Social Engineering ….

- Dr. Deepamala N

- Disclaimer: All images are from internet

Social Engineering

- Technique to influence and persuasion to deceive people to obtain the information or perform some action.
- A social engineer usually uses telecommunications or internet to get them to do something that is against the security practices and/ or policies of the organization.
- SE involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- It is an art of exploiting the trust of people.

What is Social Engineering? - YouTube

1- Can you print my resume, please?

- A man visited a company for an interview. He said to the front-desk person:

"**I have just ruined my resume by spilling coffee on it**" and started to convince the front-desk person to print his resume from the USB he has.

Once the victim plugs the USB into a company device now he can spread malware into the company or get remote access to company devices.

2- Click the link to register and win the big prize!

- As we have mentioned before, the attacker will search for his target and will know about his interests. If the target for example is a fan of a certain team the attacker can take advantage of that by sending a phishing mail to the victim telling him to register in the link and get the chance to attend the game in person.

- And of course, at this moment the target may click the link un-consciously because he didn't expect that, he was so happy, **His emotional side blinds his rational side**.

- The page he would visit is a registration page indeed but will contain other hidden frames to gain the targeted information.

Social Engineering

- Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.
- A social engineer runs what used to be called a "con game."
- or example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security.
- Social engineers often rely on the natural helpfulness of people as well as on their weaknesses.
- They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.

Classification of Social Engineering

1. **Human-Based Social Engineering**

   needs interaction with humans; it means person-to-person contact and then retrieving the desired information. People use human based social engineering techniques in different ways; the top popular methods are:

   - Impersonating an employee or valid user
   - Posing as an important user
   - Using a third person
   - Calling technical support
   - Shoulder surfing
   - Dumpster diving

2. **Computer –Based Social Engineering**

   Computer-based social engineering uses computer software that attempts to retrieve the desired information.

   - Fake E-mails
   - E-mail attachments
   - Pop-up windows

1.1. Impersonation

- In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system. A hacker can gain physical access by pretending to be a janitor, employee, or contractor.
- To attackers, sets of valid credentials are a coveted asset. An attacker who has obtained valid user credentials through social engineering techniques has the ability to roam the network with impunity searching for valuable data. In log data, the attacker's activities are easily hidden due to the inability to see the subtle differences in behaviors and access characteristics. Yet, this phase of the classic attack chain often represents the lengthiest portion of the attack.

- This is how hackers hack you using simple social engineering – YouTube
- https://youtu.be/yIG4kTJTZuY

1.2. Posing as an important user

- —In this type of attack, the hacker pretends to be a VIP or high-level manager who has the authority to use computer systems or files.
- Most of the time, low-level employees don't ask any questions of someone who appears in this position.

1.3. Being a third party

- —In this attack, the hacker pretends to have permission from an authorized person to use the computer system. It works when the authorized person is unavailable for some time.

1.4. Desktop support

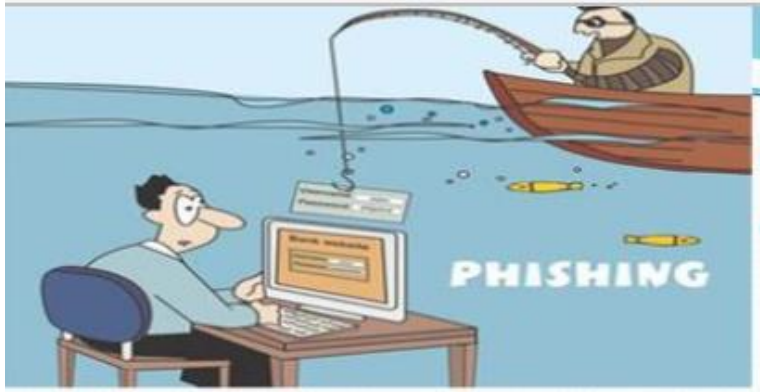
- —Calling tech support for assistance is a classic social-engineering technique.
- Help desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

1.5. Shoulder surfing

- Shoulder surfing—Shoulder surfing is the technique of gathering passwords by watching over a person's shoulder while they log in to the system.
- A hacker can watch a valid user log in and then use that password to gain access to the system.

