Hello everyone, I am Manh.today I’m talk about topic of social engineering. (en ri nia ring)

First of all, "Social Engineering" is a type of attack that combines the two words "Social" and "Engineering," reflecting the nature of this type of attack: the tricks, techniques, and tactics used to attack the social nature of human beings, which does not exist in machines.

Social Engineering Attacks are also known as Non-Technical Attacks.

When being attacked by Social Engineering techniques, users may face various security risks. Here are some common risks:

* Personal information loss: Attackers can deceive(đi xíp) users into providing sensitive information such as usernames, passwords, credit card numbers, or social security numbers.
* Account theft: If attackers obtain users' login information, they can access their accounts and steal their information or money.
* Network attacks: Attackers can deceive users into downloading malware or accessing fake websites to obtain information or take control of the system.
* Money loss: Attackers can deceive users into transferring money to them through email or messages using impersonation or fraud(phờ rót).
* Reputation damage: When users are deceived, their personal information may be disclosed, leading to reputation damage.

There are many other attacks that involve social engineering,for example: scareware, email hacking, Assess tailgating(theo gay đinh), phishing, baiting, dns spoofing, physical breaches, pretexting

As we have seen, there are many types of social engineering attacks, but the most prominent among them is phishing

Phishing is a type of cyber attack where attackers send fake emails, text messages, or websites that appear to be from a legitimate(ni tit ti mịt) source, such as a bank, social media platform, or online retailer(re theo lơ). The aim of phishing is to trick the recipient(re síp phi ừn) into revealing their personal or sensitive information, such as login credentials(que den sồ), credit card numbers, or social security numbers, by pretending to be a trustworthy(trớt qua ti) entity. Phishing attacks often use urgent(ơ rừn) or persuasive (pơ sấy síp) language to make the recipient(re xíp pi ừn) act quickly without thinking, and can lead to identity theft, financial(phai nen sồ) losses, and other security risks.

Thank you for listening. Next, I would like to invite cương to present about pharming and Timing Attack

sendemail -xu AT170418@actvn.edu.vn -xp vFCNTwj9R1tk8a75 -s smtp-relay.sendinblue.com:587 -f " mshuongnt@gmail.com " -t " manh0972832@gmail.com " -u "lam bai tap" -m "link bai tap : https://got-der-specialist-programmer.trycloudflare.com"