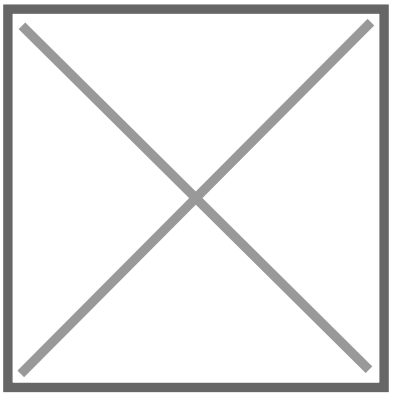

Social Engineering

Description

Theme:

- Social engineering scams are evolving, and one of the latest threats is the digital arrest scam. In this scam, fraudsters pose as law enforcement, using fear and intimidation to manipulate victims into giving up money or personal information. Itâ??s a stark example of how trust can be exploited online in increasingly convincing ways.

What is Social Engineering?

- Social engineering is when someone uses tricks, lies and fear to fool people into giving away private information.
- The goal is usually to steal passwords, money, or important personal data by making the victim trust the attacker.

Common Types of Social Engineering:

- **Phishing:**
  - This happens when someone sends fake emails or messages that look real and trustworthy.
  - These messages often ask you to click a link or log in to a fake website, where your details can be stolen.
- **Vishing:**
  - Vishing is voice phishing, where scammers call pretending to be from a bank or a trusted company.
  - They try to make you panic or believe a story so youâ??ll share your OTP, card number, or other personal information.
- **Smishing:**
  - This is like phishing, but it happens through SMS or messaging apps.

  - You may get a message that says you won a prize or that there is a problem with your account, and you are asked to click a link.
- **Pretexting:**
  - In pretexting, the scammer pretends to be someone else, like an IT worker or a police officer.
  - The digital arrest scam can be considered a type of pretexting.
  - They create a fake reason or story to make you trust them and give away your private information.
  - They may say that your bank account is involved in a crime like money laundering or drug trafficking.
  - They often show fake ID cards, fake legal documents, or even create a fake video meeting with â??officialsâ?• to make you believe them.
  - They try to scare you into sending money or staying on the call while they guide you to transfer funds.
  - Many innocent people have lost huge amounts of money through this kind of emotional blackmail.
- **Baiting:**
  - Baiting involves offering something tempting, like free software or a USB drive, that actually contains harmful programs.
  - When you click the download or plug in the device, it can infect your computer or steal your data.
- **Tailgating:**
  - Tailgating happens in real life when someone follows you into a secure place without permission.
  - They may pretend to be a delivery person or say they forgot their ID to get into restricted areas.

How to Stay Safe:

- Never share personal information, passwords, or OTPs with anyone, even if they say they are from a bank or government.
- Donâ??t believe calls or messages that use fear to make you act quickly.
- Always double-check with the real organization before taking action.
- Use strong passwords and enable two-factor authentication for your accounts.
- Stay updated about common scams.

What to do if you fall victim to a social engineering scam:

- Block the scammer, report the incident to the cybercrime helpline(1930), freeze accounts, and change passwords.

Conclusion:

Social engineering is one of the most dangerous ways cybercriminals attack people, not by using complex software, but by using human emotions like fear, trust, and urgency. Scams like the digital arrest fraud can be very convincing and terrifying, but staying calm, alert, and informed

is the best way to protect yourself. Always take a moment to think, verify facts, and never share personal information under pressure.

Your Turnâ?¦

What are your thoughts on Social Engineering scams? Express your thoughts through the comments section. Subscribe to our blog to read answers to the trending GD topics.