Cyber crime, Hacking - Avanthika

Cyber trolls and bullying - Joshitha

Spreading rumours, Online fraud - Fauziyya

Cyber stalking, Explicit content - Mahathi

Information theft, Scamming- Swathi

Piracy, forgery, Reporting cyber crime - Biancaa

Avan : Information and Communication Technology has interconnected the world and created interdependencies that we've never seen. We're a global village and what happens in one part of the world affects all of us. We live in an era where digital evidence is rampant in every crime.

Josh : Cybercrime doesn't stay still. It's constantly evolving. We see it in human trafficking. We see it in drugs related offences and terrorism. We see it in money laundering. We see it in firearms trafficking. Pure cybercrime as well.

Fauziyya : Sometimes you're exposed without knowing you're exposed. They can actually simultaneously steal information from potentially millions of people at one time. And then that data itself has now become a market in its own right. It is a daily challenge.

Mahathi : All of us are using electronic devices, all of this becomes open to criminal activity of various forms from cyber bullying in social media to cyber organized crime to governments engaging in certain forms of cyber activity. Cybercrime is huge. The average user of a digital device can be up against the very best cyber criminals anywhere in the world.

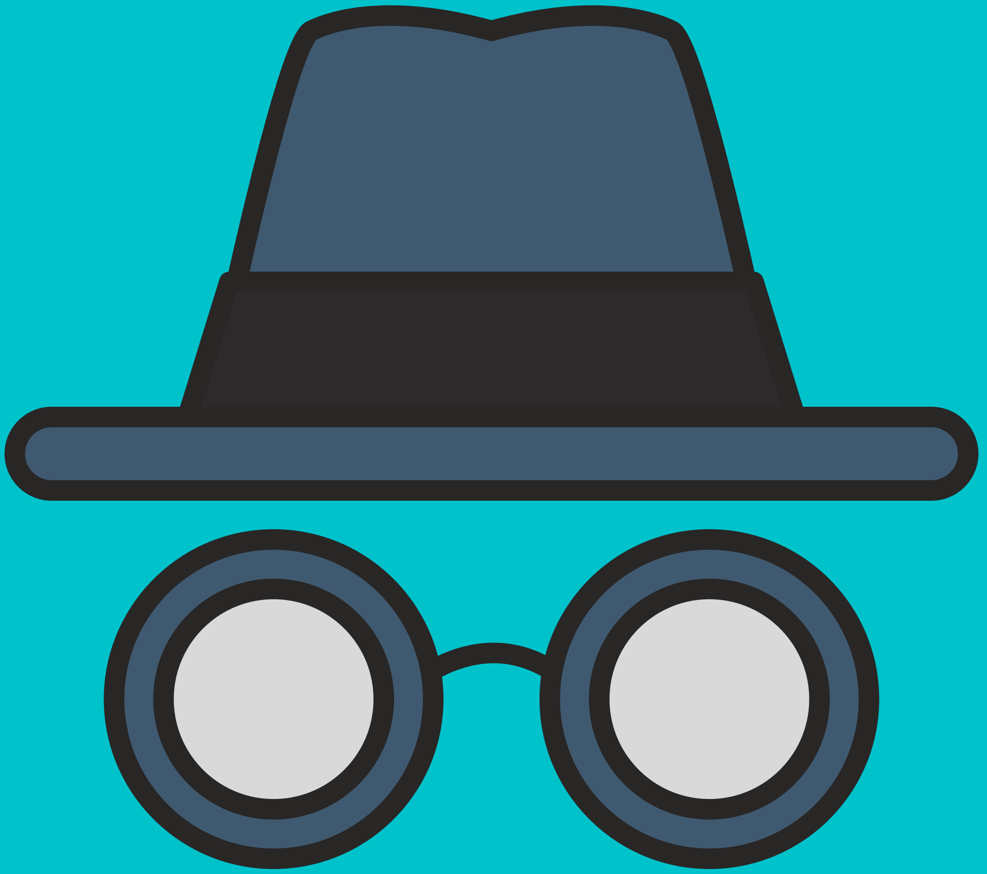
Biancaa : It's not that you're not going to be a victim but it's a matter of when. If we don't understand this technology, if we don't understand its vulnerabilities, it puts us at risk and it not only puts our own country at risk but any other country that we're connected with, we put them at risk as well.