1.6.Dumpster diving

- —Dumpster diving involves looking in the trash for information written on pieces of paper or computer printouts.
- The hacker can often find passwords, filenames, or other pieces of confidential information like SSN, PAN, Credit card ID numbers etc
- Also called dumpstering, binning, trashing, garbaging or garbage gleaning.
- scavenging

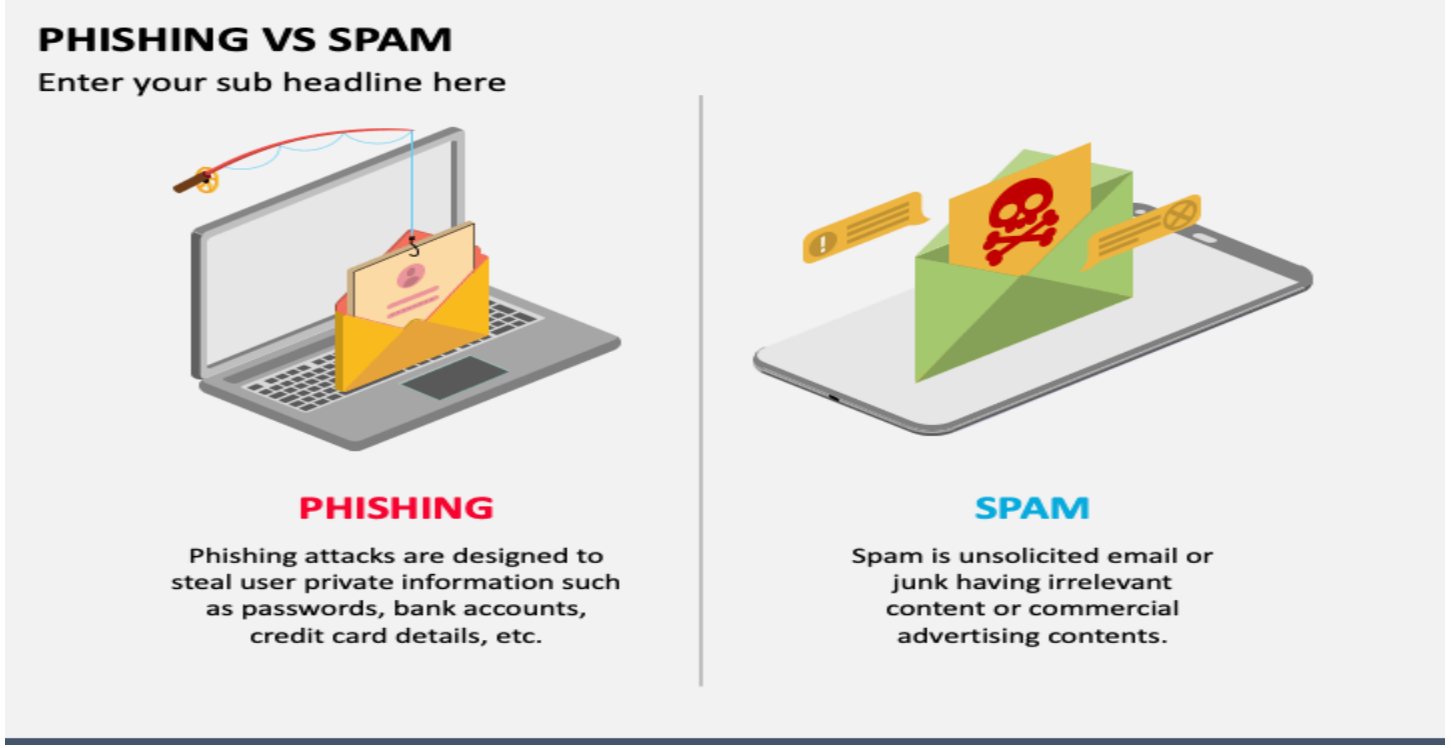


2.1Fake E-mails

- —Phishing involves false emails, chats, or websites designed to impersonate real systems with the goal of capturing sensitive data.
- A message might come from a bank or other well-known institution with the need to “verify” your login information.
- It will usually be a mocked-up login page with all the right logos to look legitimate.
- The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users.
- They replaced “f” by “ph”

Difference between Spam and Phishing

- Spam emails is referred to as junk email and is unsolicited messages sent in bulk by email. Phishing emails are fraudulent emails designed to steal users private information and data.



