ASSIGNMENT 3

Describe the key differences between intrusion detection systems (IDS) and intrusion prevention systems (IPS)

An intrusion detection system (IDS) is defined as a solution that monitors network events and analyses them to detect security incidents and imminent threats. An intrusion prevention system (IPS) is defined as a solution that performs intrusion detection and then goes one step ahead and prevents any detected threats. This article lists the key differences and similarities between IDS and IPS.

Intrusion Detection System (IDS)

Intrusion detection systems (IDS) monitor enterprise networks and analyse events to detect security incidents and imminent threats. These security solutions protect businesses by proactively thwarting potential cybersecurity incidents.

An intrusion detection system is a monitoring solution that spots suspicious network incidents and sends out alerts to incident responders or security operations center (SOC) analysts. These alerts enable security personnel to investigate the detected issues and execute the appropriate countermeasures to address them before significant damage occurs.

Two main network deployment locations exist for IDS—host-based IDS (HIDS) and network-based IDS (NIDS). HIDS is deployed at the endpoint level and protects individual endpoints from threats, while NIDS solutions monitor and protect entire enterprise networks.

Apart from its deployment location, IDS also differs in terms of the methodology used for identifying potential intrusions. Signature-based IDS leverages fingerprinting to identify known threats, such as malware. Once malicious traffic is identified, its signature is captured and added to the database. Each signature in this database is compared against network traffic in real time to detect new threats. This type of IDS is capable of detecting known threats rapidly and accurately.

False positives are extremely rare as alerts are only sent out once a known threat is detected. However, signature-based IDS solutions

cannot detect unknown threats and would be helpless in the face of zero-day vulnerabilities.

On the other hand, anomaly-based IDS operates On the other hand, anomaly-based IDS operates by creating a ‘normal’ network behaviour model. All future network activity is compared against this behaviour model, and network anomalies are highlighted as potential threats, with alerts being sent out to security personnel. This type of IDS is capable of detecting zero-day threats. However, both false positives and false negatives are possible here.

Network anomalies: A network anomaly is a sudden and short-lived deviation from the normal operation of the network. Some anomalies are deliberately caused by intruders with malicious intent such as a denial-of-service attack in an IP network, while others may be purely an accident such as an overpass falling in a busy road network.

Finally, hybrid IDS uses signature-based and anomaly-based threat detection to detect cyber-attacks with precision and speed.

Intrusion Prevention System (IPS)

Intrusion prevention systems (IPS) perform intrusion detection and then go one step ahead and stop any detected threats.

An intrusion prevention system is a network security hardware or software that continuously observes network behaviour for threats, just like an intrusion detection system. However, IPS goes one step ahead of IDS and automatically takes the appropriate action to thwart the detected threats, including measures such as reporting, blocking traffic from a particular source, dropping packets, or resetting the connection. Some IPS solutions can also be configured to use a ‘honeypot’ (a decoy that contains dummy data) to misdirect attackers and divert them from their original targets that contain accurate data.

IPS is a critical component of modern-day enterprise security. This is because the organizational networks of 2022 have numerous access points and process high data volumes, thus making manually monitoring traffic and responding to threats an imposing task. Additionally, the increased popularity of cloud platforms means enterprises are operating in highly connected environments. While this has various benefits, it presents a vast attack surface and increases vulnerability if the cloud platform is not adequately secured.

As the threats faced by enterprise systems grow in number and become more sophisticated, automated security solutions such as IPS have become more vital than ever before. This network security solution allows businesses to counter threats in near real-time without stretching security teams' capabilities. It does so by scanning high volumes of traffic without hampering network performance. Many security providers club IPS with unified threat management (UTM) or next-generation firewall (NGFW) solutions.

Unified threat management (UTM) refers to when multiple security features or services are combined into a single device within your network. Using UTM, your network's users are protected with several different features, including antivirus, content filtering, email and web filtering, anti-spam, and more.

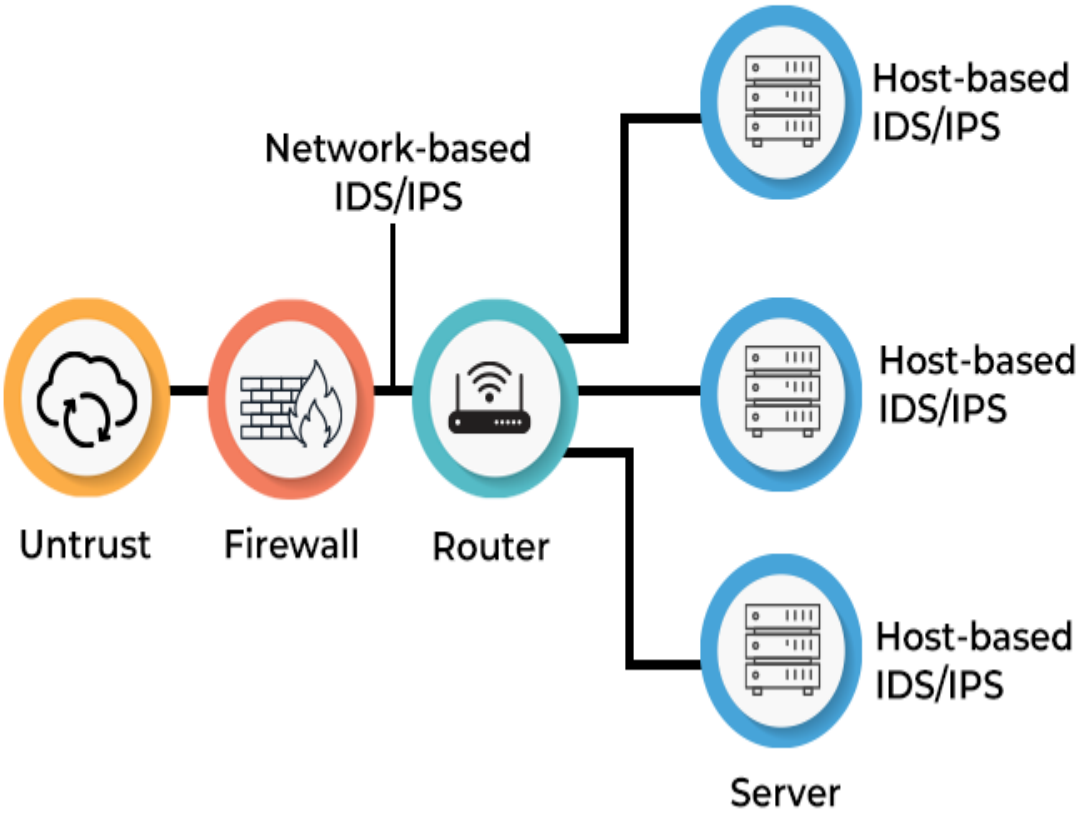
IPS solutions are placed within flowing network traffic, between the point of origin and the destination. IPS might use any one of the multiple available techniques to identify threats. For instance, signature-based IPS compares network activity against the signatures of previously detected threats. While this method can easily deflect previously spotted attacks, it's often unable to recognize newly emerged threats.

Conversely, anomaly-based IPS monitors abnormal activity by creating a baseline standard for network behaviour and comparing traffic against it in real-time. While this method is more effective at detecting unknown threats than signature-based IPS, it produces both false positives and false negatives. Cutting-edge IPS are infused with artificial intelligence (AI) and machine learning (ML) to improve their anomaly-based monitoring capabilities and reduce false alerts.