Swathy : Globally, even in advanced countries, there is a real lack of capacity in dealing with cybercrime issues. Cybercrime is a borderless crime by definition. You can't change it.

Intro to cybercrime(Avanthika)

(PPT Image)

Voice



Avanthika :

Video :

When you hear the word "cybercriminal" or "hacker," what image comes to mind? Is it a sketchy guy, perhaps wearing a dark hoodie, camped out in a dank basement somewhere, typing away furiously? While that image is in the public consciousness thanks to movies and TV, the real picture of a cybercriminal is much different: **cybercrime is incredibly professionalized and very well organised**.

Video :

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

Cybercriminals buy and sell malware online (generally on the dark web) while also trading in services that test how robust a virus is, business intelligence dashboards to track malware deployment, and tech support (that's right – crooks can contact a criminal helpline to troubleshoot their illegal hacking server or other malfeasance!)

PPT :

The professionalization and proliferation of cybercrime adds up to countless costs in damages every year, impacting individuals, businesses, and even governments. Experts estimate that cybercrime damages will reach $6 trillion annually by 2021, making it one of the most lucrative criminal enterprises.

As the Internet of Things (IoT) evolves and smart devices become more popular, cybercriminals benefit from a much broader attack surface – increased opportunities to penetrate security measures, gain unauthorized access, and commit crimes.

As the saying goes, there's more than one way to skin a cat – and there are most certainly a variety of ways to make money as a cybercriminal.

Video :

As mentioned, cybercriminals range from individuals to criminal organizations to state-sponsored actors. Just as the type of criminal varies, so do their crimes and the methods they use to break the law. From a single hacker who managed to hack into the US stock market to North Korean state-sponsored groups that propagated ransomware on a massive scale, there are a staggering amount of cybercriminals active every day. Moreover, expert skills are no longer required to become a cybercrook.

Now here are some standout examples of cybercrime to watch out for.

Hacking(Avanthika)

(PPT Image)

Voice

Video:

While breaching privacy to detect cybercrime works well when the crimes involve the theft and misuse of information, ranging from credit card numbers and personal data to file sharing of various commodities—music and videos,..what of crimes that attempt to wreak havoc on the very workings of the machines that make up the network?

The story of hacking actually goes back to the 1950s, when a group of phreaks, (short for “phone freaks”) began to hijack portions of the world’s telephone networks, making unauthorized long-distance calls and setting up special “party lines” for fellow phreaks. By the late 1970s, the informal phreaking culture began to coalesce into quasi-organized groups of individuals who graduated from the telephone network to “hacking” corporate and government computer network systems.

PPT:

The term "hacker" has come to refer to individuals who gain unauthorized access to computer networks, whether from another computer network or, as personal computers became available, from their own computer systems. One thing to notice is that most hackers have not been criminals in the sense of being vandals or of seeking illicit financial rewards.

Instead, most have been young people driven by intellectual curiosity. However, as some hackers sought notoriety among their peers, their exploits lead to clear-cut crimes. These exploits grew as hackers not only broke into but sometimes took control of government and corporate computer networks.

The scale of hacking crimes is among the most difficult to assess because the victims often prefer not to report the crimes—sometimes out of embarrassment or fear of further security breaches. Officials estimate, however, that hacking costs the world economy billions of dollars annually.

And on the other hand, not all hackers are criminals, who are also known as black-hat hackers. There are a few who are called "white-hat" hackers, meaning, they practice ethical hacking. It is nothing but identifying weakness in computer systems or computer networks and coming up with countermeasures that protect these weaknesses.

Cyber Bullying(Joshitha)

(PPT Image)

Voice

Video :

Cyberbullying or cyberharassment is a form of bullying or harassment using electronic means. It is also known as online bullying.
Cyber bullying is when someone is targeting you online, doing or saying things that upset you, or trying to make you look bad to others.