2.2 Baiting:

- —Baiting involves dangling something you want to entice you to take an action the criminal desires.
- It can be in the form of a music or movie download on a peer-to-peer site or it can be a USB flash drive with a company logo labeled “Executive Salary Summary Q1 2013″ left out in the open for you to find.
- Then, once the device is used or downloaded, the person or company’s computer is infected with malicious software allowing the criminal to advance into your system.

2.3 E-Mail attachments

- —Emails sent by scammers may have attachments that include malicious code inside the attachment. Those attachments can include keyloggers to capture users' passwords, viruses, Trojans, or worms.

2.4 Pop-up windows

- Sometimes pop-up windows can also be used in social engineering attacks.
- Pop-up windows that advertise special offers may tempt users to unintentionally install malicious software.

Don’t become a victim

- **Slow down.** Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
- **Research the facts.** Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company’s site, or a phone directory to find their phone number.
- **Delete any request for financial information or passwords.** If you get asked to reply to a message with personal information, it’s a scam.
- **Reject requests for help or offers of help.** Legitimate companies and organizations do not contact you to provide help. If you did not specifically request assistance from the sender, consider any offer to ’help’ restore credit scores, refinance a home, answer your question, etc., a scam. Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it. To give, seek out reputable charitable organizations *on your own* to avoid falling for a scam.
- **Don’t let a link in control of where you land.** Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.

Don’t become a victim

- **Email hijacking is rampant**. Hackers, spammers, and social engineerers taking over control of people’s email accounts (and other communication accounts) has become rampant. Once they control someone’s email account they prey on the trust of all the person’s contacts. Even when the sender appears to be someone you know, if you aren’t expecting an email with a link or attachment check with your friend before opening links or downloading.
- **Beware of any download.** If you don’t know the sender personally AND expect a file from them, downloading anything is a mistake.
- **Foreign offers are fake**. If you receive email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.
- **Set your spam filters to high.** Every email program has spam filters. To find yours, look under your settings options, and set these high–just remember to check your spam folder periodically to see if legitimate email has been accidentally trapped there. You can also search for a step-by-step guide to setting your spam filters by searching on the name of your email provider plus the phrase ’spam filters’.
- **Secure your computing devices.** Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn’t automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by your web browser or third party to alert you to risks.

Cyberstalking

- **Cyberstalking** is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization.
- It may include false accusations, defamation, slander and libel.
- It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.
- Cyberstalking is sometimes referred to as Internet stalking, e-stalking or online stalking.

Cyberstalking

- Cyberstalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group.
- A cyberstalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.
- Cyberstalking messages differ from ordinary spam in that a cyberstalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

Types of Stalkers

- online Stalkers
- offline stalkers.
- Both are criminal offenses.
- Both are motivated by a desire to control, intimidate or influence a victim.
- A stalker may be an online stranger or a person whom the target knows. He may be anonymous and solicit involvement of other people online who do not even know the target.

How stalking works?

1. Personal information gathering about the victim.
2. Establish a contact with the victim through telephone/ cell phone. – start threatening or harassing
3. Establish a contact with the victim through E-mail.
4. Keep sending repeated E-mails asking for various kinds of favors or threaten the victim.
5. Post victim's personal information on any website related to illicit services.
6. Whosoever comes across the information, start calling the victim on the given contact details, asking for sexual services.
7. Some stalkers may subscribe/ register E-Mail account of the victim to innumerable pornographic and sex sites, bez of which victim start receiving such kind of unsolicited E-Mails

The cyber stalking cases are dealt in India by the:

1. Information technology act 2000.
2. The criminal law (Amendment) act 2013.

SECTION 354D OF THE IPC

Any man who –

- follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
- monitors the use by a woman of the internet, email or any other form of electronic communication,
- commits the offence of stalking;

Provided that such conduct shall not amount to stalking if the man who pursued it proves that –

- it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or
- it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
- in the particular circumstances such conduct was reasonable and justified.