Finally, policy-based IPS relies on security policies set by the enterprise to detect and block violations. This type of IPS is less common than signature-based and anomaly-based measures as it requires security teams to create and set up relevant policies manually.

Network system of an on an **Enterprise** intrusion detection system (IDS) and Intrusion prevention systems (IPS) shown below

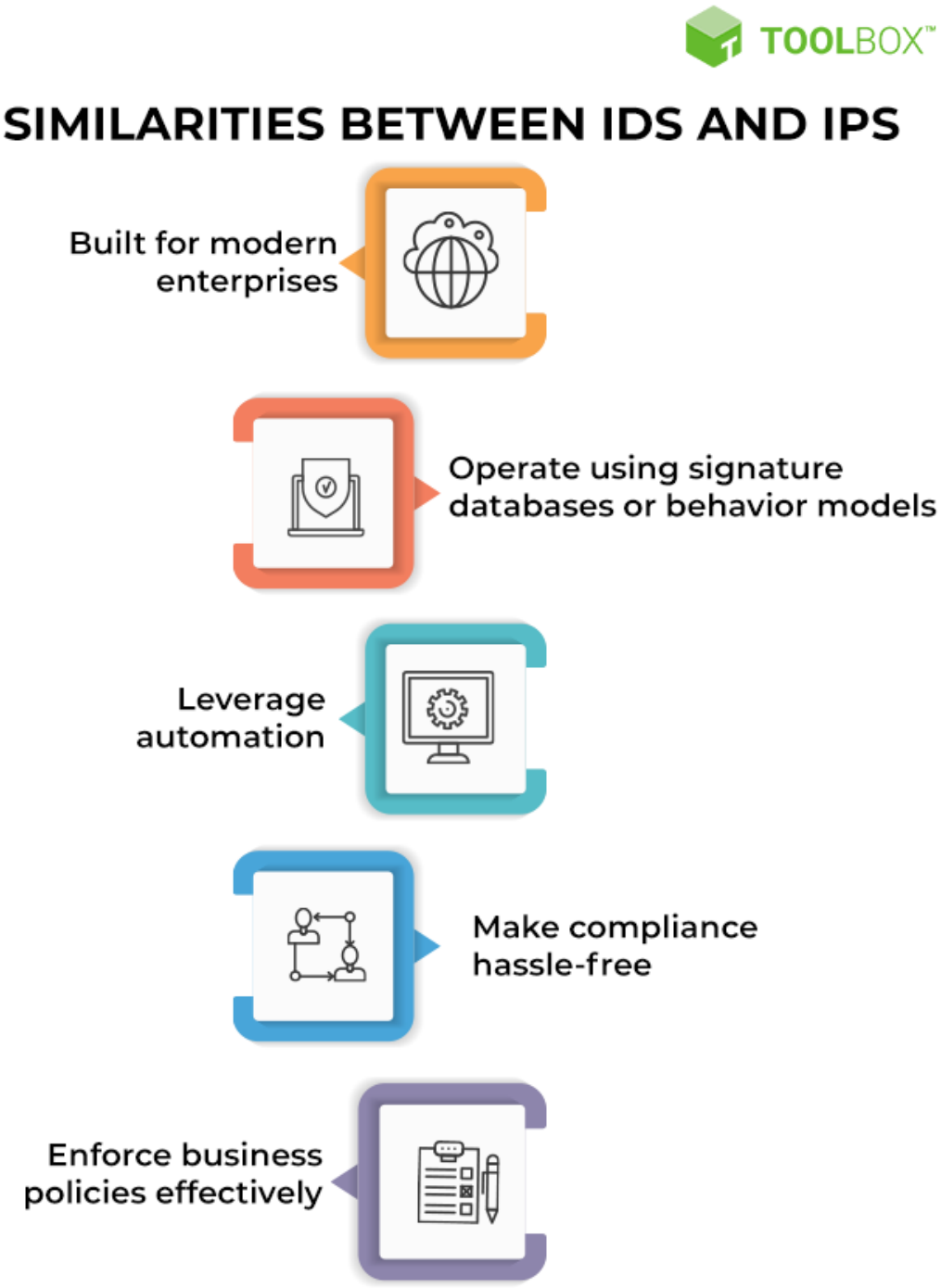
IDS/IPS on an Enterprise Network



Top Similarities between IDS and IPS

Intrusion detection systems and intrusion prevention systems both work to protect network infrastructure. They mainly detect threats by comparing network traffic against a database of known cyber attack signatures or a ‘normal’ network behaviour model. The main difference between IDS and IPS is that, while the former simply ‘monitors’ network traffic, the latter ‘controls’ it.

A significant overlap exists in the way IDS and IPS operate. Listed below are the top five similarities between the two cybersecurity solutions.



1. Built for modern enterprises

The rising prevalence of remote work in the post-pandemic corporate landscape has led to enterprise networks dealing with more access points and higher traffic volumes than in the past. As such, manual network monitoring has become extremely difficult, especially in highly connected cloud environments. In addition to this, the cyber threats

faced by enterprise security teams are increasing in number and sophistication.

All this makes cutting-edge IDS and IPS solutions a vital part of the cybersecurity systems of any modern organization. These automated security tools allow organizations to respond to attacks swiftly and efficiently. Regular updates also help these systems stay updated regarding the latest security threats.

2. Operate using signature databases or behaviour models

IDS and IPS secure enterprise systems using either a signature-based or a behaviour modelling-based approach. Some cybersecurity solutions may even adopt a hybrid methodology that combines the two approaches. Once a threat is detected, these cybersecurity systems alert IT personnel and can even initiate automated actions.

Signature-based intrusion detection and prevention systems are best suited for identifying known cyber threats. These solutions compare network data against a predetermined list of known indicators of compromise.

An indicator of compromise is defined as any specific behaviour known to precede a malicious attack. It includes known byte sequences, malicious domains, file hashes, and even suspicious email content, such as subject lines. Once an indicator of compromise is detected, the packet is flagged for further action.

Upon capturing a signature match, the intrusion detection or intrusion prevention system highlights it and takes further action. Such systems are nearly immune to false positives and negatives and detect threats with very high speed and efficiency. However, they cannot detect a threat if its signature is not present in their databases.

Conversely, behavior model-based intrusion detection and intrusion prevention systems work by detecting anomalies and initiating action in case of unknown or suspicious behavior. Rather than exclusively searching for known threats, these detection and prevention systems use machine learning to build a ‘normalized’ point of reference for how the network behaves typically. All network activity is continuously compared against this baseline. These systems do not search for known indicators of compromise. Instead, they work by identifying anomalous behavior.

IDS and IPS that operate on the behaviour analysis principle act on any network behaviours that fails to align with the created behaviour model. For instance, these systems will highlight user activity outside of business hours, the addition of new devices to a network, or multiple previously-unknown IP addresses attempting to connect with the network.

This might lead to non-malicious behaviours being highlighted simply for being abnormal. Such false positives could require the allocation of additional resources for investigation. However, IDS and IPS that use behavior bh-based anomaly detection can detect new threats that signature-based detection and prevention systems cannot.

3. Leverage automation

Unlike traditional cybersecurity measures that require round-the-clock monitoring by security personnel, IDS and IPS use automation to protect highly digitalized enterprise environments. This helps IT teams secure organizational networks from cyber threats while expending minimal resources.

Intrusion detection and prevention systems offer network protection using either a hardware-based or a software-based approach. In the former, sensors are strategically placed at key points on the enterprise network to monitor network data. In the latter, detection and prevention tools are installed on devices linked to the network to track inbound and outbound data. Once a threat is detected, these solutions automatically raise the alarm. Based on configured rules and policies, IPS can also initiate further actions without human intervention.

