Unit -4

Women & Cyber Security

What is Cyber Crime?

Cybercrime is any criminal activity that involves a computer, networked device or a network.

Phishing,

credit card frauds,

bank robbery,

illegal downloading,

child pornography,

kidnapping children via chat rooms,

scams,

cyber terrorism,

creation and/or distribution of viruses,

Spam and so on.

Phishing

Phishing is a method of trying to gather personal information using deceptive e-mails and websites.

IT Act 2008

- *Provisions Applicable:- Section 66, 66A and 66D of IT Act and Section 420 of IPC*

Prevention

- Always check the spelling of the URLs in email links before you click or enter sensitive information
- Watch out for URL redirects, where you're sent to a different website with identical design
- If you receive an email from a source you know but it seems suspicious, contact that source with a new email, rather than just hitting reply
- Don't post personal data, like your birthday, vacation plans, or your address or phone number, publicly on social media

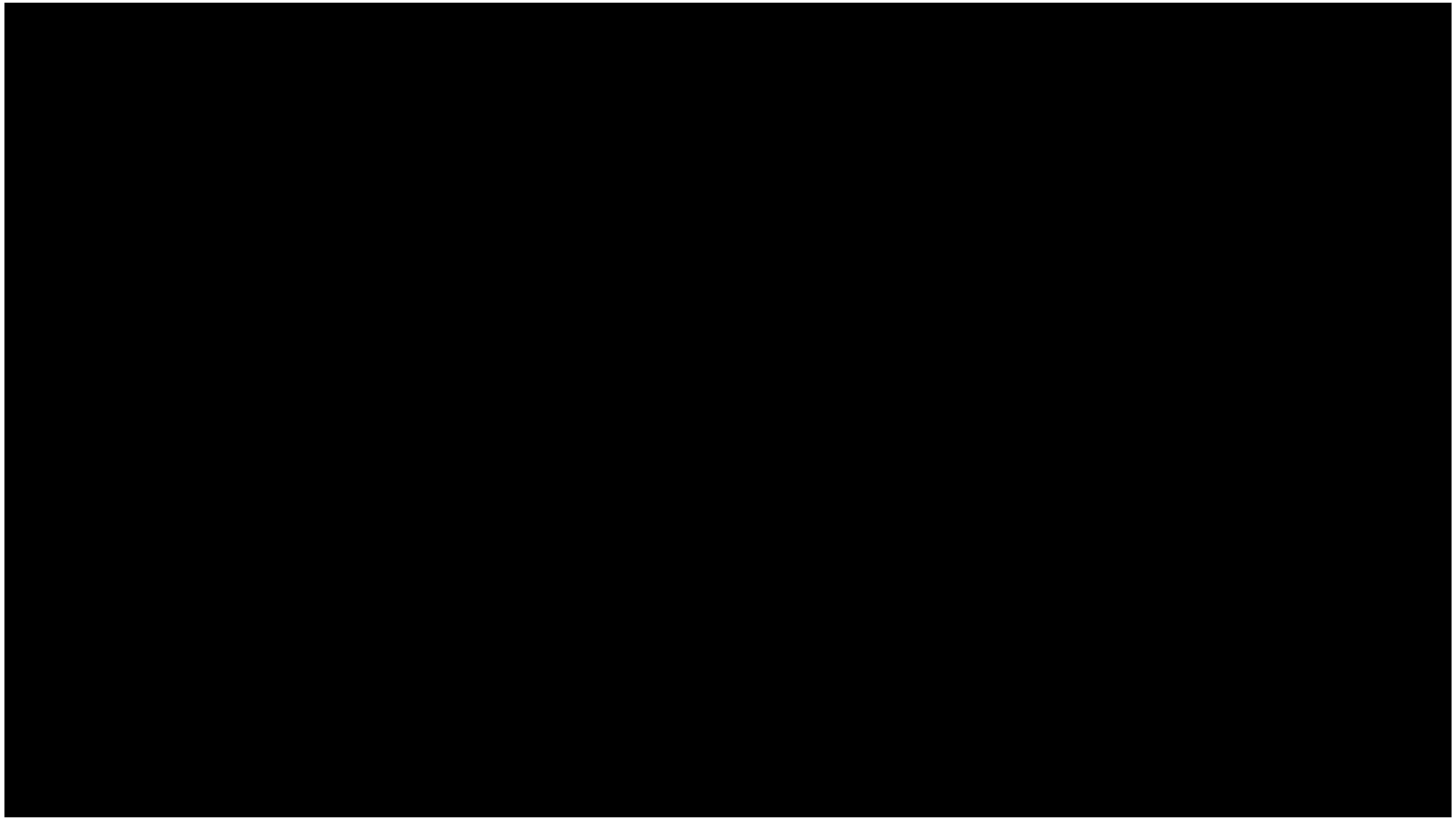
Credit/Dabit card frauds

Credit card fraud is the unauthorized use of another person’s credit card—or card information—to make purchases or access funds through cash advances using the victim’s account.

How : Radio frequency identification (RFID) technology

Lets buy some

Radio frequency identification (RFID) technology



IT Act 2008

Sections 43, 66, 66C, 66D of IT Act and section 420 of the IPC.

Prevention

- Carefully review every credit card statement.
