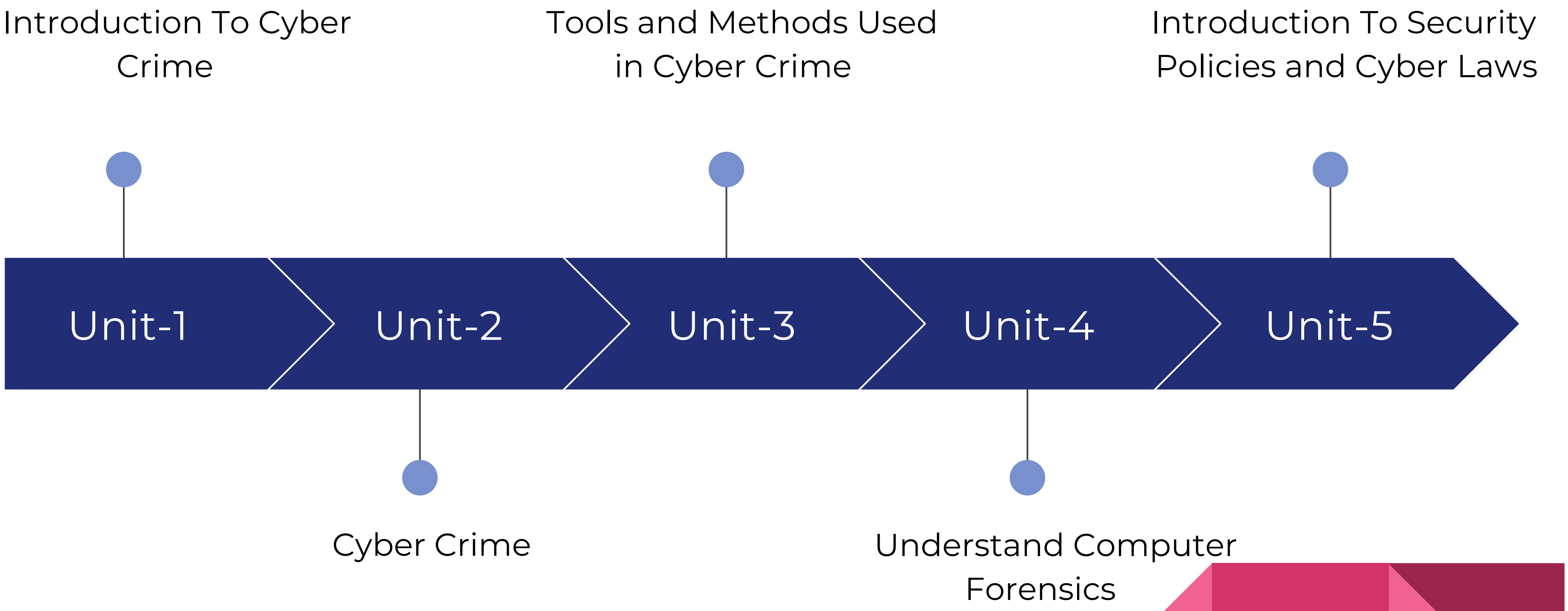


Unit-1

Introduction To Cyber Crime

Unit-2

Cyber Crime

Unit-3

Tools and Methods Used in Cyber Crime

Unit-4

Understand Computer Forensics

Unit-5

Introduction To Security Policies and Cyber Laws

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 1

Cyber Security

(BCC301 / BCC401/ BCC301H / BCC401H)

Video Overview:

- B.Tech Students - Dr. APJ Abdul Kalam Technical University(AKTU).
- This pdf provides help in the exam time for a quick revision in sorting the time.
- Notes & PPT link available in the description.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT-1: Introduction to Cyber Crime

- Cybercrime Definition and Origins of the Word Cybercrime
- Information Security
- Who Are Cybercriminals?
- Classifications of Cyber Crimes
- A Global Perspective on Cybercrimes
- Cybercrime Era: Survival Mantra for the Netizen
- How Criminals Plan the Attacks
- Social Engineering
- Cyber Stalking
- Cybercafe and Cybercrimes
- Botnets: The Fuel for Cybercrime
- Attack Vector

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 1

Introduction to Cyber Crime

Definition: Cybercrime means doing bad things using computers and the internet. It's like breaking the rules in the digital world. Imagine someone stealing information or causing trouble online—that's cybercrime.