4. Make compliance hassle-free

Regulators in many jurisdictions require corporations to ensure the security of customer data. This is especially true for enterprises operating in more sensitive industry verticals such as healthcare and finance. Complying with the laid down directives entails investments in industry-standard data protection measures, such as IDS and IPS. These security solutions help ensure compliance by addressing numerous regulatory requirements. Additionally, they maintain auditing records that are useful during compliance investigations.

With enterprises constantly increasing their digital footprint, monitoring the complete network environment requires more resources than they

normally have. IDS and IPS spot and stop malicious data before it can cause major damage. Through the automated implementation of compliance requirements, IDS, IPS, and other security devices work in unison to reduce the pressure on human security teams.

Complying with stringent regulatory directives might also require the in-depth monitoring of business infrastructure. IDS and IPS can passively monitor various network segments and control less visible traffic. For instance, if installed correctly, these solutions can highlight anomalies in traffic that exist only within a LAN connection and are unmonitored by other security solutions.

Setting IDS and IPS alerts also enables robust protection in line with compliance requirements. Real-time monitoring by intrusion detection and prevention systems allows IT personnel to take the required actions as soon as an anomaly is detected. This helps prevent violations by significantly reducing the complexity of the enterprise's decision-making process.

Finally, in case of a security breach, the data collected by IDS and IPS may be admissible in the courts of certain jurisdictions. This information can be used as evidence that the affected organization did as much as possible to thwart the violation. It might also give the authorities the forensic data needed to investigate the event and potentially identify the attackers.

5. Enforce business policies effectively

Enforcing business policies in a remote work environment is not always easy. The final key similarity between IDS and IPS is their ability to help ensure highly secure and ethical business operations through policy enforcement.

Intrusion detection and prevention solutions can be set up to enforce security policies at the enterprise network level. For instance, if company policy mandates using a specific VPN service, IPS can be configured to block traffic from other VPNs. The logs and reports generated by these tools can also be used to draft training modules and create new operational and security policies.

These security solutions can detect inappropriate cyber behavior, capture it, and process it as a security event. This makes it possible to monitor chronic or suspected policy abusers remotely and collect evidence of malicious behavior.

Top five Differences between IDS and IPS

While intrusion detection and prevention systems are similar in numerous important ways, they also have a few key differences in scope, location, type, level of intervention required, and configuration.

Scope

- IDS operates as a monitoring tool that reads and compares network packets against a known threat signatures database or a baseline created using machine learning.

  An IDS is built for detection and surveillance and will take minimal

  +Action by itself when a threat is detected.

- IPS is a control-based solution that either accepts or rejects network packets based on predetermined rule sets.

  An IPS can do the job of an IDS, but vice-versa is not possible.

Location and Range

- IDS operates across the enterprise network, monitoring and analysing traffic in real-time. Packets anywhere on the network are scanned for indicators of compromise, and any detected threats or anomalies are flagged.

  Once a violation of the configured security policies–such as a port scanner, ransomware, or malware–is detected, IDS alerts human security personnel for further action.

- IPS operates typically in the same network location as a firewall, intercepting traffic at the juncture where the internal network meets the internet at large. Once a threat is detected, IPS stops the flow of malicious traffic.

  Unlike IDS, IPS can shut down the threat and prevent the malicious packets from reaching their target while alerting security personnel.

However, its range can be limited compared to IDS. IPS can rely on IDS to increase its range of surveillance.

Types

- **Intrusion Detection System - two types**

Host-based IDS (HIDS) is deployed at the endpoint level to protect individual devices from cyber threats. This type of IDS can monitor network traffic as it flows in and out of a device. It can also track running processes and examine system logs.

HIDS only protects its host machine, which means it does not have access to the complete network data and the associated context for decision-making. However, it has granular visibility into the workings of the host device.

Network-based IDS (NIDS) monitors the entire enterprise network.

It tracks all the traffic that passes to and from every device on the network and makes decisions by studying the metadata and content of packet.

NIDS has a wider viewpoint than HIDS, giving it more contextual information and allowing it to detect widespread threats. However, such systems might not have granular visibility into the devices that they secure.

- **Intrusion Prevention System – three types**

Host-based IPS (HIPS) is a cybersecurity software that is located on individual clients and servers. It monitors events and thwarts attacks at the device level.

Network-based IPS (NIPS) is deployed within the enterprise network infrastructure. It monitors all the data in the complete network and thwarts threats before they can reach their targets.

Wireless IPS (WIPS) is a network security device that monitors radio waves for unauthorized access points and automatically takes countermeasures to prevent them from causing damage to enterprise systems.

Intervention Level Required

- IDS relies on the intervention of IT teams or other security systems to prevent threats. It is capable of scanning networks for known and previously unknown threats. However, it is not able to use the results of these scans to implement a predetermined plan of action and address identified threats independently.

If another solution, such as IPS, is not implemented, IDS would require a dedicated human resource to deal with malicious traffic once spotted.

- IPS is a highly proactive cybersecurity solution that leverages either a database of the latest threat signatures or an ML-powered behaviour model to detect and prevent cybersecurity violations.

Unlike IDS, IPS solutions are capable of autonomously stopping threats before they are able to cause any damage.

Configuration

- IDS is generally set to operate in the inline mode.

Security teams can specify the expected action of the IDS once a threat is detected. For instance, IDS can create a log of the event, transmit a notification to a pager or a console, or communicate a command to a router or firewall.

Logging the activity provides forensic information that allows security teams to analyse successful exploits. Logs can also be used to update router, firewall, and server policies to stop such events from recurring.

Firewall means a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

Enterprises normally set up IDS to handle logs and alerts while the routers, firewalls, and servers fight threats.

- In a network, IPS is placed behind the firewall.

IPS is generally configured to operate either as an end host or in the inline mode. Behaviour-based IPS might occasionally raise false alarms as harmless anomalies are caught in its filter.

By fine-tuning the configuration of this type of IPS, it can be set to recognize normal network traffic and let it through, thus detecting threats without disrupting day-to-day network operations.

In the post-pandemic world, cyber threats have become more dangerous than ever before. Network security systems that integrate signature databases and artificial intelligence, such as IDS and IPS, are powerful tools that enable IT teams to bolster their security posture against advanced threat actors.

Design a hypothetical network architecture for a medium-sized enterprise and outline how you would integrate both intrusion detection and prevention mechanisms. Consider factors such as placement of sensors, types of detection techniques (e.g., signature-based, anomaly-based), and strategies for blocking or mitigating identified threats.

To design, plan, and implement a medium level network for a hypothetical client. Consider the following the steps

Information Gathering

You are a networking consultant who has been hired by a hypothetical company to evaluate their current network and propose changes to upgrade it. Your job is to prepare a "Network Upgrade Plan" that includes the following.

The following information is obtained during some hypothetical interviews with selected number of the staff.

Physical Structures

Provide the detailed information about the buildings, floors, and the measurements.

Offices

How many offices does your client have?

Are they already connected?

LAN Clients

Provide the categories of clients (perhaps one category per department) and number of clients per category

Wireless Clients

Provide the maximum number of wireless clients. Do you support public clients?

Servers

Would you use peer-to-peer or centralized network?

How many servers does your client have?

Provide types and number of Servers that are required by the network, i.e. File servers, Domain Servers, Name Servers, etc. (see internet hosting for alternate configuration)

Hosting and Internet Users

How to do support internet users?

