What is Cyber-Crime?

Cyber-crime can be defined as a crime or an unlawful act where the computer is used either as a tool, a target or both. In other terms, cyber-crimes in India can be defined as an unauthorized access to some computer system without the permission of rightful owner or place of criminal activity and include everything from online cracking to denial-of-service attacks.

Some examples of cyber-crime include phishing, spoofing, DoS (Denial of Service) attack, credit card fraud, online transaction fraud, cyber defamation, child pornography, etc.

Cyber criminals always choose an easy way to make big money. They target rich people or rich organizations like banks, casinos and financial firms where the transaction of a huge amount of money is made on an everyday basis and hack sensitive information.

Catching such criminals is difficult. Hence, that increases the number of cyber-crimes. Computers are vulnerable, so laws are required to protect and safeguard them against cyber criminals.

Different Kinds of Cyber Crimes
The different kinds of cyber-crimes are:

1. Unauthorized Access and Hacking:

Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the

target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are the most targeted sites for the hackers.

2. Web Hijacking:

Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

3. Pornography:

Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.

4. Child Pornography:

The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cyber-crime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet. Pedophiles lure the children by distributing pornographic material and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Sometimes Pedophiles contact children in the chat rooms posing as teenagers or a child of similar age and then they start becoming friendlier with them and win their confidence. Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them some money or falsely promising them good opportunities in life. The pedophiles then sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet.

How do they operate?

- Pedophiles use false identity to trap the children/teenagers
- Pedophiles contact children/teens in various chat rooms which are used by children/teen to interact with other children/teen.
- Befriend the child/teen.
- Extract personal information from the child/teen by winning his confidence.
- Gets the e-mail address of the child/teen and starts making contacts on the victim's e-mail address.
- Starts sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
- Extract personal information from child/teen
- At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him into the net to further sexually assault him or to use him as a sex object.

5. Cyber Stalking:

In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber Stalking means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.

How do Cyber Stalkers operate?

- They collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

- The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.

- People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.

- Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

- Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.

- In online stalking the stalker can make third party to harass the victim.

- Follow their victim from board to board. They “hangout” on the same BB’s as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed. Many times they will “flame” their victim (becoming argumentative, insulting) to get their attention.

- Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.

- Contact victim via telephone. If the stalker is able to access the victim's telephone, he will many times make calls to the victim to threaten, harass, or intimidate them.

- Track the victim to his/her home.

6. Denial of service Attack:

This is an attack in which the criminal floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCp/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

7. Virus attacks:

Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attach themselves to other software. Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of themselves and do this repeatedly till they eat up all the available.

Trojan Horse is a program that acts like something useful but do the things that are quiet damping. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will

then use the Client to connect to the Server and start using the Trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

8. Software Piracy:

Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kinds of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber squatters register domain name identical to popular service provider's name so as to attract their users and get benefit from them.

9. Salami attacks:

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

10. Phishing:

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately.

11. Sale of illegal articles:

This category of cybercrimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

12. Online gambling:

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported.

13. Email spoofing:

Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.

14. Cyber Defamation:

When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation.

15. Forgery:

Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high-quality scanners and printers.

16. Theft of information contained in electronic form:

This includes theft of information stored in computer hard disks, removable storage media etc.

17. Email bombing:

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

18. Data diddling:

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

19. Internet time theft:

Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

20. Theft of computer system:

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

21. Physically damaging a computer system:

This crime is committed by physically damaging a computer or its peripherals.

22. Breach of Privacy and Confidentiality:

Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information.

Confidentiality means non-disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

Generally, for protecting secrecy of such information, parties while sharing information forms an agreement about, he procedure of handling of information and to not to disclose such information to third parties or use it in such a way that

it will be disclosed to third parties. Many times, party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality. Special techniques such as Social Engineering are commonly used to obtain confidential information.

23. Data diddling:

Data diddling involves changing data prior or during input into a computer. The information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also includes automatic changing the financial information for some time before processing and then restoring original information.

24. E-commerce/ Investment Frauds:

An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

25. Cyber Terrorism:

Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.

Cyber terrorism is an attractive option for modern terrorists for several reasons.

- It is cheaper than traditional terrorist methods.
- Cyber terrorism is more anonymous than traditional terrorist methods.
- The variety and number of targets are enormous.

- Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.

- Cyber terrorism has the potential to affect directly a larger number of people.

Concept of Cybercrime

Cybercrime refers to criminal activities that are carried out using computers, networks, and the internet. It encompasses a broad range of illegal activities, from financial fraud and data breaches to hacking, identity theft, and the spread of malware. The concept of cybercrime has evolved with the increasing reliance on technology and the internet in various aspects of our lives.