> I GET AT LEAST 4-5 CASES OF CYBERSTALKING EVERY DAY. TILL A FEW YEARS AGO, 75% CASES OF CYBERSTALKING HAD WOMEN AS THE VICTIM, BUT NOW THE RATIO IS 50:50
>
> – Karnika Seth, Supreme Court lawyer

Cyberstalking

Facts:
One Mrs. Ritu Kohli complained to the police against the a person who was using her identity to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days.

Mrs. Kohli further complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call Ritu Kohli at odd hours.

Consequently, Mrs Kohli received almost 40 callsin three days mostly at odd hours from as far away as Kuwait, Cochin, Bombay and Ahmedabad.

Contd...

The said calls created havoc in the personal life and mental peace of Ritu Kohliwho decided to report the matter.

Investigation: By Delhi Police the IP addresses were traced and the police investigated the entire matter and ultimately arrested Manish Kathuriaon the said complaint. Manish apparently pleaded guilty and was arrested.

Actions: A case was registered under section 509, of the Indian Penal Code (IPC). Nothing in IT Act

Cyber-stalking: case studies

Perth: Man charged with cyber-stalking

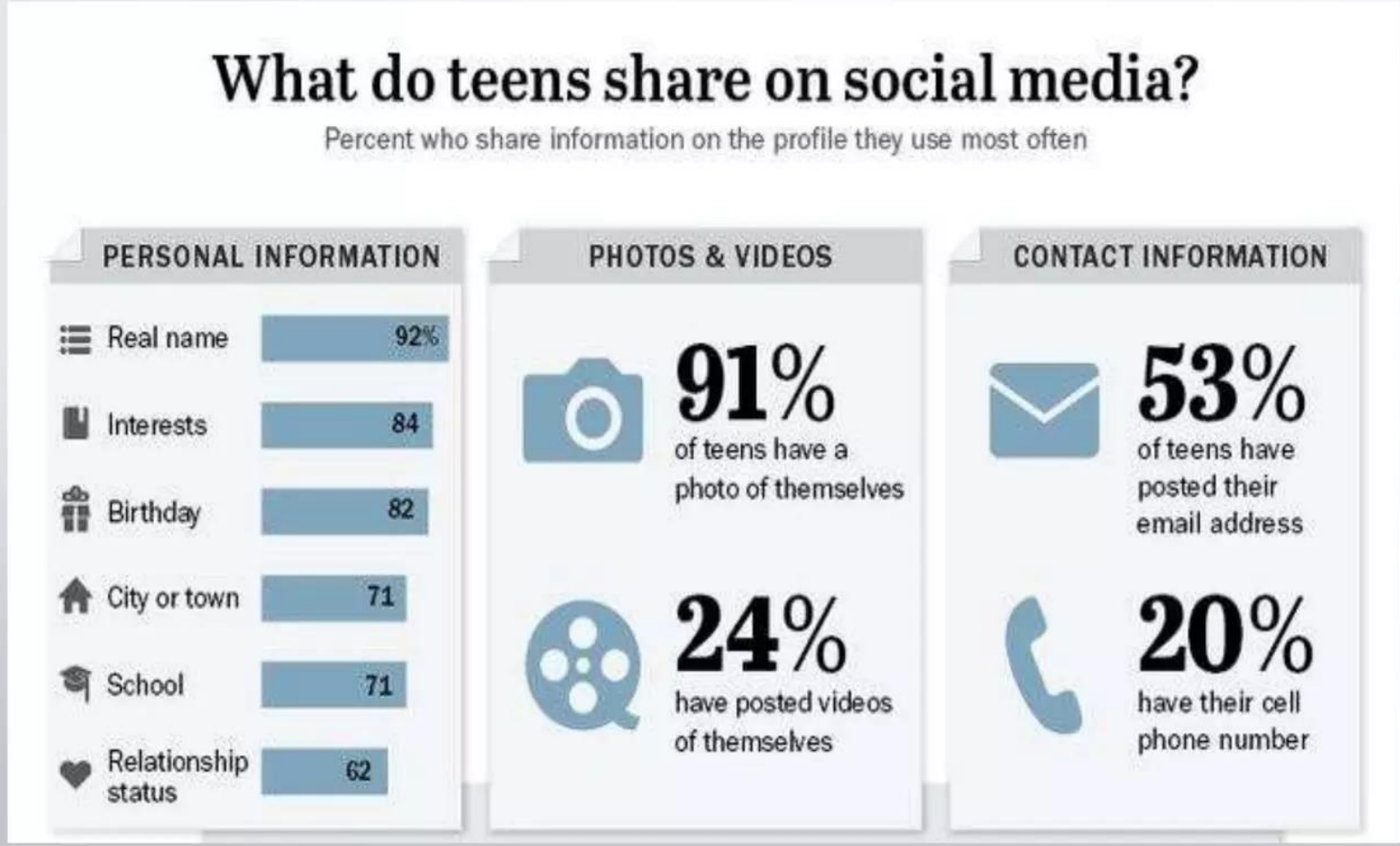
- 29 year old man in Armadale, Perth
- Stalker sent naked pictures of victims in the shower
- Threatening to post the photos on the internet if she reported to the police
- 128 charges, including:
  - unlawfully installing optical surveillance equipment,
  - indecently dealing with a child and stalking