How has your internet domain been hosted (internally or via a hosting provider) and where is the company mail server located?

Do you support file transfer?

How internet users access resources on the private network?

Firewalls and DMZ

If applicable, identify the zones of the network nodes, and specify how public servers are accessed from the Internet

Internet Support

How do the employees access the internet?

Shared Resources

List all types of shared resources that are used in the network (i.e. printers, file servers, etc.)
Provide the status quo as well as the deaired quota that the client is requesting. List the network needs (what's not working at the moment). This may be a list of issues and how to resolve them at a high-level. Since the client is hypothetical, the status quo may be bare minimum.

Network Design

Outline the Network Design. Include the following information in your proposal:
- Number of networks and subnets; addresses and VLANs; DHCP reservations, etc.
- Number (and models) of network equipment (i.e. routers, switches, hubs, modems, access points, etc.)
- Number, type, and measurement of the connecting cables (see structured cabling).

Packet Tracer Implementation

Implement the proposed network in packet tracer. The packet tracer file includes the network simulation of the logical network.
Your implementation must include the following:
- Include all user types as sub networks and include some examples of users as nodes on the sub network. One node per category would suffice.
- Include shared resources as needed: i.e. file servers, web servers, networked printers, etc.
- Ensure that all notes are properly configured with IP addresses, subnet

masks, default gateways, etc.
- Ensure that ping works across the board.
- Manually configure or use DHCP for IP address configuration.
- Manually configure or use RIP for routing configuration.

Future Upgrade

Include and plan the clients' future needs in your implementation. Examples of possible future need is given in the following:
- How many workstations does the current network have? How many workstations will the network need in a year from now?
- How about connection speeds? Wireless Access Points?

Cost Estimation

Provide the implementation cost. Your estimate includes all network devices, computer upgrades (software or hardware), as well as Labour. Make a list of all your network elements (based on your Packet Tracer simulation) and research the cost of each. Tally up the total cost of your network and explain why your client should spend this money to upgrade their network.
This is how the network architecture for a medium-sized enterprise.

Integration of intrusion detection and prevention mechanisms:

The network-based intrusion detection system (NIDS) is one of the smartest devices on the network, carefully examining the traffic from the equipment it is located in. NIDS can be hardware or software based systems, and depending on the manufacturer, they can be Ethernet, FDDI, etc. can be connected to various environments. Typically, NIDS has two network interfaces. One for listening to network conversations in random mode and the other for management and reporting.

The Network Based Intrusion Detection System (NIDS) is responsible for monitoring and analysing network traffic to identify potentially suspicious activity and genuine threats through the utilization of NIDS sensors. It

examines the content and header information of all data packets moving on the network.

NIDS sensors are strategically positioned within the network to examine traffic originating from various network devices. As an illustration, these sensors are commonly deployed in the same subnet as the firewall to effectively identify attacks such as denial of service (DoS) and other malicious activities.

How does an IDS work?

* The primary role of an Intrusion Detection System (IDS) is to constantly monitor the traffic within a computer network, diligently searching for any indications of unusual or suspicious activity.

* It analyses data flowing over the network for abnormal behavior patterns and symptoms.

* An IDS compares network activity against defined criteria and patterns to identify activities that could indicate an attack or intrusion.

* If IDS finds a match for any of these rules or patterns, it sends a notification to the system administrator.

* Administrators can control the warning and prevent further damage or access.

Detection Method of IDS

1. Signature-based intrusion detection

Signature-based intrusion detection aims to identify potential threats by comparing network traffic and log data with existing attack patterns. These patterns are called sequences (hence the name) and may contain sequences of bytes called malicious instruction sequences. Signature-based detection allows you to identify and identify known attacks.

2. Anomaly-based intrusion detection

It is designed to detect unknown attacks, such as new malware and instantly adapt to them using machine learning. Machine learning techniques enable intrusion detection systems (IDS) to build a base of trust (called a trust model) and then compare the new behavior with the trust model. False positives can occur when using a weak IDS, as

previously unknown but legitimate communications can be misidentified as malicious.

Comparison of IDS with Firewalls

Both IDSs and firewalls are related to network security, but IDSs are different from firewalls because firewalls look for outside access to prevent this from happening. The firewall restricts the access of networks to block access and does not show the attack if it comes from the network. When an intrusion occurs, IDS discloses the suspected intrusion and then sets up an alert.

Intrusion Prevention System

The utilization of automated IPS solutions is highly beneficial in safeguarding other security devices or controls by effectively filtering out and preventing malicious activity from reaching them. This reduces the manual work of the security team and allows other security products to work more efficiently.

IPS solutions are highly proficient in both detecting and preventing instances of fraud, making them an effective tool for maintaining security and protecting against fraudulent activities. When a vulnerability is discovered, it is usually found before the security is exploited. An immigration prevention system is used here to quickly stop such attacks.

IPS devices were first developed and released as a device in the mid-2000s. This capability is integrated into advanced threat management (UTM) solutions and firewalls. Next IPS solutions now depend on cloud-based computing and networking services.

It can also do more monitoring and analysis, such as intrusion prevention, monitoring, and reacting to bad traffic patterns or packets. Search mechanisms may include:

* HTTP string and substring matching

* TCP/UDP port matching

* Generic pattern matching

* Packet anomaly detection

* Address matching

* Traffic anomaly detection

* TCP connection analysis

An intrusion detection system (IDS) is a powerful tool that can help businesses detect and block unauthorized access to their networks. IDS can detect suspicious activity and alert administrators by analyzing network connectivity patterns. Adding an IDS to an organization's security infrastructure offers substantial benefits by increasing visibility into network operations and enhancing network performance.

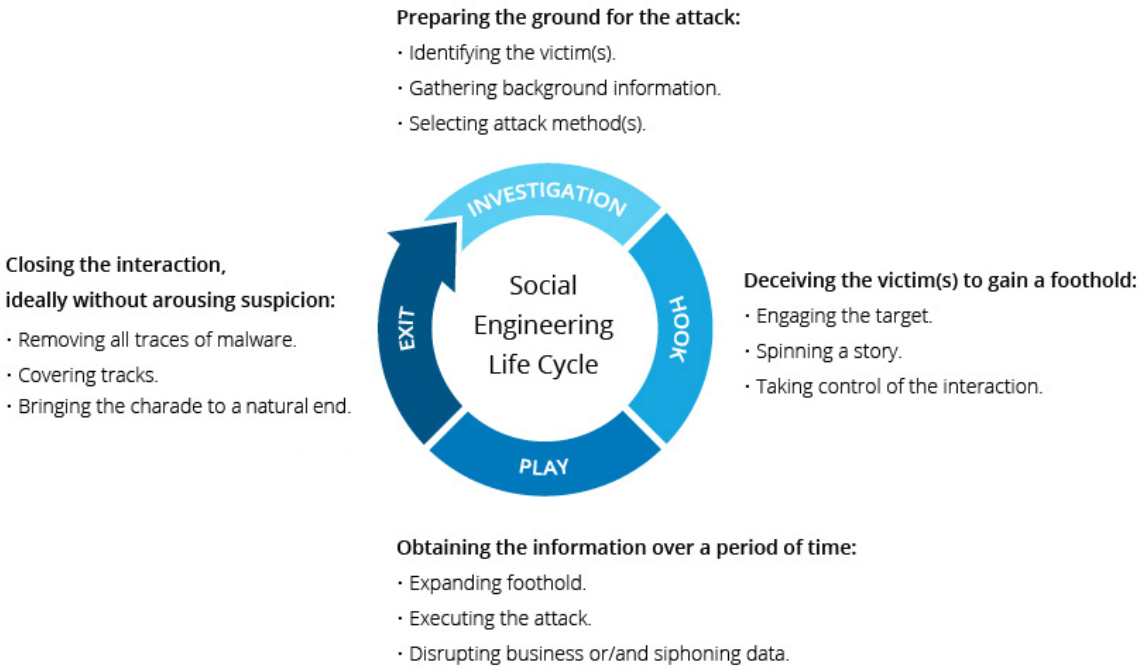
Analyse the impact of social engineering attacks on individuals and organizations, considering factors such as financial losses, reputational damage, and compromised data security.