This could be by writing nasty things about you, either in a public way, like commenting on a YouTube video, replying on Twitter or tweeting about you, writing Facebook posts about you or commenting on your posts, writing a blog about you, etc. Or it could be a more private bully, who may send you emails, Facebook PMs, private Twitter and Instagram messages, and so on.

PPT :

Now let's see what are the common types of cyberbullying that happens today

Exclusion is the act of leaving someone out deliberately. For example, a person might be excluded/uninvited to groups or parties while they see other friends being included, or left out of message threads or conversations that involve mutual friends.

Harassment is a broad category under which many types of cyberbullying fall into, but it generally refers to a sustained and constant pattern of hurtful or threatening online messages sent with the intention of doing harm to someone.

Outing, also known as doxing, refers to the act of openly revealing sensitive or personal information about someone without their consent for purposes of embarrassing or humiliating them. This can range from the spreading of personal photos or documents of public figures to sharing an individual’s saved personal messages in an online private group.

Trickery is similar to outing, with an added element of deception. In these situations, the bully will befriend their target and lull them into a false sense of security. Once the bully has gained their target’s trust, they abuse that trust and share the victim’s secrets and private information to a third party or multiple third parties.

PPT :

Cyberstalking is a form of online harassment in which the perpetrator uses electronic communications to stalk a victim. This is considered more dangerous than other forms of cyberbullying because it generally involves a credible threat to the victim's safety.

Fraping is when a bully uses a person’s social networking accounts to post inappropriate content with their name. It can be harmless when friends write funny posts on each other’s profiles, but has potential to be incredibly harmful.

Masquerading happens when a bully creates a made up profile or identity online with the sole purpose of cyberbullying someone. This could involve creating a fake email account, fake social media profile, and selecting a new identity and photos to fool the victim.

Dissing refers to the act of a bully spreading cruel information about their target through public posts or private messages to either ruin their reputation or relationships with other people. In these situations, the bully tends to have a personal relationship with the victim, either as an acquaintance or as a friend.

Video :

When bullying happens online it can feel as if you’re being attacked everywhere, even inside your own home. It can seem like there’s no escape. The effects can last a long time and affect a person emotionally, physically and mentally. The feeling of being laughed at or harassed by others, can prevent people from speaking up or trying to deal with the problem. In extreme cases, cyberbullying can even lead to people taking their own lives. So,..what can you do to handle it?

If you think you’re being bullied, the first step is to seek help from someone you trust such as your parents, a close family member or another trusted adult. In your school you can reach out to a counsellor or your favourite teacher. And if you are not comfortable talking to someone you know, search for a helpline to talk to a professional counsellor.

If the bullying is happening on a social platform, consider blocking the bully and formally reporting their behaviour on the platform itself. Social media companies are obligated to keep their users safe. It can also help to show the bully that their behaviour is unacceptable.

For bullying to stop, it needs to be identified and reporting it is key.

Cyber Trolls(Joshitha)

(PPT Image)

Voice

Video :

If you’ve been on the internet for any period of time, you’ve likely run into a troll at some point. An internet troll is someone who makes intentionally inflammatory, rude, or upsetting statements online to elicit strong emotional responses in people or to steer the conversation off-topic. They can come in many forms. Most trolls do this for their own amusement, but other forms of trolling are done to push a specific agenda.

This type of online bullying constitutes of posting about or directly sending insults and profanity to their target. Flaming is similar to trolling, but will usually be a more direct attack on a victim to incite them into online fights.

Trolling is distinct from other forms of cyberbullying or harassment. It is normally not targeted towards any one person and relies on other people paying attention and becoming provoked.

PPT :

Trolling exists on many online platforms, from small private group chats to the biggest social media websites.

The places online where we can likely see trolls happening are listed below:

Anonymous online forums: Places like Reddit, 4chan, and other anonymous message boards are prime real-estate for online trolls. Because there’s no way of tracing who someone is, trolls can post very inflammatory content without repercussion. This is especially true if the forum has lax or inactive moderation.

Twitter: Twitter also has the option to be anonymous, and has become a hotbed for internet trolls. Frequent Twitter trolling methods involve hijacking popular hashtags and mentioning popular Twitter personalities to gain attention from their followers.