- Protect your account information. Don’t leave account information out in the open where others might see it.
- Destroy old statements. When you finish with the monthly statement, shred it before discarding it.

Online shopper? Stay safe

- Be sure that any page that asks you to enter credit card or other personal information has “https” in the address bar (the “s” means secure). Remember, “https” not just “http”.
- Avoid “phishing” scams.

Social Engineering

Social engineering is an attack that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain.

How ??

- Research and observation on the target.
- Focus on the behaviors and patterns.
- Scan the person's social media profiles for information and study their behavior online and in person.

The hacker can design an attack based on the information collected and exploit the weakness uncovered during the reconnaissance phase.

Types of social engineering attacks

- **Baiting:** Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive, in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.

Malware : software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Types of social engineering attacks

- **Fishing**: (We have already seen)

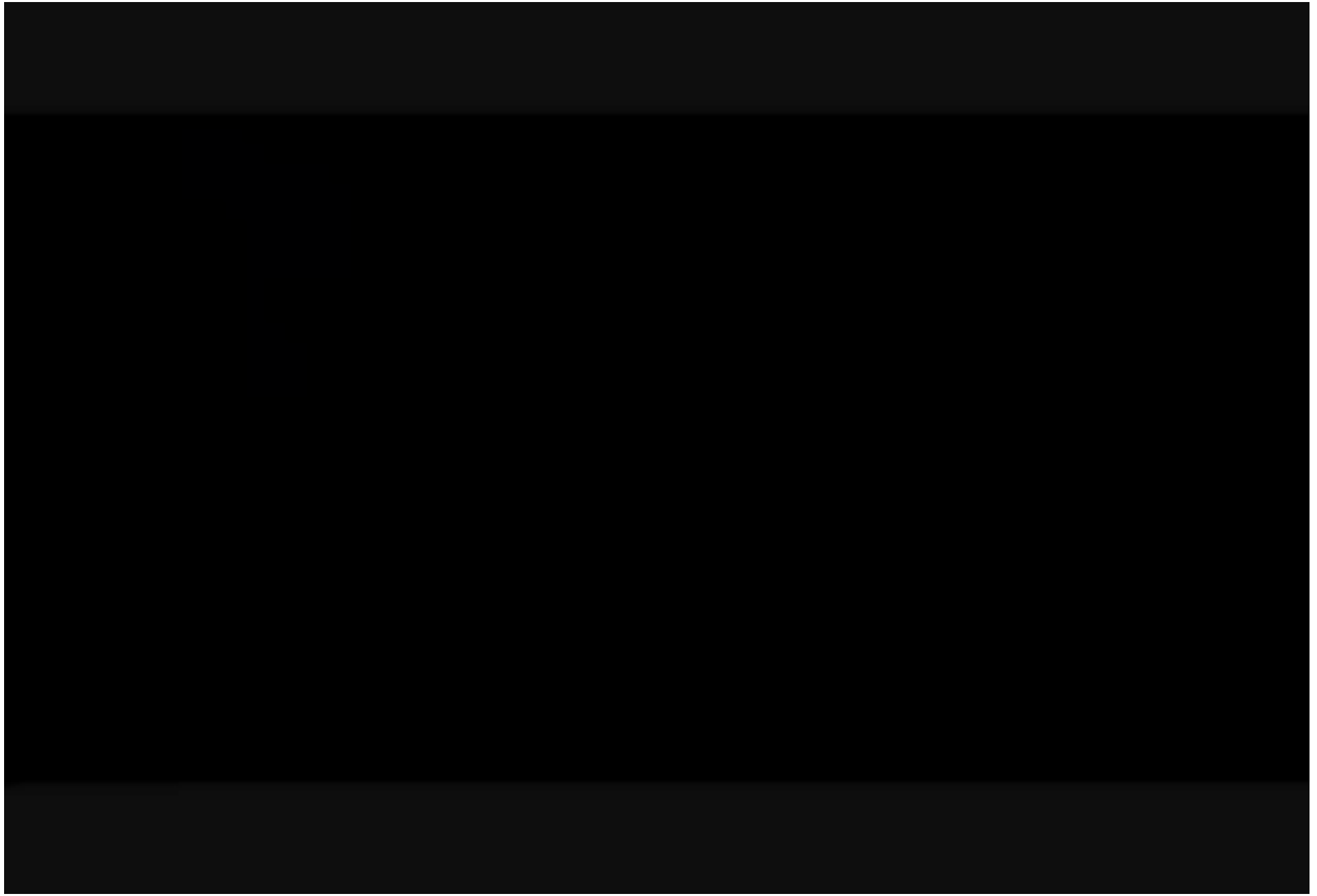
- **Vishing:** Vishing is also known as voice phishing, and it's the use of social engineering over the phone to gather personal and financial information from the target.
- **Scareware:** Scareware involves tricking the victim into thinking his computer is infected with malware or has accidentally downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.