Social engineering is the term used for a broad range of **malicious activities accomplished through human interactions**. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the **attacker** moves to gain the victim’s trust and provide stimuli for subsequent actions that break security practices, such as revealing **sensitive information or granting access to critical resources.**

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

Social engineering life cycle shown below



Social engineering attack techniques

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.

Baiting

As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-

infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list.

Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.

Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing **the web,** displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.

Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.

Pretexting

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions

that are ostensibly required to confirm the victim's identity, through which they gather important personal data.

All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Phishing

As one of the most popular social engineering attack types, **phishing** scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.

Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having **access to threat sharing platforms.**

Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. **Spear phishing** requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skilfully.

A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic

message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

The impact of social engineering on businesses

Social engineering attacks can be extremely lucrative for cybercriminals. The motive is usually financial gain, which can cost you or your customers a lot of money. Beyond this calculable loss is the damage done to your company's reputation, which can have significant, long-term repercussions for your business.

Financial losses

Losses due to social engineering attacks can quickly add up to millions of dollars. Remediation costs include stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, and fraud. According to the FBI, about 19,000 victims of tech-support scams submitted complaints between January 2023 and June 2023. Estimated losses totaled more than $542 million. As of August 2023, losses have already exceeded those in 2022 by 40%.

Reputational damage

Falling victim to social engineering can tarnish a company's reputation and erode trust. Trust is hard to regain once it's lost, and customers or business partners may be hesitant to do business with a company that has been compromised or doesn't make security a top priority. In fact, according to **Malware bytes Labs**, 75% of those surveyed said they'd stop doing business with a company that has fallen victim to a breach or cyberattack that potentially compromised data.

Recognizing individual social engineering attacks

Becoming the victim of a social engineering attack is not inevitable. There are certain signs you can look out for to help you recognize social engineering attempts everywhere you connect in today's digital world: your inbox, voicemail, direct messages (DMs), text messages, marketplace accounts, and more.

Common signs of social engineering attempts

- You receive an urgent message requesting immediate assistance
- The message contains a suspicious file attachment or URL
- The message has multiple grammatical errors or typos
- The sender's email is misspelled or doesn't match the organization
- You are asked to verify your information
- A message arrives unexpectedly with a specific request
- The message asks you to perform an action that is out of the ordinary
- The offer appears too good to be true
- The message feels overly eager or threatening

Spotting social engineering attempts on your platform

Bad actors want to take advantage of the community you've worked hard to build. Whether your business is a social media platform, marketplace, online dating site, crypto currency exchange, or other platform, the more you know about your users and can tune your fraud tools to spot anomalies, the easier it will be to automatically flag suspicious behavior for further investigation.

There are common risky behaviors, anomalies, and repeated suspicious activities you should look out for. It's also important to scan your internal data to spot new patterns and continually tune your fraud tech stack.

Signs of potential social engineering in your community

- Multiple users logging in from the same devices and IPs
- Multiple accounts created using the same onboarding information (names, addresses)
- Change in IP and device post-account creation
- Consistent or identical user behavior from seemingly disconnected accounts

Prevention strategies for businesses

Even though social engineering attacks are becoming more sophisticated by the day, there are a few approaches you can take to be proactive about fraud and help prevent these types of crimes. Just remember, your fraud tooling isn't a "set it and forget it" program you review once a year. It also shouldn't be hyper-focused on addressing one type of fraud or tactic, but rather offer a multilayered approach to prevention that addresses many types of fraud and methods of attack.

The only way to be on top of social engineering is to always be aware of the current trends that are happening in your space when it comes to fraud, and using those trends to alter and update your content.

Encourage users to implement strong authentication measures

One password isn't enough to secure an account. Requiring users to implement two-factor (2FA) or multi-factor authentication (MFA) and educating them on its importance significantly reduces the risk of unauthorized access. These additional layers of authentication can come in the form of security questions, captcha, fingerprinting, face scanning, SMS confirmation codes, and more.

Add progressive risk segmentation

Your user onboarding process is the first hurdle a fraudster must cross to gain access to your platform and community. This is where you can block potential fraudsters and lower your risk.

Progressive risk segmentation is a strategy that helps you balance fraud prevention with user experience by automatically segmenting individuals based on real-time signals and adjusting the level of identity verification based on the riskiness of the interaction.

Traditional verification methods ask users to complete the same steps no matter how risky the transaction. Progressive risk segmentation lets you step up and down friction to modify a user's experience based on signals it picks up during the verification process.

With Persona's Verifications and Dynamic Flow products, you can quickly set up custom flows to verify good users and block bad actors — no code needed. Users who readily pass your initial verification checks can move quickly through your flow while others exhibiting passive risk signals — hesitation time, shortcut usage, and more — can be automatically routed to a different path where they may be asked to take a selfie or check their email or phone for a confirmation code, for

example. Criminals possessing hundreds of fake IDs and stolen information will likely not remember the phone number or email address they entered for a fake account they created, giving you a better chance of deterring would-be fraudsters.

Customer education and open communication

Fraudsters continue to innovate, so awareness and education are key. Sometimes your best defense against fraudsters are the good actors and legitimate users on your platform. Keep the lines of communication open and offer helpful educational resources they can easily access and put to good use:

- Provide help center articles and customer support to address these types of attacks
- Provide customer avenues to contact you directly to provide feedback and report social engineering attacks
- Add prompts to your user flow that stop victims and ask them to think about the information they are about to divulge. Some good examples of this are the pop-ups commonly seen on payment apps when you send money to a user you've never paid before.

Document an incident response plan

Prevention is the goal, but you also need to develop an incident response (IR) plan to minimize damage in case of a suspected social engineering attack. This detailed plan should outline how your organization prepares, detects, and responds to fraud on your platform.

If you suspect fraud in your community, you should:

- Collect examples of confirmed or presumed social engineering for investigation
- Expand your investigation outward for more intelligence leveraging link analysis, a method of analyzing data that allows you to study relationships that aren't visible in raw data, like known patterns, new patterns, and anomalies
- Acknowledge that a lot of fraud resulting from social engineering happens outside of systems you can monitor (email, messaging

apps, etc.), so you may need to ask victims for correspondence and instruction from fraudsters to help with the investigation

- Update policies, procedures, and technology based on the findings

Employee awareness training

The types of social engineering affecting your users are the same ones hitting the inboxes of your employees sent by bad actors trying to infiltrate your company. This is why employee awareness training is critical.

Educate your team about the dangers of social engineering, how to recognize potential threats, and the best ways to report incidents to security. Some employee security training offers phishing simulations and exercises to help your teams engage and interact with cybersecurity scenarios and best practices.