Comment sections: The comment sections of places such as YouTube and news websites are also popular areas for trolls to feed. You’ll find a lot of obvious trolling here, and they frequently generate a lot of responses from angry readers or viewers.

Video :

The most classic adage regarding trolling is, “Don’t feed the trolls.”
Trolls seek out emotional responses and find provocation amusing, so replying to them or attempting to debate them will only make them troll more.
By ignoring a troll completely, they will likely become frustrated and go somewhere else on the internet.

You should try your best not to take anything trolls say seriously. No matter how poorly they behave, remember these people spend countless unproductive hours trying to make people mad. They’re not worth your time of day.
If a troll becomes spammy or begins to clog up a thread, you can also opt to report them to the site’s moderation team.

Depending on the website, there’s a chance nothing happens, but you should do your part to actively dissuade them from trolling on that platform. If your report is successful, the troll may be temporarily suspended or their account might be banned entirely.

Spreading online rumours(Fauziyya)

(PPT Image)

Voice

Video :

Rumors are pieces of information or a story that has not been verified. What this means, is that the person telling the story does not know for certain if it is true or not. Most of the time, people who spread rumors do not bother to determine if there is any truth to what they are saying.

Typically, rumors are spread from person to person and can change slightly each time they are told. As a result, they can become exaggerated and altered over time.

People often think that they can make a fake profile with some different name and do anything online and will not be caught. Through such fake profiles, people sometimes indulge in posting false information on social media, or comments that could hurt others or spread rumours that may trigger panic or hurt religious sentiments of other people resulting into clashes and sometimes even riots. Spreading rumours online is a punishable offence.

PPT :

The rumor is propagated through the population by pair-wise contacts between spreaders and others in the population. Any spreader involved in a pair-wise meeting attempts to “infect” the other individual with the rumor. In the case this other individual is an ignorant, he or she becomes a spreader.

Video :

Social networks like Facebook and Twitter are reshaping the way people take collective actions. It has been argued that the ‘instantaneous nature’ of these networks influence the speed at which events are unfolding.

It is quite remarkable that social networks spread news so fast. Both the structure of social networks and the process that distributes the news are not designed with this purpose in mind. On the contrary, they are not designed at all, but have evolved in a random and decentralized manner.

PPT :

Governments, companies, and users are all waking up to how serious public opinion manipulation—as manifested in “fake news”—can be.

Governments are starting to recognize that false rumours are something that must be actively fought. Various government agencies are now setting up services to debunk stories that they consider to be false. Regulations have also been imposed and there has been punishing the sites that do publish misinformation.

So..what should you do if someone is spreading rumours about you? Turn to a trusted adult for support. Talk to someone you can confide in, like a parent, teacher, school counselor, or coach. Find your friends. Find a friend or two who will stick by you and who won't listen to rumors. Speak up.

Online Fraud(Fauziyya)

(PPT Image)

Voice

Video :

Online fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace. It is, however, differentiated from theft since, in this case, the victim voluntarily and knowingly provides the information, money, or property to the perpetrator.

Online fraud may occur in many forms such as :

- Non-delivered goods
- Non-existent companies
- Stealing information
- Fraudulent payments etc.

While the first two types of fraud can be countered by setting up official bodies ensuring the validity of e-commerce companies and promised delivery of goods, the last two types of frauds are more frightening. Examples of such frauds include credit card frauds and identity theft.

PPT :

Now, here are some common online frauds:

Charity fraud – Here, the scammer poses as a charitable organization soliciting donations to help the victims of a natural disaster, terrorist attack, regional conflict or epidemic. The scammer asks for donations, often linking to online news articles to strengthen their story of a funds drive. The scammer's victims are charitable people who believe they are helping a worthy cause and expect nothing in return. Once sent, the money is gone and the scammer often disappears.

Internet ticket fraud – Here, the scammer offers tickets to sought-after events such as concerts, shows, and sports events. The tickets are fake or are never delivered. The proliferation of online ticket agencies and the existence of experienced and dishonest ticket resellers has fueled this kind of fraud.