Types of social engineering attacks

- **Honey trap:** An attack in which the social engineer pretends to be an attractive person to interact with a person online, fake an online relationship and gather sensitive information through that relationship.

Types of social engineering attacks

Example : Frank Abagnale is considered one of the foremost experts in social engineering techniques. In the 1960s, he used various tactics to impersonate at least eight people, including an airline pilot, a doctor and a lawyer. Abagnale was also a check forger during this time.



IT Act 2008

- Sections 43, 66, 66C, 66D of IT Act and section 420 of the IPC.

Prevention

- Change password
- Smart move
- Beware of fake

kidnapping children via chat rooms

- How ?
  - Profile pic
  - School information
  - Phone number
  - Behave like a cool
  - Same liking interest

Prevention

- Educate your kids
- Know what’s out there
- Enable safety features on all devices like Geotagging, Checking in
- Enhance privacy settings
- Don’t let kids flag up their age
- Know your child’s passwords
- Monitor online activity
- Communicate

IT Act 2008

- IPC 363
- 7 years jail and fine

Cyber terrorism

Hackers who break into computer systems can introduce viruses to vulnerable networks, deface websites, launch denial-of-service attacks and/or make terroristic threats electronically.

Example

- Viruses, computer worms and malware targeting control systems can affect water supplies, transportation systems, power grids, critical infrastructure and military systems and may be used to further cyberterrorist goals.
- DoS attacks, cybersecurity events that occur when attackers take action to prevent legitimate users from accessing targeted computer systems, devices or other network resources.
- Hacking and theft of critical data from institutions, governments and businesses.
- Ransomware that holds computer systems hostage until the victims pay ransom.

Prevention

- By installing reputable cybersecurity measures such as antivirus and antimalware software and updating them regularly. This offers a base defense system against cyberterrorists.

Fortunately, phishing victimization is preventable. The following security precautions are recommended:

- Use updated computer security tools, such as anti-virus software, spyware and firewall.
- Never open unknown or suspicious email attachments.
- Never give personal information requested by email, such as your name or credit card number.
- Double check the website URL
- Verify the website's phone number before placing any calls to the phone number provided via email.