Key elements and types of cybercrime include:

1. **Unauthorized Access and Hacking:** Criminals gain unauthorized access to computer systems or networks to steal, manipulate, or delete data. This can also involve hacking into personal accounts or confidential databases.

2. **Malware:** Malicious software, such as viruses, worms, trojan horses, ransomware, and spyware, is designed to damage or disrupt computer systems, steal sensitive information, or gain unauthorized access.

3. **Phishing:** Cybercriminals use deceptive emails, websites, or messages to trick individuals into providing sensitive information, such as usernames, passwords, or financial details.

4. **Identity Theft:** Criminals steal personal information, such as social security numbers, credit card details, or bank account information, to commit fraud or other criminal activities in the victim's name.

5. **Financial Fraud:** Cybercriminals use various techniques, such as online scams, phishing, or hacking, to steal money or financial information from individuals, businesses, or financial institutions.

6. **Cyber Espionage:** State-sponsored or organized crime groups engage in cyber espionage to gain unauthorized access to sensitive information, trade secrets, or government data.

7. **Online Harassment and Cyberbullying**: Using online platforms to harass, threaten, or intimidate individuals, often through social media, email, or other communication channels.

8. **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:** These attacks aim to overwhelm a website or online service with traffic, rendering it unavailable to users.

9. **Child Exploitation:** The internet is sometimes used as a medium for the distribution of child pornography and other forms of exploitation.

10. **Cyber Terrorism:** The use of cyber tools to create fear, disrupt critical infrastructure, or cause harm for ideological, political, or religious reasons.

Addressing cybercrime requires a multi-faceted approach involving legal, technological, and educational measures. Law enforcement agencies, governments, businesses, and individuals all play a role in preventing and mitigating cyber threats. This includes implementing robust cybersecurity measures, staying informed about the latest threats, and promoting responsible online behaviour.

Categories of Cyber Crime

Cybercrime is a broad term that encompasses various criminal activities carried out using technology and the internet. These activities can be categorized into several types. Keep in mind that the boundaries between these categories are not always distinct, and many cybercrimes may involve elements of multiple categories. Here are some common categories of cybercrime:

1. **Financial Crimes:**

Online Fraud: Includes activities such as phishing, identity theft, and credit card fraud.

Cyber Espionage: Involves stealing sensitive information, trade secrets, or intellectual property for financial gain.

2. **Cyber Attacks:**

Malware: Includes viruses, worms, Trojans, and other malicious software designed to harm or exploit computer systems.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: Overwhelm a system or network, making it unavailable to users.

3. **Computer Hacking:**

Unauthorized Access: Gaining access to computer systems, networks, or data without permission.

SQL Injection and Cross-Site Scripting (XSS): Techniques used to exploit vulnerabilities in web applications.

4. **Online Harassment and Bullying:**

Cyberbullying: Harassment, threats, or intimidation using digital communication methods.

Online Stalking: Unwanted and obsessive attention through online channels.

5. Child Exploitation:

Child Pornography: Production, distribution, or possession of explicit material involving minors.

Online Grooming: Building an emotional connection with a minor for illicit purposes.

6. Intellectual Property Theft:

Software Piracy: Unauthorized distribution or use of software.

Digital Copyright Infringement: Unauthorized use or reproduction of digital content.

7. Cyber Terrorism:

Attacks on Critical Infrastructure: Targeting key systems such as power grids, transportation, or communication networks.

Propaganda and Recruitment: Using the internet to spread extremist ideologies and recruit members.

8. Online Scams:

Phishing: Deceptive attempts to acquire sensitive information by posing as a trustworthy entity.

Business Email Compromise (BEC): Manipulating employees to transfer funds or sensitive information through fraudulent emails.

9. Data Breaches:

Unauthorized Access to Data: Stealing or exposing sensitive information stored in databases.

Ransomware Attacks: Encrypting data and demanding payment for its release.

10.Social Engineering:

Manipulating People: Tricking individuals into revealing confidential information or performing actions against their best interests.

Virus

A computer virus is a type of malicious software or malware that is designed to infect and spread to other computer programs, files, or systems. It is called a "virus" because it behaves like a biological virus, capable of replicating itself and spreading from one host to another. The primary goal of a computer virus is to disrupt the normal functioning of a computer or network, often causing damage to data, hardware, or software.

Here are some key characteristics of computer viruses:

1. **Replication:** A computer virus can replicate itself by attaching its code to other programs or files. When these infected files are executed, the virus can spread to other parts of the system or to other connected systems.