Purchase fraud – A fraudster uses the World Wide Web to advertise non-existent goods or services. Payment is sent remotely but the goods or services never arrive.

Credit card frauds - It is where the credit card details of the user are stolen from his/her online activities and then some payment frauds are carried out using this information, leading to a huge amount of money loss.

Identity theft - People tend to disclose a lot of personal information about themselves in their social networking profiles. This personally identifiable information could be used by fraudsters to steal users' identities, and posting this information on social media makes it a lot easier for fraudsters to take control of it.

Some measures to stop these frauds may include
- A monitoring official body that ensures the sanctity of E-commerce Company and the delivery of goods/services as promised
- Strong security mechanism by the E-commerce site and payment gateways to prevent stealing of crucial information.
- Official guidelines and safeguards on the selling of users' data to third parties.

Cyberstalking(Mahathi)

(PPT Image)

Voice

Video :

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation, or gathering information that may be used to threaten, embarrass or harass.

Cyberstalking doesn’t have to involve direct communication, and some victims may not even realize they are being stalked online. In some cases, the line between cyberspace and real life can become blurred. Attackers can collect your personal data, contact your friends and attempt to harass you offline.

Cyberstalking can take many different forms, but in the broadest sense, it is stalking or harassment that takes place via online channels such as social media, forums or email. It is typically planned and sustained over a period of time.

Video :

Typically, most cyberstalkers know their victims and instead of resorting to offline stalking, they use the internet to stalk. A cyber stalker relies upon the anonymity afforded by the internet to allow them to stalk their victim without being detected.

Other cases of cyberstalking, particularly those involving celebrities or other high-profile individuals, might involve complete strangers. Some perpetrators suffer from mental health issues and even believe their behavior is welcomed. Cyberstalking isn’t always conducted by individuals and might involve a group of people. They could be targeting an individual, group or organization for various reasons including opposing beliefs, revenge or financial gain.

PPT :

How to avoid cyberstalking?

As with many things in life, it’s better to be proactive than reactive when it comes to cyberstalking. Becoming a victim will be far less likely if you can do some simple steps..

Keep a low profile – You should always avoid posting personal details such as your address and phone number, and think carefully about revealing real-time information such as where you are and who you’re with.

Update your software – Regular software updates are crucial when it comes to preventing information leaks. Many updates are developed to patch security vulnerabilities and help ensure your information remains safe.

Hide your IP address – Many applications and services reveal your IP address to the person with whom you’re communicating. Cyberstalkers can begin with your IP address and use it to find your credit card data and physical address.

Maintain good digital hygiene – ‘Digital hygiene’ is a new term but represents a very important topic, especially with regard to social networks. Maintaining good digital hygiene helps protect you from cyber harassment, cyberbullying and cyberstalking.

Avoid disclosing sensitive information – Disclosing information increases the likelihood of someone getting their hand on your personal data.

PPT :

What to do in case you are being cyberstalked?

Block the person – If the tools are there, block anyone who you wish to stop hearing from, even if the messages are just annoying and not yet threatening. Only you can decide when this boundary has been passed.

Report to the platform involved – If someone is harassing or threatening you, you should block them immediately and report their behavior to the platform involved. Twitter, Facebook, LinkedIn,and many other platforms have created easy-to-use buttons to quickly report abusive behavior.

Call the police – If you believe their behavior is illegal or you fear for your safety, then you should contact the police and report the cyberstalker.

Obscene content(Mahathi)

(PPT Image)

Voice

PPT :

The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances, these communications may be illegal. The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of the internet that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world. It is defined as any visual or written representation that depict or advocate sexual activity of anyone under the age of 18.

According to the new Information Technology Bill, Section 67 has been amended that – not only creating and transmitting obscene material in electronic form, but also to browse such sites is an offence.

Piracy(Biancaa)

(PPT Image)

Voice

Video :

Piracy refers to the unauthorized duplication of copyrighted content that is then sold at substantially lower prices in the 'grey' market. The ease of access to technology has meant that over the years, piracy has become more prevalent.