How Persona can help mitigate the effects of social engineering

No technology can put a stop to social engineering. The best you can do is ensure your team is vigilant and has a process in place for identifying activity typical of social engineering and working with an identity verification and fraud prevention partner to mitigate its downstream effects.

Persona is a unified identity platform, helping companies from multiple industries, including fintech, digital health, e-learning, and marketplaces combat social engineering attacks and sophisticated fraud.

We are privileged to partner with Rently, a company that lets potential buyers or renters schedule self-tours to view properties, for its verification and fraud prevention needs. It uses Persona to verify that the same individual who signed up online is the person who shows up to view the property. This helps prevent fraudsters from impersonating legitimate property managers to take listings off-platform or gain access to properties under false pretenses.

With Persona, Rently built workflows to support ID types for all geographies and automated decisioning so only the approved IDs are passed through the system. Dynamic Flow makes it possible to introduce and adjust friction based on the user's risk profile, which

doesn’t have much of an impact on good users but makes things a lot harder on bad actors. And Persona’s reverification functionality makes it easy for renters to safely tour multiple properties.

Compare and contrast the characteristics of malware and ransomware attacks, including their methods of propagation, objectives, and potential consequences for victims. Evaluate the effectiveness of proactive measures such as regular software updates, antivirus software, and user awareness training in preventing and mitigating the impact of these types of cyber threats.

Ransomware type of malware that, once installed on a user’s computer, can deny a user access to files. Ransomware works by encrypting the files so that a cybercriminal can demand the user pay a ransom to decrypt them.

Ransomware has become a top **cyber threat** to organizations and can even drive a company into bankruptcy.

This article explains how ransomware differs from other malware, how it can get installed on your device and how to prevent it from happening.

The Differences between Ransomware and Malware

Malware means “malicious software” and refers to **any type** of malicious software designed to harm a computer system. This includes ransomware, viruses, Trojan horses, spyware, adware and more.

Ransomware, on the other hand, is a type of malware that specifically takes data or systems hostage while a cybercriminal demands a ransom for them to be released. Paying the ransom and retrieving your data doesn’t mean you’re in the clear. If cybercriminals know you’re willing to pay the ransom, they may keep targeting you with more ransomware attacks. In some cases, even if the ransom is paid, cybercriminals will not decrypt the files.

Types of Malware

Besides ransomware, let's take a look at the other main types of malware.

1. **Virus**: A **computer virus** is malicious software that infects other programs and causes damage to the system. Viruses depend on other files and programs. It can't exist on its own and requires a host (like a file or program) to spread.

2. **Trojan horse**: Malicious code or software that runs on a device without the user's knowledge, disguised as a legitimate application or file.

3. **Spyware**: Software that collects information without the user's knowledge and sends it to a third party. Cybercriminals can spy on you using your computer's camera or track your keystrokes using a type of spyware called a keylogger.

4. **Adware**: Software that displays malicious banner advertisements. It acts similarly to spyware without installing software on the device or capturing keystrokes.

5. **Worm**: A computer worm replicates itself over the network and spreads the infection over a large area. The worm operates independently. It can spread on its own without relying on other files or programs.

6. **Cryptojacking**: The act of illegally using another person's computer to mine virtual currency. This can be done through phishing or by injecting JavaScript code into websites that run automatically on your computer.

7. How Does Ransomware Get Installed?

There are several types of ransomware and they can infect a network or system in different ways, but here are the most common ways in which it can get installed.

Malicious email attachments and links

Ransomware attackers use phishing attempts to send large numbers of emails with malicious attachments or links to get victims to click on the attachments or links. Once the attachment or link is clicked, ransomware can be automatically downloaded on the device.

Fraudulent advertising on websites

If you see something, such as a pop-up ad, appear on your screen while browsing the web, it's important to carefully check its content. Your system may become infected by clicking on malicious advertisements, also known as malvertising.

Additionally, you may encounter situations where you are redirected to a suspicious URL, otherwise known as a website address , that has been spoofed to look legitimate and encourage you to download a file. These situations require special attention. Always inspect a URL before clicking on it to avoid falling victim to a ransomware attack.

Downloading applications or software

Downloading applications or software from websites other than official ones is risky. There are many suspicious apps on spoofed websites, and if you click the download button, you'll be downloading malware.

Always use caution when downloading an application. Only download apps from official app stores such as the Google Play Store or Apple's App Store.

Avoid connecting to public WiFi

Public WiFi comes with risks, one of them being the possibility of having your device become infected with malware. If a public WiFi network or a device already connected to the network is infected with ransomware or other types of malware, it can spread the infection to your device and any other devices connected to the same network.

Access through remote desktop

If your organization's remote desktop service has configuration issues or security weaknesses, attackers can exploit these vulnerabilities to gain access to your servers and deploy ransomware. If your remote access system is poorly secured, the possibility of a ransomware infection is even greater.

How to Prevent Malware and Ransomware

Let's take a look at how you can protect yourself from malware and ransomware.

Keep your OS and software up to date

Keeping your Operating System (OS) and the software you use up to date is essential to stay protected from ransomware. Software updates fix security vulnerabilities and reduce the chance of infection.

Continuing to use outdated versions of your OS and software increases security risks. Therefore, it is recommended that you update regularly and use the latest version.

Use strong and unique passwords

One effective defense against ransomware is to use strong and unique passwords. Strong passwords are at least 16 characters long and contain a combination of uppercase and lowercase letters, numbers and special characters. These passwords should not contain consecutive numbers, birthdays, common words or phrases or personal information, and most importantly, they should not be reused for multiple accounts.

Consider using a password manager to generate strong passwords and store them securely. A password manager is an encrypted digital vault that securely stores your passwords, generates new ones, detects weak and reused passwords, and stores 2FA codes and other sensitive information. Keeper® offers a 30-day free trial so you can start protecting your passwords.

Enable multi-factor authentication

Once you have set strong passwords for all your accounts, you should enable Multi-Factor Authentication (MFA). MFA provides an additional layer of security to your accounts by requiring one or more forms of authentication in addition to your password to access your account.

MFA is a great defense against account takeover attacks because even if a cybercriminal somehow manages to compromise your password, they won't be able to log in to your account without providing additional authentication factors.

Pay attention to emails and attachments

To prevent ransomware, it's important to pay special attention to email security. Avoid opening emails from unknown senders, emails with

suspicious attachments or links, and emails containing a sense of urgency, grammatical errors or too-good-to-be-true offers.

Be sure to take the following measures:

- **Confirm sender**: Check whether the sender of the email is trustworthy and do not open it if it is suspicious.
- **Inspect the attachment**: Scan any attachments with reliable antivirus software.
- **Validate the link**: Do not click on links in emails. Instead, safely copy the URL of the website and paste it directly into the Google Transparency Report tool to check if it's safe to click.

Perform regular backups

With regular backups, you can recover your data and prevent the worst-case scenario in the event of a ransomware attack. The best way to back up your data is to store all your data in encrypted cloud storage. This ensures that your data is always encrypted, meaning no one can know what your data is, and that you'll be able to access your data online from anywhere on any device due to it being stored in the cloud.

Check if the software is from an official source

As an important part of ransomware and malware protection, you should always download software from official sources. Use official websites and trusted app stores and avoid downloading from third-party websites and unverified links. Malicious software or modified applications can be a source of ransomware infections, so verifying the legitimacy of the source is critical.