2. **Concealment:** Viruses often try to conceal their presence to avoid detection. They may employ various techniques to hide within legitimate files or disguise their activities.

3. **Activation:** Some viruses are designed to remain dormant until a specific trigger event or condition is met. Once activated, they may perform malicious actions, such as deleting files, corrupting data, or spreading further.

4. **Payload:** The payload of a virus refers to the specific malicious actions it performs on an infected system. This could include stealing sensitive information, displaying unwanted messages, or even rendering the system inoperable.

5. **Propagation:** Viruses spread from one system to another through various means, such as infected email attachments, malicious downloads, or exploiting vulnerabilities in software.

To protect against computer viruses, it is essential to use antivirus software, keep operating systems and software up-to-date, be cautious of email attachments and downloads from unknown sources, and regularly back up important data. Security best practices help minimize the risk of virus infections and mitigate potential damage.

Worms

A computer worm is a type of malicious software (malware) that is designed to spread across computer networks, often without user intervention. Unlike viruses, worms do not need a host program to attach themselves to; instead, they can replicate and spread independently. Worms can exploit vulnerabilities in operating systems, network protocols, or other software to gain access to a computer, and once inside, they can replicate and spread to other connected systems.

The primary goal of computer worms is to propagate and spread rapidly, often causing harm by consuming system resources, slowing down network performance, or even damaging files and data. Some worms are designed with specific payloads, such as deleting files, stealing sensitive information, or creating backdoors for remote access by attackers.

Worms can spread through various means, including email attachments, malicious websites, or exploiting vulnerabilities in software. To protect against worms and other malware, it is crucial for users to keep their software up to date, use antivirus and anti-malware tools, and practice safe computing habits such as avoiding suspicious links and attachments.

Software Piracy

Software piracy refers to the unauthorized use, reproduction, distribution, or sale of software. This illegal activity typically involves copying or downloading software without the proper license or permission from the copyright owner. Software piracy can take various forms, including:

Counterfeiting: Producing and selling unauthorized copies of software, often packaged to look like legitimate versions.

Internet Piracy: Illegally downloading or sharing software from the internet without the appropriate license.

End-User Piracy*:* Using a single licensed copy of software on multiple computers or by multiple users, exceeding the terms of the software license.

Corporate Piracy: Organizations using unauthorized copies of software across their network, either knowingly or unknowingly.

Software Key/Crack Distribution*:* Distributing or using unauthorized software keys, cracks, or patches to bypass licensing restrictions.

Software License Violation: Violating the terms and conditions of a software license agreement.

Software piracy has significant negative consequences for both individuals and the software industry. It results in financial losses for software developers and publishers, undermines innovation, and can lead to a decrease in overall software quality and support. It's important for individuals and organizations to respect software licenses, as well as for governments and industry stakeholders to enforce copyright laws to combat piracy.

To combat software piracy, many software companies implement various security measures, such as product activation, serial number verification, and digital rights management (DRM) technologies. Additionally, legal actions can be taken against individuals or entities engaging in software piracy. Education and awareness campaigns are also crucial to informing users about the importance of using legitimate software and respecting intellectual property rights.

Web Jacking

Illegally seeking control of a website by taking over a domain is known as Web Jacking. In web jacking attack method hackers' compromises with the domain name system (DNS) that resolves website URL to IP address but the actual website is never touched. Web jacking attack method is another type of social engineering phishing attack where an attacker create a fake web page of victim website and send it to the victim and when a victim click on that link, a message display on the browser "the site abc.com has move on another address, click here to go to the new location" and if a victim does click on the link, he/she will redirect on the fake website page where an attacker can ask for any sensitive data such as credit card number, username, password etc. Web jacking attack method is one kind of trap which is spread by the attacker to steal the sensitive data of any people, and those people got trapped who are not aware about cyber security.
Web Jacking Attack Method:

1. The first step of web jacking attack method is to create a fake page of victim website for example www.anywebsite.com/login.php.
2. The second step is to host it either on your local computer or shared hosting.
3. The third step is to send the link of a fake page to the victim.
4. The fourth step victim will open the link and enter their details and submit.
5. Last step, you will get all the details submitted by victim.

How to apply web jacking attack method:

Step-1: So to apply web jacking attack method we will use a tool in kali linux called setoolkit.

Step-2: Open your kali linux operating system, and then open Terminal window.

Step-3: Type setoolkit on the terminal.

Step-4: It will display lots of attacking method but you have to select Social-engineering attack.