Origins of the Term: The word “cybercrime" comes from combining "cyber" (related to computers) and "crime" (doing bad things). Back in the 1990s, when computers were becoming popular globally, people needed a word for these new digital crimes. So, they created "cybercrime" to describe illegal activities happening in the digital space.

UNIT 1

Information Security

Information Security is like a digital superhero—it protects your personal information from digital bad guys. It's the guardian that ensures only the right people can access and use your digital secrets.

Importance: Imagine it as the lock on your digital diary. Information Security keeps your personal details safe from online mischief-makers. Without it, your digital secrets could be like an open book for anyone to read.

Key Aspects:

1. **Confidentiality:** Keeping your secrets safe.
2. **Integrity:** Making sure your information is accurate and not tampered with.
3. **Availability:** Ensuring you can access your information when you need it.

UNIT 1

Who are CyberCriminals?

Cybercriminals are like digital bad guys. They're people who use computers and the internet to do naughty stuff.

1. **Anyone Can Be a Cybercriminal:** It could be your neighbour, someone across the world, or even someone you know. There's no specific "look" for a cybercriminal.
2. **Digital Rule-Breakers:** They break the online rules by doing things like stealing information, spreading viruses, or causing trouble in the digital world.

Classification of Cybercrimes

Cyber crimes can be classified in to 4 major categories as the following:

- Cyber crime Against Individual
- Cyber crime Against Property
- Cyber crime Against Organization
- Cyber crime Against Society

UNIT 1

1. Cyber crimes Against Individual

Email spoofing: A spoofed email is one in which the email header is forged so that the mail appears to originate from one source but actually has been sent from another source.

Spamming: Spamming means sending multiple copies of unsolicited mails or mass emails such as chain letters.

Harassment & Cyber stalking: Cyber Stalking Means following an individual's activity over internet.
It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

UNIT 1

2. Cyber crimes Against Property

Credit Card Fraud: As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.

Intellectual Property Crimes:

- **These include Software piracy:** Illegal copying of programs, distribution of copies of software.
- **Copyright infringement:** Using copyrighted material without proper permission.
- **Trademarks violations:** Using trademarks and associated rights without permission of the actual holder.
- **Theft of computer source code:** Stealing, destroying or misusing the source code of a computer.

Internet Time Theft: This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

UNIT 1

3. Cyber crimes Against Organisations

Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner.

Denial Of Service: When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

Virus attack: A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

Email Bombing: Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

Trojan Horse: This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

UNIT 1

4. Cyber crimes Against Society

Forgery: Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.

Web Jacking: Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

UNIT 1

A Global Perspective on Cybercrimes

A Global Perspective on Cybercrimes is like looking at naughty actions happening all around the world using computers and the internet.

More Details:

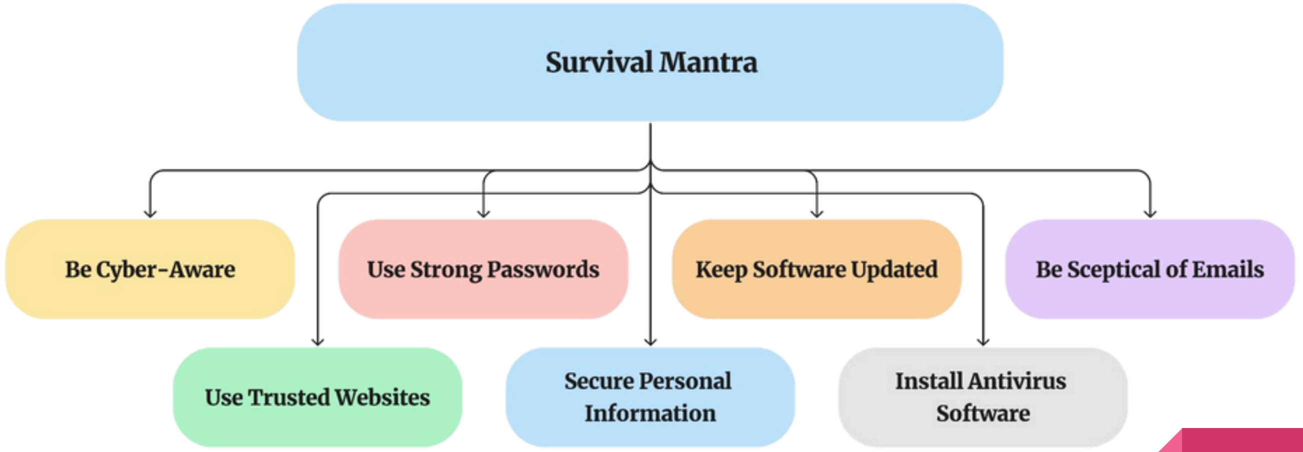
1. **No Borders:** Cybercrimes don't follow country lines. They can happen anywhere, and bad actors from different countries might even work together.
2. **Digital Challenges Everywhere:** It's not just a problem in one place. People worldwide face similar digital troubles, and everyone needs to be careful online.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 1