Educate employees about cybersecurity awareness

Ransomware is one of the most serious cyber threats that can damage organizations. It encrypts important data and disrupts business operations. Employee cybersecurity education and awareness is a core part of ransomware protection. Regular training should be conducted to thoroughly educate employees on how to recognize phishing emails and avoid clicking on suspicious links and attachments.

When employees are aware of cyber threats, they can improve the overall security of an organization and protect it from cyber-attacks.

Actions to take

There are some actions you can take to help prepare your organisation from potential malware and ransomware attacks.

Action 1: make regular backups

Action 2: prevent malware from being delivered and spreading to devices

Action 3: prevent malware from running on devices

Action 4: prepare for an incident

Take Precautions to Protect Against Ransomware

Malware, especially ransomware, poses a significant threat to people and businesses. If you don't take the time to plan and invest wisely, you could end up jeopardizing your business, paying recovery costs, including fines and severely damaging your reputation.

How has the IT Act of 2000, along with its subsequent amendments, shaped the legal landscape for addressing cyber-crime and offenses in India? Discuss the key provisions of the Act related to cyber-security and examine their effectiveness in prosecuting cyber-criminals and protecting individuals and organizations from cyber threats

According to a general cyber law definition, Cyber law is a legal system that deals with the internet, computer systems, cyberspace, and all matters related to cyberspace or information technology. Cyberspace

law covers a wide range of topics including aspects of contract law, privacy laws, and intellectual property laws. It directs the electronic circulation of software, information, and data security as well as electronic commerce. E-documents are given legal recognition under cyber law. Moreover, the system provides a structure for electronic commerce transactions and electronic filing of forms. To put it simply, it is a law that deals with cyber-crimess . As e-commerce has increased in popularity, it has become important to ensure there are proper regulations in place to prevent malpractices.

There are many different laws governing cybersecurity, largely depending on each country's territorial extent. The punishments for the same also vary according to the offence committed, ranging from fines to imprisonment. **The Computer Fraud and Abuse Act of 1986** was the first cyber law that was ever to be enacted. It prohibits unauthorized access to computers and the illegal use of digital information.

Internet usage has increased, and so has cyber crimes. There are several stories of cyber crimes in the media today ranging from identity theft, cryptojacking, child pornography, cyber terrorism etc. In cybercrimes, the computer is used either as a tool or a target, or both, in order to commit unlawful conduct. In our fast-moving digital age, there has been a phenomenal surge in electronic commerce (e-commerce) and online stock trading, leading to more cybercrimes.

Overview of cybercrimes and cyber law

What is cyber crime

Any criminal activity that involves a computer, networked device, or any other related device can be considered a cyber crime. There are some instances when cybercrimes are carried out with the intention of generating profit for the cybercriminals, whereas other times a cybercrime is carried out directly to damage or disable the computer or device. It is also possible that others use computers or networks to spread malware, illegal information, images, or any other kind of material.

As a result of cybercrime, many types of profit-driven criminal activities can be perpetrated, such as ransomware attacks, email and internet

fraud, identity theft, and frauds involving financial accounts, credit cards or any other payment card. The theft and resale of personal and corporate data could be the goal of cybercriminals.

In India, cybercrimes are covered by the **Information Technology Act, 2000** and the **Indian Penal Code, 1860**. It is the Information Technology Act, 2000, which deals with issues related to cybercrimes and electronic commerce. However, in the year 2008, the Act was amended and outlined the definition and punishment of cybercrime. Several amendments to the Indian Penal Code 1860 and the **Reserve Bank of India Act** were also made.

Types of cyber crimes

The following are considered to be types of cyber-crimes:

Child pornography or child sexually abusive material (CSAM):

In its simplest sense, child sexual abuse materials (CSAMs) include any material containing sexual images in any form, wherein both the child being exploited or abused may be seen. There is a provision in Section 67(B) of the Information Technology Act which states that the publication or transmission of material depicting children in sexually explicit acts in an electronic form is punishable.

Cyberbullying:

A cyberbully is someone who harasses or bullies others using electronic devices like computers, mobile phones, laptops, etc. Cyberbullying refers to bullying conducted through the use of digital technology. The use of social media, messaging platforms, gaming platforms, and mobile devices may be involved. Oftentimes, this involves repeated behaviour that is intended to scare, anger, or shame those being targeted.

Cyberstalking:

Cyberstalking is the act of harassing or stalking another person online using the internet and other technologies. Cyberstalking is done through

texts, emails, social media posts, and other forms and is often persistent, methodical, and deliberate.

Cyber grooming:

The phenomenon of cyber grooming involves a person building a relationship with a teenager and having a strategy of luring, teasing, or even putting pressure on them to perform a sexual act.

Online job fraud:

An online job fraud scheme involves misleading people who require a job by promising them a better job with higher wages while giving them false hope. On March 21, 2022, the Reserve Bank of India (RBI) alerted people not to fall prey to job scams. By this, the RBI has explained the way in which online job fraud is perpetrated, as well as precautions the common man should take when applying for any job opportunity, whether in India or abroad.

Online sextortion:

The act of online sextortion occurs when the cybercriminal threatens any individual to publish sensitive and private material on an electronic medium. These criminals threaten in order to get a sexual image, sexual favour, or money from such individuals.

Phishing:

Fraud involving phishing is when an email appears to be from a legitimate source but contains a malicious attachment that is designed to steal personal information from the user such as their ID, IPIN, Card number, expiration date, CVV, etc. and then selling the information on the dark web.

Vishing:

In vishing, victims' confidential information is stolen by using their phones. Cybercriminals use sophisticated social engineering tactics to get victims to divulge private information and access personal accounts. In the same way as phishing and smishing, vishing convincingly fools victims into thinking that they are being polite by responding to the call.

Callers can often pretend that they are from the government, tax department, police department, or victim's bank..

Smishing:

As the name suggests, smishing is a fraud that uses text messages via mobile phones to trick its victims into calling a fake phone number, visiting a fraudulent website or downloading malicious software that resides on the victim's computer.

Credit card fraud or debit card fraud:

In credit card (or debit card) fraud, unauthorized purchases or withdrawals from another's card are made to gain access to their funds. When unauthorized purchases or withdrawals of cash are made from a customer's account, they are considered credit/debit card fraud. Fraudulent activity occurs when a criminal gains access to the cardholder's debit/credit number, or personal identification number (PIN). Your information can be obtained by unscrupulous employees or hackers.

Impersonation and identity theft:

A person is impersonated or exposed to identity theft when they make fraudulent use of an electronic signature, a password, or any other unique identifier on another person's behalf.

Prevention of cyber crimes

As per the recommendations of the **International Maritime Organization** (IMO), the cyber-attack risk must be approached using the following framework:

- The first step is to define the roles and responsibilities of the personnel responsible for cyber risk management.
- The second step is to identify the systems, assets, data, or capabilities that will put the operation at stake if disrupted.

- To protect against a potential cyber event and to maintain continuity of operations, it is important to implement risk-control processes and contingency plans.
- It is also important to develop and implement measures to detect a cyber-attack as quickly as possible.
- Preparation and implementation of plans to restore critical systems for continued operations by providing resilience.
- Finally, identify and implement measures to be taken to backup and restore any affected systems.

The following can be the strategies can be used to prevent cybercrime:

Analyze your risk exposure:

In order to adequately prepare for a cyberattack, you must assess the threat and give due consideration. Companies should consider the following:

- They should consider all areas where they are susceptible to cyberattacks and any operational vulnerabilities resulting from them.
- A vulnerability assessment of all systems is necessary to identify those that are critical to the business, to understand the potential exposures each has, and to assess the impact of any cyber-attack on business continuity.
- IT systems and operational technology systems should be checked by businesses.