Step-5: Type 1 to select Social-engineering attack, it will display lots of social engineering attack method. Here, you have to select website attack vector, so type 2, it will display different website attack method. Above methods will create a fake website page same as victim website page and host it on your computer.

Step-6: Copy the link(your computer IP which you entered previously) of fake website and send it to the victim. If the link is your local computer IP address then convert it into domain name. To convert your IP address in domain name, open the link and type your computer IP address here, it will create a link. Now, your link is ready copy it and send it to the victim and wait till he/she entered their details.

Step-7: When a victim will open the link in their browser, the browser display the message “the site www.abc.com has move on another address, click here to go to the new location” and if the victim clicks on this link he will get redirected on the fake webpage.

How to be safe from web jacking attack method !

1. First of all do not enter sensitive data in any link sent to you.
2. Check the URL
3. Just because the address looks Ok, don’t assume this is a legitimate site.
4. Read company name carefully, is it right or wrong.
5. check that there is http protocol or https, if http then do not enter your data.
6. If you are not sure, site is real or fake, enter a wrong username and password.
7. Use a browser with antiphishing detection.

Web Defacement

Web defacement refers to the unauthorized alteration or modification of the content on a website by an individual or group, often with the intent of conveying a message, expressing dissent, or causing disruption. This can involve changing the visual appearance of a website, replacing the original content with a different message, or adding images and text to make a statement.

Web defacement is considered a form of cyber-attack and is typically carried out by hackers or hacktivist groups. These individuals may exploit vulnerabilities in a website's security, such as weak passwords, outdated software, or other security loopholes, to gain unauthorized access and make changes to the site.

The motives behind web defacement can vary widely. Some defacements are politically motivated, with attackers seeking to express their views or protest against a particular cause. Others may be carried out for personal satisfaction, as a form of vandalism, or to gain attention.

Website owners and administrators typically respond to web defacements by restoring the original content and addressing the security vulnerabilities that allowed the attack to occur. This involves removing unauthorized changes, fixing security flaws, and implementing measures to prevent future attacks.

To protect against web defacement, website owners should prioritize security measures, such as using strong and unique passwords, keeping software up-to-date, regularly auditing and monitoring their websites for vulnerabilities, and implementing security protocols, such as firewalls and intrusion detection systems.

Cyber Stalking

In Cyber Stalking, a cyber criminal uses the internet to consistently threaten somebody. This crime is often perpetrated through email, social media, and the other online medium. Cyber Stalking can even occur in conjunction with the additional ancient type of stalking, wherever the bad person harasses the victim offline. There's no unified legal approach to cyber Stalking, however, several governments have moved toward creating these practices punishable by law. Social media, blogs, image sharing sites and lots of different ordinarily used online sharing activities offer cyber Stalkers with a wealth of data that helps them arrange their harassment. It includes actions like false accusations, fraud, information destruction, threats to life and manipulation through threats of exposure. It has stalkers take the assistance of e-mails and other forms of message applications, messages announce to an online website or a discussion cluster, typically even the social media to send unwanted messages, and harass a specific person with unwanted attention. Cyber Stalking is typically cited as internet stalking, e-stalking or online stalking.

Types of Cyber Stalking:

- **Webcam Hijacking:** Internet stalkers would attempt to trick you into downloading and putting in a malware-infected file that may grant them access to your webcam. the method is therefore sneaky that it's probably you wouldn't suspect anything strange.
- **Observing location check-ins on social media:** In case you're adding location check-ins to your Facebook posts, you're making it overly simple for an internet stalker to follow you by just looking through your social media profiles.
- **Catfishing:** Catfishing happens via social media sites, for example, Facebook, when internet stalkers make counterfeit user-profiles and approach their victims as a companion of a companion.
- **Visiting virtually via Google Maps Street View:** If a stalker discovers the victim's address, then it is not hard to find the area, neighbourhood, and surroundings by using Street View. Tech-savvy stalkers don't need that too.
- **Installing Stalkerware:** One more method which is increasing its popularity is the use of Stalkerware. It is a kind of software or spyware which keeps track

of the location, enable access to text and browsing history, make an audio recording, etc. And an important thing is that it runs in the background without any knowledge to the victim.

- **Looking at geotags to track location:** Mostly digital pictures contain geotags which is having information like the time and location of the picture when shot in the form of metadata. Geotags comes in the EXIF format embedded into an image and is readable with the help of special apps. In this way, the stalker keeps an eye on the victim and gets the information about their whereabouts.