CyberCrime Era

The Cybercrime Era is like living in a time where digital mischief is a common challenge. Survival Mantra for the Netizens means having a set of rules or practices to stay safe in this digital age.



Survival Mantra

Be Cyber-Aware

Use Strong Passwords

Keep Software Updated

Be Sceptical of Emails

Use Trusted Websites

Secure Personal Information

Install Antivirus Software

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

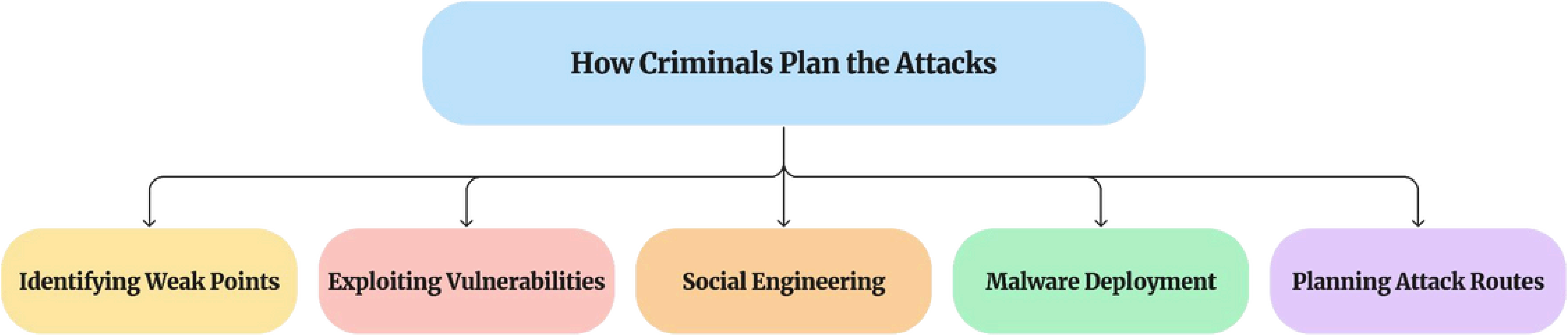
Survival Mantra for Netizens

1. **Be Cyber-Aware:** Stay alert and aware of potential online threats.
2. **Use Strong Passwords:** Create and regularly update strong, unique passwords.
3. **Keep Software Updated:** Ensure your computer and apps have the latest security updates.
4. **Be Sceptical of Emails:** Don't trust every email; be cautious, especially with links or attachments.
5. **Use Trusted Websites:** Stick to reputable websites to minimise risks.
6. **Secure Personal Information:** Be cautious about sharing sensitive info online.
7. **Install Antivirus Software:** Have reliable antivirus software to protect against digital threats.

UNIT 1

How Criminals Plan the Attacks

Cyber Offences are like digital crimes, and understanding how criminals plan their attacks is crucial. It involves the strategies and methods they use to carry out illegal activities in the digital space.



UNIT 1

Planning Strategies

1. **Identifying Weak Points:** Criminals look for vulnerabilities in computer systems or networks.
2. **Exploiting Vulnerabilities:** They use weaknesses to gain unauthorised access or control.
3. **Social Engineering:** Tricking individuals into divulging sensitive information.

4 **Malware Deployment:** Spreading malicious software to compromise systems.

. **Planning Attack Routes:** Deciding the best way to execute their digital mischief.

5.