Cyber-stalking: case studies

Illinois: ex-boyfriend cyber-stalking former lover

- "Hacker X"
- tampering and stalking ex-girlfriend online
- stealing identities and altering passwords
- Threatening her with physical harm
- 20 year sentence in jail

So is social media SAFE ?



Cybercafe and Cybercrimes

- An **Internet café** or **cybercafé** is a place which provides Internet access to the public, usually for a fee.
- According to Nielsen Survey on the profile of cybercafes users in India:

1. 37% of the total population use cybercafes
2. 90% of this were males in age group 15-35 years
3. 52% graduates and post graduates
4. > 50% were students

Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.

Role of Cybercafe

- used for either real or false terrorist communication.
- for stealing bank passwords, fraudulent withdrawal of money
  - Keyloggers or spywares
  - Shoulder surfing
- For sending obscene mails to harass people.
- They are not network service providers according to ITA2000
- They are responsible for “due deligence”

Illegal activities observed in Cybercafes

- Pirated softwares: OS, browser, Office
- Antiviruse software not updated
- Cybercafes have installed “deep freeze” software
  - This software clears details of all activities carried out, when one clicks “restart” button.
- Annual Maintenance Contract(AMC): not in place
  - Is a risk bez a cybercriminal can install Malacious code for criminal activities without any interruption
- Pornographic websites and similar websites are not blocked
- Owners have less awareness about IT Security and IT Governance.
- IT Governance guide lines are not provided by cyber cell wing
- No periodic visits to cybercafes by Cyber cell wing(state police) or Cybercafe association

Safety and security measures while using the computer in Cyber Cafe

1. Always Logout:

   do not save login information through automatic login information
2. Stay with the computer
3. Clear History and temporary files
4. Be alert:

   don't be a victim of Shoulder surfing
5. Avoid Online Financial Transaction
6. Change passwords
7. Virtual Keyboards
8. Security warnings

- Cyber Cafe Fraud #mahacyber #mumbaipolice #maharashtrapolice #cybercafe #fraud #citizen #fraudsters #fraudalert #staysafe #cybersafety #cybercrime... | By Maharashtra Cyber | Facebook

- Cyber Crime Division | CID Bangalore Karnataka (cyberpolicebangalore.nic.in)