Protective Measures:

- Develop the habit of logging out of the PC when not in use.
- Remove any future events you're close to attending from the social networks if they're recorded on online approaching events and calendars.
- Set strong and distinctive passwords for your online accounts.
- Cyber Stalkers can exploit the low security of public Wi-Fi networks to snoop on your online activity. Therefore, avoid sending personal emails or sharing your sensitive info when connected to an unsecured public Wi-Fi.
- Make use of the privacy settings provided by the social networking sites and keep all info restricted to the nearest of friends.
- Do a daily search on the internet to search out what information is accessible regarding you for the public to check.

Cyber Pornography

Cyber pornography, often referred to as online pornography, involves the use of the internet and digital technology to create, distribute, or consume sexually explicit material. This can include images, videos, or other forms of media that are intended to sexually arouse or satisfy individuals. It is a subset of the broader category of pornography but specifically focuses on content that is disseminated through online platforms.

The availability of the internet has significantly changed the landscape of pornography, making it more accessible to a global audience. While some people view and produce adult content consensually, the production and distribution of explicit material can sometimes involve illegal or unethical activities, such as non-consensual sharing of intimate images (revenge porn), exploitation, child pornography, or human trafficking.

Laws regarding cyber pornography vary across different countries, and many jurisdictions have measures in place to combat illegal and harmful activities related to online adult content. It's important to distinguish between consensual adult content and illegal activities, and to be aware of and comply with local laws and regulations. Additionally, promoting a safe and consensual approach to adult content consumption is essential to respect individuals' rights and well-being.

Hacking

Hacking (also called cyber hacking) is the use of unconventional or illicit means to gain unauthorized access to a digital device, computer system or computer network.

The classic example of a hacker is a cybercriminal who exploits security vulnerabilities or overcomes security measures to break into a computer or computer network to steal data. But hacking does not always have malicious intent. A consumer who jiggers their personal smartphone to run custom programs is also, technically speaking, a hacker.

Malicious hackers have built a enormous cybercrime economy, where outlaws profit by launching cyberattacks or selling malware or stolen data to one another. By one estimate (link resides outside ibm.com), this underground market is the world's third-largest economy behind the US and China.

On the other end of the hacking spectrum, the cybersecurity community depends increasingly on ethical hackers—hackers with helpful rather than criminal intentions—to test security measures, identify and address security flaws, and prevent cyberthreats. Ethical hackers make an excellent living by helping companies shore up their security systems, or by working with law enforcement to take their malicious counterparts down.

Malicious hackers

Malicious hackers (sometimes called “black hat hackers”) carry out cyberattacks themselves, or develop malware or exploits that they sell to other hackers on the dark web (see, for example, ransomware-as-a-service arrangements). They may work alone or as part of an organized hacker or cybercriminal group.

Financial gain is the most common motivator for malicious hackers. Typically, they

- Steal information or personal data—login credentials, credit card numbers, bank account numbers, social security numbers—they can use to break into other systems or commit identity theft.

- Launch social engineering attacks, such as phishing or business email compromise scams, to trick people into sending money or sensitive data to them.

- Practice extortion—e.g., use ransomware attacks or distributed denial of service (DDoS) attacks to hold data, devices or business operations hostage until the victim pays a ransom. According to the X-Force Threat Intelligence Index, 27 percent of cyberattacks extort their victims.

- Conduct corporate espionage for hire, stealing intellectual property or other sensitive from their client company's competitiors.

But malicious hackers can have different or additional motivations for committing or enabling cyberattacks. For example, a disgruntled employee might hack an employer's system purely for spite over being denied a promotion.

Ethical hackers

Ethical hackers (sometimes called "white hat hackers") use their skills to help companies find and fix security vulnerabilities so malicious actors can't use them.

Ethical hacking is a legitimate profession, and ethical hackers often work as security consultants or employees of the companies they're hacking. Ethical hackers follow a strict code of conduct: they always get permission before they hack, don't do any damage, and keep their findings confidential.

One of the most common ethical hacking services is penetration testing, in which hackers launch mock cyberattacks against web applications, networks, or other assets to find their weaknesses. They then work with the owners of the assets to remediate those weaknesses. Ethical hackers may also conduct vulnerability assessments, analyze malware to gather threat intelligence, or participate in secure software development lifecycles.

Other types of hackers

Some hackers don't fit neatly into the ethical or malicious camps. These hackers (sometimes called “gray hat hackers”) break into systems without permission, but they don't do it for malicious purposes. Instead, these hackers tell the companies they hack about the flaws they find in their systems. They may offer to fix vulnerabilities in exchange for a fee or even a job offer. While they have good intentions, these vigilante hackers can accidentally tip off malicious hackers about new attack vectors.