PPT :

There Are Five Main Types of Software Piracy

Counterfeiting

This type of piracy is the illegal duplication, distribution and/or sale of copyrighted material with the intent of imitating the copyrighted product. In the case of packaged software, it is common to find counterfeit copies of the compact discs incorporating the software programs, as well as related packaging, manuals, license agreements, labels, registration cards and security features.

Internet Piracy

This occurs when software is downloaded from the Internet. Common Internet piracy techniques are: websites that make software available for free download or in exchange for others, internet auction sites that offer counterfeit or out-of-channel software, peer-to-peer networks that enable unauthorized transfer of copyrighted programs

Hard-Disk Loading

This occurs when a business sells new computers with illegal copies of software loaded onto the hard disks to make the purchase of the machines more attractive.

End User Piracy

This occurs when an individual reproduces copies of software without authorization. These include: Using one licensed copy to install a program on multiple computers, copying discs for installation or distribution, taking advantage of upgrade offers without having a legal copy of the version to be upgraded, acquiring academic or other restricted or non-retail software without a proper license, swapping discs in or outside the workplace.

Client-Server Overuse

This type of piracy occurs when too many users on a network are using a central copy of a program at the same time. If you have a local-area network and install programs on the server for several people to use, you have to be sure your license entitles you to do so. If you have more users than allowed by the license, that's "overuse."

Denial of Service attacks(Biancaa)

(PPT Image)

Voice

Video :

A “denial of service” or DoS attack is used to tie up a website’s resources so that users who need to access the site cannot do so. Many major companies have been the focus of DoS attacks. Because a DoS attack can be easily engineered from nearly any location, finding those responsible can be extremely difficult.

DoS attacks generally take one of two forms. They either flood web services or crash them.

PPT :

Flooding attacks - Flooding is the more common DoS attack. It occurs when the attacked system is overwhelmed by large amounts of traffic that the server is unable to handle. The system eventually stops. An ICMP flood — also known as a ping flood — is a type of DoS attack that sends spoofed packets of information that hits every computer in a targeted network, taking advantage of misconfigured network devices. A SYN flood is a variation that exploits a vulnerability in the TCP connection sequence. This is often referred to as the three-way handshake connection with the host and the server. Here’s how it works: The targeted server receives a request to begin the handshake. But, in a SYN flood, the handshake is never completed. That leaves the connected port as occupied and unavailable to process further requests. Meanwhile, the cybercriminal continues to send more and more requests, overwhelming all open ports and shutting down the server.

Crash attacks – Crash attacks occur less often, when cybercriminals transmit bugs that exploit flaws in the targeted system. The result? The system crashes.

Crash attacks and flooding attacks prevent legitimate users from accessing online services such as websites, gaming sites, email, and bank accounts.

Video :

DDoS - Distributed denial of service (DDoS) attacks:

These represent the next step in the evolution of DoS attacks as a way of disrupting the Internet. These attacks use large numbers of compromised computers, as well as other electronic devices — such as webcams and smart televisions that make up the ever-increasing Internet of Things — to force the shutdown of the targeted website, server or network. Security vulnerabilities in Internet-of-Things devices can make them accessible to cybercriminals seeking to anonymously and easily launch DDoS attacks. In contrast, a DoS attack generally uses a single computer and a single IP address to attack its target, making it easier to defend against.

PPT :
How to help prevent DoS attacks?

- **Get help recognizing attacks** – Companies often use technology or anti-DDoS services to help defend themselves. These can help you recognize between legitimate spikes in network traffic and a DDoS attack.
- **Contact your Internet Service provider** – If you find your website is under attack, you should notify your Internet Service Provider as soon as possible to determine if your traffic can be rerouted. Also, consider services that can disperse the massive DDoS traffic among a network of servers.
- **Investigate black hole routing –** "Black hole routing" directs excessive traffic into a null route, sometimes referred to as a black hole. This can help prevent the targeted website or network from crashing. The drawback is that both legitimate and illegitimate traffic is rerouted in the same way.
- **Configure firewalls and routers –** Firewalls and routers should be configured to reject bogus traffic. Remember to keep your routers and firewalls updated with the latest security patches.
- **Consider front-end hardware –** Application front-end hardware that’s integrated into the network before traffic reaches a server can help analyze and screen data packets. The hardware classifies the data as priority, regular, or dangerous as they enter a system. It can also help block threatening data.