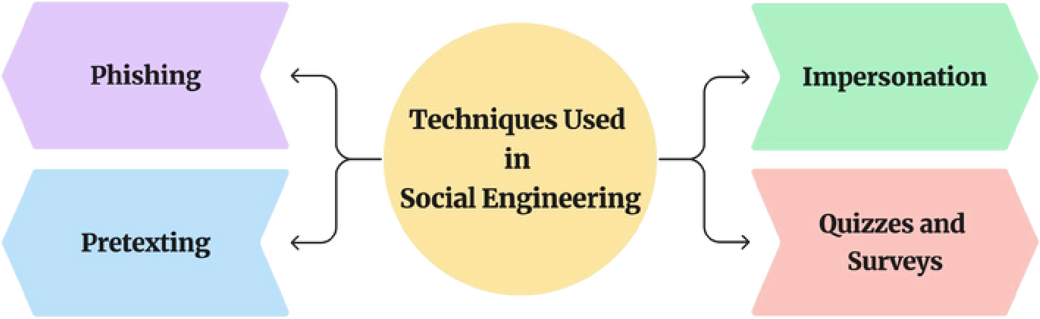
Example: Think of Cyber Offences like planning a heist. Criminals study the target (identifying weak points), find ways to break in (exploiting vulnerabilities), use deception (social engineering), deploy tools for the job (malware), and plan their entry and exit routes (planning attack routes). Understanding these steps helps in building stronger digital defences.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 1

Social Engineering

Social Engineering is like a digital magic trick. It's when cybercriminals use charm, manipulation, or deceit to trick people into giving up their personal information or doing something they shouldn't.



Techniques Used in Social Engineering

- Phishing
- Pretexting
- Impersonation
- Quizzes and Surveys

UNIT 1

Techniques Used in Social Engineering

1. **Phishing:** Sending fake emails or messages to trick individuals into revealing sensitive information.
2. **Pretexting:** Creating a made-up scenario to obtain personal information.
3. **Impersonation:** Posing as someone trustworthy to gain access to information or systems.
4. **Quizzes and Surveys:** Using seemingly harmless quizzes or surveys to gather information.

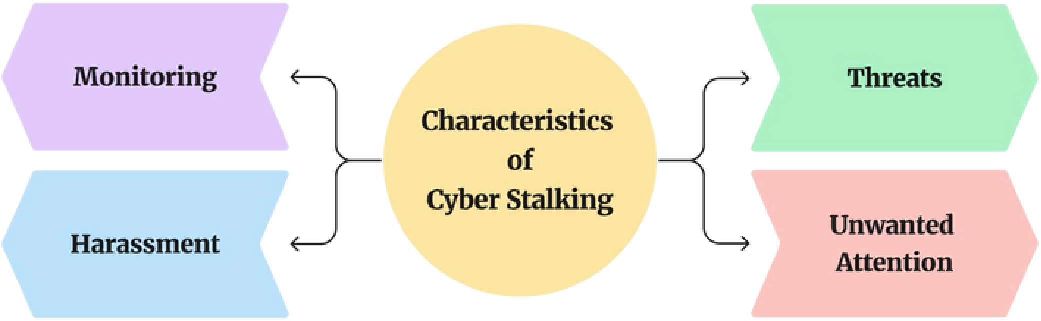
.

Example: Imagine someone pretending to be a friend and asking for your password. That's Social Engineering in action. It's like a digital con artist using charm or deception to get people to share their secrets. Always be cautious, and never share sensitive information online, even if it seems harmless

UNIT 1

Cyber Stalking

Cyber Stalking is like someone following you online. It involves persistent and unwanted attention, harassment, or monitoring through digital means.



Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

Characteristics of Cyber Stalking

1. **Unwanted Attention:** Receiving excessive, unsolicited online communication.
2. **Monitoring:** Being observed without consent, often through social media or other online platforms.
3. **Harassment:** Repeated and intrusive behaviour causing emotional distress.

4 **Threats:** Expressing harmful intentions or making individuals feel unsafe.

.

Example: Imagine someone constantly commenting on your social media, sending numerous messages, or tracking your online activity. That's Cyber Stalking. It's like an online shadow that won't go away, causing discomfort and potentially putting your digital well-being at risk. Always report such behaviour and take steps to protect your online privacy.

UNIT 1

C ybercafe

A Cybercafe is like a digital hangout spot where people can use computers and the internet. It's a place where individuals, often without personal computers, can access online services, play games, or work on projects.