Some amateur programmers simply hack for fun, to learn new things, or to gain notoriety for breaching difficult targets.

‘Hacktivists’ are activists who hack systems to bring attention to social and political issues. The loose collective Anonymous is probably the most well-known hacktivist group, having staged attacks against targets like the Russian government (link resides outside ibm.com).

State-sponsored hackers have the official backing of a nation-state. They work with a government to spy on adversaries, disrupt critical infrastructure, or spread misinformation. Whether these hackers are ethical or malicious is in the eye of the beholder. For example, the Stuxnet attack on Iranian nuclear facilities—believed to have been carried out by the US and Israeli governments—is likely to be considered ethical by anyone who views Iran's nuclear program as a threat.

Hacking tools

There's no such thing as a “typical” hack. Hackers use different tactics depending on their goals and the systems they're targeting. A hack can be as simple as sending out mass phishing emails to steal passwords from anyone who bites or as elaborate as an advanced persistent threat (APT) that secretly lurks in a network for months, waiting for the chance to strike.

That said, hackers do share a standard set of tools they tend to use.

Specialized operating systems: While hackers can launch attacks from standard Mac or Microsoft operating systems, many use customized OSs. For example, Kali Linux, an open-source Linux distribution designed for penetration testing, is popular among ethical hackers.

Credential-cracking tools: These programs can uncover passwords by breaking encryptions or launching brute-force attacks, which use bots or scripts to automatically generate and test potential passwords until one works.

Port scanners: Port scanners remotely test devices for open and available ports, which hackers can use to gain access to a network.

Vulnerability scanners: Vulnerability scanners search systems for known vulnerabilities, allowing hackers to quickly find entryways into a target.

Packet analyzers: These tools analyze network traffic to determine where it's coming from, where it's going, and—in some cases—what data it contains.

Malware: Malicious software, or malware, is a key weapon in malicious hackers' arsenals. Some of the most commonly used malware types include:

- Ransomware locks up a victim's devices or data and demands a ransom payment to unlock them.
- Botnets are networks of internet-connected, malware-infected devices under a hacker's control. Hackers often use botnets to launch distributed denial of service (DDoS) attacks.
- Trojan horses disguise themselves as useful programs or hide within legitimate software to trick users into installing them. Hackers use Trojans to secretly gain remote access to devices or download additional malware without users knowing.
- Spyware secretly gathers sensitive information—like passwords or bank account details—and transmits it back to the attacker.

What is phishing?

Phishing attacks are fraudulent emails, text messages, phone calls or web sites designed to trick users into downloading malware, sharing sensitive information or personal data (e.g., Social Security and credit card numbers, bank account numbers, login credentials), or taking other actions that expose themselves or their organizations to cybercrime.

Successful phishing attacks often lead to identity theft, credit card fraud, ransomware attacks, data breaches, and huge financial losses for individuals and corporations.

Phishing is the most common type of social engineering, the practice of deceiving, pressuring or manipulating people into sending information or assets to the wrong people. Social engineering attacks rely on human error and pressure tactics for success. The attacker typically masquerades as a person or organization the victim trusts—e.g., a coworker, a boss, a company the victim or victim's employer does business with—and creates a sense of urgency that drives the victim to act rashly. Hackers and fraudsters use these tactics because it's easier and less expensive to trick people than it is to hack into a computer or network.

According to the FBI, phishing emails are the most popular attack method, or vector, used by hackers to deliver ransomware to individuals and organizations. IBM's Cost of a Data Breach 2022 found that phishing is the second most common cause of a data breach (up from fourth most common last year), and that data breaches caused by phishing were the most expensive, costing victims USD 4.91 million on average.

Types of phishing attacks

Bulk phishing emails

Bulk email phishing is the most common type of phishing attack. A scammer creates an email message that appears to come from a large, well-known legitimate business or organization—a national or global bank, a large online retailer, the makers of a popular software application or app—and sends the message to millions of recipients. Bulk email phishing is a numbers game: The

larger or more popular the impersonated sender, the more recipients who are likely to customers, subscribers or members.

Cybercriminals go to various lengths to make the phishing email appear legitimate. They typically include the impersonated sender's logo in the email, and mask the 'from' email address to include impersonated sender's domain name; some will even spoof the sender's domain name—e.g., using 'rnicrosoft.com' instead of 'microsoft.com'—to appear legit at a glance.

