services of a professional data

recovery company if the data was of such value (be it sentimental or financial) that the cost of the services are less than the perceived value of the data which is no longer accessible.

What is Data Recovery?

Data recovery is the process involving **restoration of corrupted, lost, accidentally deleted, or inaccessible data**. It mostly involves data recovery from internal or external storage media such as USB drives, hard disk drives (HDD), solid-state drives (SSD), CDs, DVDs, floppy disks, memory cards, magnetic tapes, and other data storage devices.

In corporate, data recovery services include restoration of data from a backup to a laptop, desktop, external storage system or server.

Data recovery services enable the recovery of files that were accidentally deleted without a back-up, but which are present in fragments on the hard disk drive.

Common Causes of Data Loss

Data loss can occur due to multiple reasons such as **virus or malware attack, damaged/corrupted files, unexpected system shutdown, unrecognized format, natural disasters, theft** and much more. Human error is also one of the most important and common causes of data loss.

The causes of data loss can be broadly divided into physical and logical damage as explained below.

Causes of Data Loss – Physical Damage

Physical damage to storage media can result from a wide range of failures due to natural disasters or human errors. Some examples of data loss due to physical damage are:

- The breaking of magnetic tapes
- Scratching off of the dye layer of the metallic substrate of CD/DVDs
- Mechanical failures of hard disks such as motor failure or head crash
- Electrical failure

Expert data recovery services help in addressing data loss due to physical damage, say to a hard disk drive. IFF Lab provides data recovery services in Bangalore for retrieving most, if not all, of the information lost to physical damage.

In case the hard disk is still repairable, then the logical file structure can be rebuilt by creating a full image or clone. However, in certain cases where the hard drive platter is severely damaged, data recovery may be challenging or impossible.

Data Recovery Due to Physical Damage Requires Special Expertise

Opening a hard disk drive requires proper hardware and technical experience and expertise, and a dust-free environment.

Data recovery from physically damaged hard disk drives requires **class 100 dust- and static-free cleanrooms**. This is because airborne dust present in the ambient surroundings can settle on the hard disk platters and damage them further. Thus, it may lead to the compromise of the data recovery process.

Data Recovery Technique – Physical Damage

One method of data recovery due to physical damage is by repairing the hard disk and replacing the damaged parts. Although there may still be logical damages to the hard disk which requires a different approach.

A **special disk-imaging procedure** is then used to recover every portion of a readable bit from the hard disk. This image can be later analyzed for logical damage and used for reconstruction of the original file system.

Causes of Data Loss – Logical Damage

Logical damage refers to data loss due to software and not hardware related issues.

The **logical bad sector** is one of the common causes of logical failure of hard disks. In this, the data in a particular sector of the hard disk becomes inaccessible. This is usually resolved by using data recovery software for repairing the bad sectors of the hard disk drive. Or, replacement of the hardware containing the bad sectors.

Damages in the file system or partition table of hard disk drives or media errors can also render data unreadable. In such cases, data recovery software helps in repairing the damaged portions. Subsequently, one can recover a part of the original data.

Overwritten data can is also one of the causes of data loss due to logical damage. It is little easier to recover the original data in case of data overwriting for solid-state drives (SSD) than hard disk drives. This is because SSDs use flash memory to store data in pages and blocks.

Use of Data Recovery Software

Data recovery software comes into use in case a storage device suffers a data loss due to logical damage. This includes media errors, corrupt partitions or file systems, logical bad sectors or accidental deletion.

Data recovery software help in the effective repair and recovery of files, storage media, databases and corrupt partitions. Such software can be easily purchased online but often require professional experience to use them appropriately.

Some commonly used data recovery software are:

- CDRoller
- Hetman Partition Recovery
- Norton Utilities
- EnCase
- Finnix
- Knoppix
- R-Studio
- Windows Preinstallation Environment
- Disk Drill Basic
- Testdisk
- GetDataBack, and much more.

Fraud detection

Fraud detection is a set of activities undertaken to prevent money or property from being obtained through false pretenses. Fraud detection is applied to many industries such as banking or insurance. In banking, fraud may include forging checks or using stolen credit cards. Other forms of fraud may involve exaggerating losses or causing an accident with the sole intent for the payout.

With an unlimited and rising number of ways someone can commit fraud, detection can be difficult to accomplish. Activities such as reorganization, downsizing, moving to new information systems or encountering a cyber security breach could weaken an organization's ability to detect fraud. This means techniques such as real-time monitoring for frauds is recommended. Organizations should look for fraud in financial transactions, location, devices used, initiated sessions and authentication systems.

Fraud detection techniques

Fraud is typically an act which involves many repeated methods; making searching for patterns a general focus for fraud detection. For example, data analysts can prevent insurance fraud by making algorithms to detect patterns and anomalies.

Fraud detection can be separated by the use of statistical data analysis techniques or artificial intelligence (AI).

Statistical data analysis techniques include the use of:

- Calculating statistical parameters
- Regression analysis
- Probability distributions and models.
- Data matching

AI techniques used to detect fraud include the use of:

- Data mining- Which can classify, group and segment data to search through up to millions of transactions to find patterns and detect fraud.
- Neural networks- Which can learn suspicious looking patterns, and use those patterns to detect them further.
- Machine learning- Which can automatically identify characteristics found in fraud.
- Pattern recognition- Which can detect classes, clusters and patterns of suspicious behavior.

Types of fraud

Fraud can be committed in a number of different ways and in a number of different settings. For example, fraud can be committed in banking, insurance, and government and in healthcare sectors.

One common type of fraud in banking is customer account takeover, where someone illegally gains access to a victim's bank account using bots. Other examples of fraud in banking include the use of malicious applications, the use of false identities, money laundering, credit card fraud and mobile fraud.

Fraud in insurance can include premium diversion fraud, which is the embezzlement of insurance premiums; or frees churning, which is excessive trading by a stockbroker to maximize commissions. Other forms of insurance fraud include asset diversion, workers compensation, car accident, stolen or damaged car, and house fire fraud. The motive behind all insurance fraud is financial profits.

Government fraud is committing fraud against federal agencies such as the departments of Health and Human Services, Transportation, Education, or Energy. Types of government fraud include billing for unnecessary procedures, overcharging for items that cost much less, providing old equipment when billing for new or reporting hours worked for a worker that does not exist.

Healthcare fraud includes drug fraud and medical fraud, as well as encompassing some insurance fraud. Healthcare fraud is committed when someone defrauds an insurer or government health care program.

Website Hacking

Hacking means carrying unauthorized access of a website or the website details. For example if someone opens another person's e-mail without knowing the password, then it is termed as hacking.

Hacking a website is nothing but getting the password to add, edit, delete data stored in that website. After the attack done by a hacker, if he has changed the password of that website software, then it will be tough for the Webmaster to get it back. Hacker will insert harmful programs by inserting malicious codes into the website. It will also cause to the website server to be slow. In the past years, even Amazon and Yahoo had been attacked by the hacker experts, but it would not affect much to them. In the last year we had seen that, the world wide hackers are tried their level best to make fear on the famous companies like PayPal and Facebook.