Reporting cyber crime(Biancaa)

(PPT Image)

Voice

Video :

Cybercrime can be particularly difficult to investigate and prosecute because it often crosses legal jurisdictions and even international boundaries. Additionally, an offender may disband one online criminal operation – only to start up a new activity with a new approach – before an incident even comes to the attention of the authorities.

The good news is that federal, state and local law enforcement authorities are becoming more sophisticated about cybercrime and are devoting more resources to responding to these threats. Furthermore, over the past several years, many new anti-cybercrime statutes have been passed that empower federal, state and local authorities to investigate and prosecute these crimes. However, law enforcement needs your help to stop the nefarious behavior of cybercriminals and bring them to justice.

Reporting cybercrime is easy. Here's how.

PPT :

To report a cybercrime:

- The local police stations can be approached for filing complaints just as the cybercrime cells specially designated with the jurisdiction to register a complaint.
- Provisions have now been made for filing of "E-FIR" in most of the states
- In addition, the Ministry of Home affairs has recently launched a website for registering cybercrimes against women and children online including cybercrimes.

- The Cybercrime portal

The government has created the National Cyber Crime Reporting Portal for the convenience of those who want to report cyber crimes online. The portal has been created with special focus on cyber crimes committed against women and children. The complaints registered on the portal are dealt by the law enforcement agencies swiftly based on the information provided on the portal. The portal has a section for cyber crimes committed against women and children like child pornography, sexual abuse among others. The other section deals with cyber crimes like financial fraud or hacking among others.

Information theft (Swathy)

(PPT Image)

Voice

Video :

Information theft or Data theft is the act of stealing information stored on computers, servers, or other devices from an unknowing victim with the intent to compromise privacy or obtain confidential information.

Data theft is a growing problem for individual computer users as well as large corporations and organizations.

Data theft occurs both outside and inside companies, and reducing the risk of insider data theft at the corporate level is anything but easy.
This is especially true because system administrators and employees have access to technology such as database servers, desktop computers, and external devices including USBs, smart phones, and other removable and mobile devices.

PPT :

Common ways in which cyber criminals get hold of your data

Data Breaches – A data breach happens when someone gains access to an organization's data without authorization. The most common types of information stolen in data breaches include full names, Social Security numbers and credit card numbers.

Unsecure Browsing – For the most part, you can browse the internet safely, especially if you stick to well-known websites. But if you share any information on an unsecure website or a website that's been compromised by hackers, you could be putting your sensitive information directly in the hands of a thief. Depending on your browser, you may get an alert if you try to access a risky website.

Mail Theft – Since long before the internet, identity thieves have been combing through the mail to find documents that held personal information. Bank and credit card statements and any other document you send or receive through the postal system can be intercepted and used to gain access to your data.

PPT :

Wi-Fi Hacking - If you use our computer or phone on a public network—airport, department store or coffee shop Wi-Fi—hackers may be able to "eavesdrop" on your connection. This means that if you type in a password, bank account or credit card number, Social Security number or anything else, an eavesdropper can easily intercept it and use it for their own purposes

How can you prevent information theft?

- Properly dispose of sensitive data
- Use password protection wherever possible
- Encrypt data
- Protect against viruses and malware
- Keep your software and operating systems upto date
- Secure access to your network
- Verify security controls of third parties
- Be alert to phishing and spoofing

Scams (Swathy)

(PPT Image)

Voice

Video :

The term “scamming” is closely related to the criminological terminology of the advance fraud, but particularly includes many forms of online fraud.

Deceivers use false pretenses to try to persuade their victims into making a payment in "advance". At the same time, they promise profits, inheritances, or slightly higher repayments.

Once criminals receive payment, contact is usually terminated immediately. A fulfillment of the aforementioned promise doesn’t follow, and the paid money is usually irretrievably lost. Making contact online generally happens via e-mail, but now contact can also be made through chat portals, messengers and social networks. Scammers have even spread to online marketplaces for real estate, jobs, or used cars.