The subject line addresses a topic that the impersonated sender might credibly address, and that appeals to strong emotions—fear, greed, curiosity, a sense of urgency or time pressure—to get the recipient's attention. Typical subject lines include 'Please update your user profile,' 'Problem with your order,' 'Your closing documents are ready to sign,' Your invoice is attached.'

The body of the email instructs the recipient to take an action that seems perfectly reasonable and consistent with the topic, but will result in the recipient divulging sensitive information—social security numbers, bank account numbers, credit card numbers, login credentials—or downloading a file that infects the recipient's device or network.

For example, recipients might be directed to 'click here to update your profile', but the underlying hyperlink takes them to a fake website that tricks them into entering their actual login credentials as part of the profile update process. Or they may be told to open an attachment that appears to be legitimate (e.g., 'invoice20.xlsx') but that delivers malware or malicious code to the recipient's device or network.

Spear phishing

Spear phishing is a phishing attack that targets a specific individual—usually a person who has privileged access to sensitive data or network resources, or special authority that the scammer can exploit for fraudulent or nefarious purposes.

A spear phisher studies the target to gather information needed to pose as a person or entity the target truly trusts—a friend, boss, co-worker, colleague, trusted vendor or financial institution—or to pose as the target individual. Social media and social networking sites—where people publicly congratulate coworkers, endorse colleagues and vendors, and tend to overshare about meetings or events or travel plans—have become rich sources of information for spear phishing research.

With this information the spear phisher can send a message containing specific personal details or financial information and a credible request to the target—as in, 'I know you're leaving tonight for vacation—but can you please pay this invoice (or transfer USDXXX.XX to this account) before close of business today?'

A spear phishing attack aimed a C-level executive, a wealthy individual or some other high-value target is often called a whale phishing or whaling attack.

Business email compromise (BEC)

BEC is a class of spear phishing attack that attempts to steal large sums of money or extremely valuable information—e.g. trade secrets, customer data, financial information—from corporations or institutions.

BEC attacks can take several different forms. Two of the most common include:

CEO fraud: The scammer impersonates a C-level executive's email account, or hacks into it directly, and sends a message to a lower-level employee instructing them to transfer funds to a fraudulent account, make a purchase from a fraudulent vendor, or send files to an unauthorized party.

Email account compromise (EAC): Here the scammer gains access to the email account of a lower-level employee—e.g., a manager in finance, sales, R&D—and uses it to send fraudulent invoices to vendors, instruct other employees to make fraudulent payments or deposits, or request access to confidential data.

As part of these attacks, scammers often gains access to company email accounts by sending an executive or employee a spear phishing message that tricks them into divulging email account credentials (username and password). For example, a message such as ‘Your password is about to expire. Click this link to update your account’ might conceal a malicious link to a fake website designed to steal account information.

Other phishing techniques and tactics

SMS phishing, or smishing, is phishing using mobile or smartphone text messages. The most effective smishing schemes are contextual—that is, related to smartphone account management or apps. For example, recipients may receive a text message offering a gift as 'thanks' for paying a wireless bill, or asking them to update their credit card information in order to continue using a streaming media service.

Voice phishing, or vishing, is phishing via phone call. Thanks to voice over IP (VoIP) technology, scammers can make millions of automated vishing calls per day; they often use caller ID spoofing to make their calls appear as if they're made from legitimate organizations or local phone numbers. Vishing calls typically scare recipients with warnings of credit card processing problems, overdue payments or trouble with the IRS. Callers who respond end up providing sensitive data to people working for the cybercriminals; some even end up granting remote control of their computers to the scammers on the other end of the phone call.

Social media phishing employs various capabilities of a social media platform to phish for members' sensitive information. Scammers use the platforms' own messaging capabilities—e.g., Facebook Messenger, LinkedIn messaging or InMail, Twitter DMs—in much the same ways they use regular email and text messaging. They also send users phishing emails that appear to come from the social networking site, asking recipients to update login credentials or payment information. These attacks can be especially costly to victims who use the same login credentials across multiple social media sites, an all-too-common 'worst practice.'

Application or in-app messaging. Popular mobile device apps and web-based (software-as-a-service, or SaaS) applications email their users regularly. As a result, these users are ripe for phishing campaigns that spoof emails from app or software vendors. Again playing the numbers game, scammers will typically spoof emails from the most popular apps and web applications—e.g. PayPal, Microsoft Office 365 or Teams—to get the most bang for their phishing buck.

What is Internet Fraud?

Internet fraud involves using online services and software with access to the internet to defraud or take advantage of victims. The term "internet fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money.