Features:

1. **Computer Access:** Provides computers with internet connectivity for public use.
2. **Internet Browsing:** Users can surf the web, check emails, and engage in online activities.
3. **Gaming:** Some cyber cafes offer gaming setups for multiplayer or individual gaming sessions.

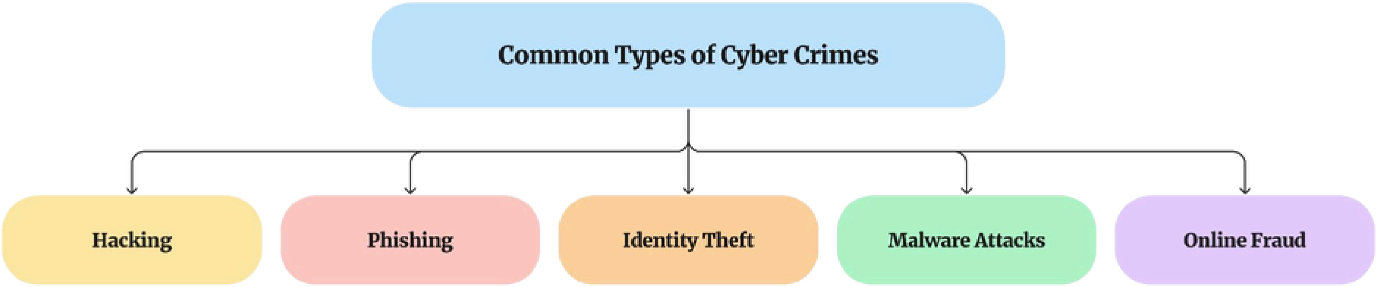
Common Uses:

1. **Study and Work:** Students or professionals without personal computers may use cyber cafes for assignments or work.
2. **Socialising:** People may gather to play games, socialise, or collaborate on projects.

UNIT 1

C ybercrime

Cybercrimes are like digital offences, where people use computers and the internet to break the law or cause harm. These actions can range from stealing personal information to disrupting digital systems.



Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 1

Common Types of Cybercrime

1. **Hacking:** Unauthorised access to computer systems or networks.
2. **Phishing:** Tricking individuals into revealing sensitive information through fake emails or messages.
3. **Identity Theft:** Pretending to be someone else online to steal personal information.
4. **Malware Attacks:** Spreading harmful software to compromise computer systems.
5. **Online Fraud:** Deceiving individuals to gain money or sensitive information.

Impact:

1. **Financial Loss:** Individuals or businesses may lose money.
2. **Privacy Invasion:** Personal information may be exposed.
3. **Disruption**: Digital systems may be interrupted or damaged.

P revention:

1. **Use Strong Passwords:** Create complex and unique passwords.
2. **Install Antivirus Software:** Protect devices from malicious software.
3. **Be Cautious Online:** Avoid clicking on suspicious links or sharing sensitive information.

Faculty: VIKRAM SHARMA
Vikram1532018@gmail.com

UNIT 1

Botnets

Botnets are like digital zombie armies. They're networks of infected computers controlled by a single entity, often a cybercriminal. These infected computers, known as "bots," work together without their owners' knowledge to perform malicious activities.

How Botnets Work:

1. **Infection:** Cybercriminals infect computers with malicious software.
2. **Control:** Once infected, these computers become part of the botnet, and the attacker can control them remotely.
3. **Coordination:** Bots work together to perform tasks, like spreading malware, stealing information, or launching cyber attacks.

Botnets: Fuel for Cybercrime

1. **Distributed Power:** Botnets provide attackers with a distributed and powerful network, making it harder to trace and stop their activities.
2. **Multipurpose Use:** They can be used for various cybercrimes, from launching massive DDoS attacks to sending spam emails.

UNIT 1

Attack Vector

An Attack Vector is like finding a secret entry point. It's the method or path that cybercriminals use to gain unauthorised access to computer systems or networks.

Types of Attack Vectors:

1. **Malware:** Infecting systems with malicious software.
2. **Phishing:** Tricking individuals into revealing sensitive information.
3. **Drive-By Downloads:** Installing malware when a user visits a compromised website.

4 **Zero-Day Exploits:** Taking advantage of undiscovered vulnerabilities in software.

.