Preventive measures:

It is recommended that businesses adopt national or international technical standards that provide a high level of protection. These general prevention measures are recommended for companies that currently lack the necessary technical or financial capabilities. The following is the list of preventive measures:

- Applying multiple layers of defence, beginning with physical security, followed by management policies and procedures, firewalls and network architecture, computer policies, account

management, security updates and finally antivirus applications.

- Implementing a principle of least privilege, which restricts information and access to only those set of people who needs to know that particular information.
- Implementing network-hardening measures, assuring patch management is sufficient and is proactively reviewed.
- Securing critical systems by utilizing technology such as protocol-aware filtering and segregation.
- Ensuring that removable devices are encrypted and that any USB used with any other device is tested for viruses.
- Furthermore, in order to prevent the negative impact of a cyberattack from further escalating and restoring business operations, it is important to develop business continuity plans, identify key personnel, and implement processes.
- Additionally, organising frequent training and awareness sessions for all employees can also help.
- Compliance audits of third-party service providers will also be beneficial.

Cybercrime laws in India

In terms of cybersecurity, there are five main types of laws that must be followed. Cyber laws are becoming increasingly important in countries such as India which have extremely extensive internet use. There are strict laws that govern the use of cyberspace and supervise the use of information, software, electronic commerce, and financial transactions in the digital environment. India’s cyber laws have helped to enable electronic commerce and electronic governance to flourish in India by safeguarding maximum connectivity and minimizing security concerns. This has also made digital media accessible in a wider range of applications and enhanced its scope and effectiveness.

Information Technology Act, 2000 (IT Act):

Overview of the Act:

It is the first cyber law to be approved by the Indian Parliament. The Act defines the following as its object:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

However, as cyber-attacks become dangerous, along with the tendency of humans to misunderstand technology, several amendments are being made to the legislation. It highlights the grievous penalties and sanctions that have been enacted by the Parliament of India as a means to protect the e-governance, e-banking, and e-commerce sectors. It is important to note that the IT Act's scope has now been broadened to include all the latest communication devices.

The Act states that an acceptance of a contract may be expressed electronically unless otherwise agreed and that the same shall have legal validity and be enforceable. In addition, the Act is intended to achieve its objectives of promoting and developing an environment conducive to the implementation of electronic commerce.

The important provisions of the Act

The IT Act is prominent in the entire Indian legal framework, as it directs the whole investigation process for governing cyber crimes. Following are the appropriate sections:

- **Section 43:** This section of the IT Act applies to individuals who indulge in cybercrimes such as damaging the computers of the victim, without taking the due permission of the victim. In such a situation, if a computer is damaged without the owner's consent, the owner is fully entitled to a refund for the complete damage.

In *Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others (2018)*, Rajesh Aggarwal of Maharashtra's IT

department (representative in the present case) ordered Punjab National Bank to pay Rs 45 lakh to Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. In this case, a fraudster transferred Rs 80.10 lakh from Matharu's account at PNB, Pune after the latter answered a phishing email. Since the complainant responded to the phishing mail, the complainant was asked to share the liability. However, the bank was found negligent because there were no security checks conducted against fraudulent accounts opened to defraud the Complainant.

- **Section 66**: Applies to any conduct described in Section 43 that is dishonest or fraudulent. There can be up to three years of imprisonment in such instances, or a fine of up to Rs. 5 lakh.

In *Kumar v. Whiteley (1991)*, during the course of the investigation, the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added, and changed files. As a result of investigations, Kumar had been logging on to a BSNL broadband Internet connection as if he was an authorized legitimate user and modifying computer databases pertaining to broadband Internet user accounts of subscribers. On the basis of an anonymous complaint, the CBI registered a cybercrime case against Kumar and conducted investigations after finding unauthorized use of broadband Internet on Kumar's computer. Kumar's wrongful act also caused the subscribers to incur a loss of Rs 38,248. N G Arun Kumar was sentenced by the Additional Chief Metropolitan Magistrate. The magistrate ordered him to undergo a rigorous year of imprisonment with a fine of Rs 5,000 under Sections 420 of IPC and 66 of the IT Act.

- **Section 66B:** This section describes the penalties for fraudulently receiving stolen communication devices or computers, and confirms a possible three-year prison sentence. Depending on the severity, a fine of up to Rs. 1 lakh may also be imposed.
- **Section 66C:** The focus of this section is digital signatures, password hacking, and other forms of identity theft. This section imposes imprisonment up to 3 years along with one lakh rupees as a fine.
- **Section 66D**: This section involves cheating by personation using computer Resources. Punishment if found guilty can be imprisonment of up to three years and/or up-to Rs 1 lakh fine.

- **Section 66E**: Taking pictures of private areas, publishing or transmitting them without a person's consent is punishable under this section. Penalties, if found guilty, can be imprisonment of up to three years and/or up-to Rs 2 lakh fine.
- **Section 66F**: Acts of cyber terrorism. An individual convicted of a crime can face imprisonment of up to life. An example: When a threat email was sent to the Bombay Stock Exchange and the National Stock Exchange, which challenged the security forces to prevent a terror attack planned on these institutions. The criminal was apprehended and charged under Section 66F of the IT Act.
- **Section 67**: This involves electronically publishing obscenities. If convicted, the prison term is up to five years and the fine is up to Rs 10 lakh.

Positive and negative aspects of the IT Act

This legislation contains the following benefits:

- Several companies are now able to conduct e-commerce without any fear because of the presence of this Act. Until recently, the development of electronic commerce in our country was hindered primarily due to a lack of legal infrastructure to govern commercial transactions online.
- Digital signatures are now able to be used by corporations to conduct online transactions. Digital signatures are officially recognized and sanctioned by the Act.
- Additionally, the Act also paves the way for corporate entities to also act as Certification Authorities for the issuance of Digital Signature Certificates under the Act. There are no distinctions in the Act as to what legal entity may be designated as a Certifying Authority, provided the government's standards are followed.
- Furthermore, the Act permits the companies to electronically file any of their documents with any office, authority, body or agency owned or controlled by the appropriate government by using the electronic form prescribed by that government.
- It also provides information on the security concerns that are so crucial to the success of the use of electronic transactions. As part of the Act, the term secure digital signatures were defined

and approved, which are required to have been submitted to a system of a security procedure. Therefore, it can be assumed that digital signatures are now secured and will play a huge part in the economy. Digital signatures can help conduct a secure online trade.

It is common for companies to have their systems and information hacked. However, the IT Act changed the landscape completely. A statutory remedy is now being provided to corporate entities in the event that anyone breaches their computer systems or network and damages or copies data. Damages are charged to anyone who uses a computer, computer system or computer network without the permission of the owner or other person in charge.

However, the said Act has a few problems:

- **Section 66A** is considered to be in accordance with **Article 19(2)** of the Constitution of India since it does not define the terms ‘offensive’ and ‘menacing’. It did not specify whether or not these terms involved defamation, public order, incitement or morality. As such, these terms are open to interpretation.
- Considering how vulnerable the internet is, the Act has not addressed issues such as privacy and content regulation, which are essential.
- A domain name is not included in the scope of the Act. The law does not include any definition of domain names, nor does it state what the rights and liabilities of domain name owners are.
- The Act doesn’t make any provision for the intellectual property rights of domain name proprietors. In the said law, important issues pertaining to copyright, trademark, and patent have not been addressed, therefore creating many loopholes.