Here are some common types of e-fraud:

1. **Phishing:** Involves tricking individuals into revealing sensitive information, such as usernames, passwords, or credit card numbers, by posing as a trustworthy entity in electronic communication.

2. **Identity Theft:** The unauthorized use of someone else's personal information, such as Social Security numbers or credit card details, to commit fraud or other crimes.

3. **Online Scams:** Various scams can occur online, such as lottery scams, romance scams, or fake job offers designed to trick people into sending money or providing personal information.

4. **Credit Card Fraud:** Illegitimate use of credit card information to make unauthorized purchases.

5. **Malware and Ransomware:** Malicious software or code that is designed to damage or gain unauthorized access to computer systems. Ransomware encrypts files and demands payment for their release.

6. **Account Takeover (ATO):** Unauthorized access to someone else's online account, often through stolen credentials obtained from data breaches or phishing.

7. **Business Email Compromise (BEC):** Involves attackers compromising business email accounts to conduct fraudulent activities, such as unauthorized fund transfers.

8. **Online Auction and Shopping Fraud:** Scams related to online auctions, fake online stores, or deceptive product listings that lead to financial loss for consumers.

Threatening Email

A threatening email is a message sent via email that includes language or content intended to intimidate, harm, or cause fear to the recipient. Threatening emails can take various forms, such as explicit threats of physical harm, emotional abuse, blackmail, extortion, or any other form of malicious intent. The content of these emails may include aggressive language, explicit threats, or attempts to coerce the recipient into taking certain actions against their will.

Threatening emails can be sent by individuals, groups, or even automated systems, and they may be motivated by personal vendettas, harassment, extortion attempts, or other malicious purposes. In many cases, threatening emails can be a form of cyberbullying or online harassment.

Types of email security threats

Email remains the undisputed primary medium used to conduct cyberattacks. As cybercriminals become more sophisticated in launching email attacks, we've seen popular and damaging email threats rapidly evolve.

Common types of email threats such as:

Malware: a broad category of email threats that comprises software designed to damage systems or gain unauthorized access to mission critical systems.

Phishing emails: A form of email fraud where cybercriminals impersonate reputable entities to gain access to sensitive information.

Ransomware: A type of email-borne threat which uses software to block access to files usually containing important intellectual property. Access to infected files cannot be accessed until a sum of money is paid to the anonymous cybercriminal. Spoiler, the sum of money required is never cheap!

Email spoofing: A form of email threat where attackers fabricate email headers to give the illusion they have originated from trusted sources. Individuals are tricked into divulging sensitive information.

Spam: Irrelevant email messages sent on large scales to unexpecting recipients. Spam can massively impact an organization's productivity if left unchecked. Organizations large and small rely on email spam filters.

Cyber Terrorism

Cyberterrorism refers to the use of technology to conduct terrorist activities, including attacks on computer systems, networks, and infrastructure. It involves the use of digital tools and techniques to create fear, disrupt operations, and cause harm on a large scale. Cyberterrorists leverage the vulnerabilities of digital systems to achieve their objectives, which can range from spreading propaganda and inciting fear to causing significant economic damage or compromising national security.

Some common forms of cyberterrorism include:

Denial-of-Service (DoS) Attacks: These attacks overwhelm a target's computer systems or network with a flood of traffic, making it unavailable to users.

Malware Attacks: Cyberterrorists may use malicious software, such as viruses, worms, or ransomware, to compromise and control computer systems or steal sensitive information.

Cyber Espionage: Gathering classified or sensitive information from government, military, or corporate networks to use for political or economic gain.

Social Engineering: Manipulating individuals or groups to divulge confidential information or perform actions that compromise security.

Critical Infrastructure Attacks: Targeting essential systems like power grids, water supplies, or transportation networks to disrupt normal functioning and create chaos.

Propaganda and Psychological Warfare: Spreading propaganda, misinformation, or fear through online channels to achieve political or ideological goals.

Governments, businesses, and organizations invest significant resources in cybersecurity measures to protect against cyberterrorism. This includes implementing firewalls, intrusion detection systems, encryption, and regular security assessments. International cooperation is also crucial to addressing cyber threats, as many cyberattacks can originate from different parts of the world.

Efforts to combat cyberterrorism involve a combination of legal, technical, and diplomatic measures. Governments and international organizations work together to establish laws and agreements that help prosecute cybercriminals and prevent the spread of cyber threats. Cybersecurity professionals play a crucial role in developing and implementing strategies to detect, prevent, and respond to cyberterrorism incidents.