PPT :

Now we will see some of the common types of scams

Job scams – Internet criminals use the distress of jobseekers to their advantage They entice them with a dream job, top pay, and minimal work hours. Usually, the victim is supposed to transfer money for work materials, uniforms, or shoes in advance. Once the money is delivered to the scammers, contact is broken off. There is never a contract of employment and the supposedly purchased goods aren’t delivered.

Greetting card scams – Whether it’s Christmas or Easter, we all get all kinds of holiday greeting cards in our email inbox that seem to be coming from a friend or someone we care. If you open such an email and click on the card, you usually end up with malicious software that is being downloaded and installed on your operating system. The malware may be an annoying program that will launch pop-ups with ads, unexpected windows all over the screen.

Email scams

Phishing emails that try to trick you into revealing your bank details – they may direct you to copycat websites that look like your bank’s website

Stranded traveller emails – supposedly from a friend (whose email account has probably been hacked) who says they’ve been robbed abroad and asks you to send them money

Advance fee – the sender has something valuable and offers a reward for your help moving it from one country to another, but you have to make a payment or provide bank details

Inheritance – someone has left you money in a will and you have to send an administration fee to get the money

Lottery scams:

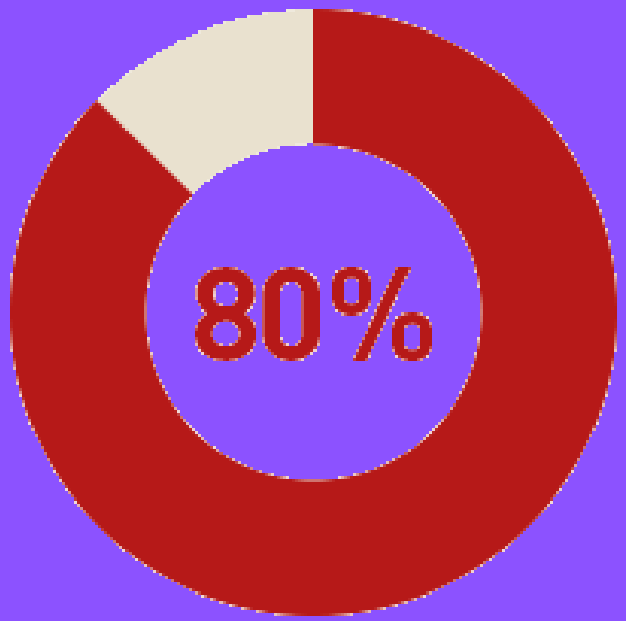
A lottery scam comes as an email message informing you that you won a huge amount of money and, in order to claim your prize or winnings, you need to pay some small fees. It doesn’t even matter that you don’t recall ever purchasing lottery tickets. Our imagination falls prey easily to amazing scenarios someone can only dream of. But the dream ends as soon as you realize you have been just another scam victim.

How do you avoid online scams?

- Never enter personal information or any financial information on unsecure websites,i.e., the sites that do not employ HTTPS and do not have a padlock sign.
- Never reply to emails from any unknown or unreliable source.
- Never click on any links that you have received in your email, even if you know the sender. Rather, open a browser window and type the url yourself than clicking on the link in the email.
- Never respond to an e-mail or advertisement claiming you have won something.

Some facts to know on cyber crime

1. There is a hacker attack every 39 seconds
2. In 2020, 80% of firms have seen an increase in cyberattacks
3. 700 million people in 21 countries experienced some form of cybercrime
4. Healthcare Organizations Are The Number One Cyber Attacked Industry
5. The number of cyber attacks is going UP not down
6. In April 2020, Google blocked 18 million daily malware and phishing emails related to Coronavirus.
7. 95% of cybersecurity breaches are caused by human error
8. An estimated 300 billion passwords are used by humans and machines worldwide
9. By 2023, the total number of DDoS attacks worldwide will be 15.4 million.
10. 1 in 36 mobile devices have high- risk apps installed.



Google