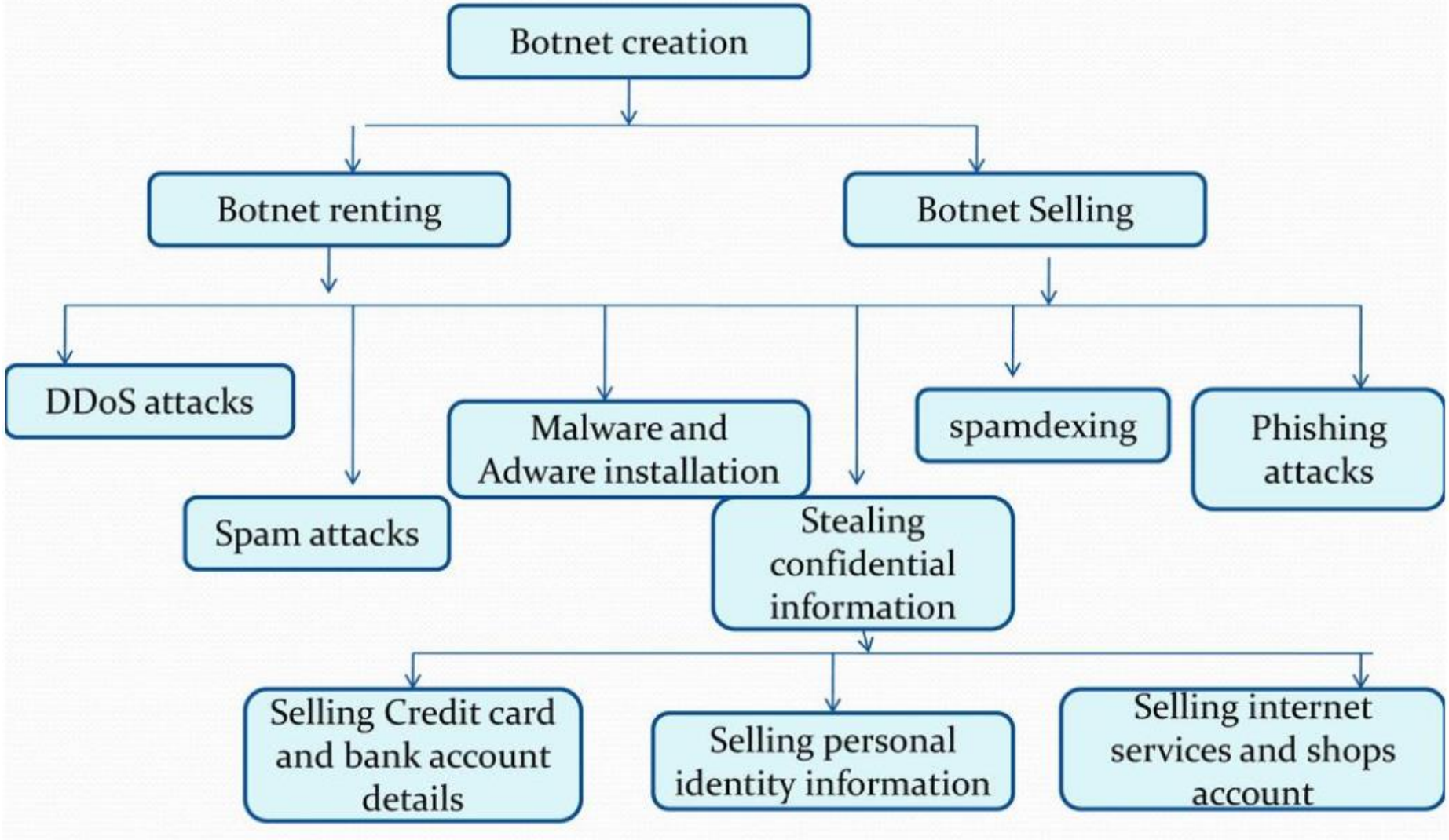
- Maharashtra Cyber | Mumbai | Facebook

Botnets: The fuel for Cybercrime

- Bot: “ an automated program for doing some particular task, often over a network”
- A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.
- Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator.
- Most computers compromised in this way are home-based.
- According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet

- What is a botnet? When IoT devices attack - YouTube

Botnet used for gainful purposes



Spamdexing

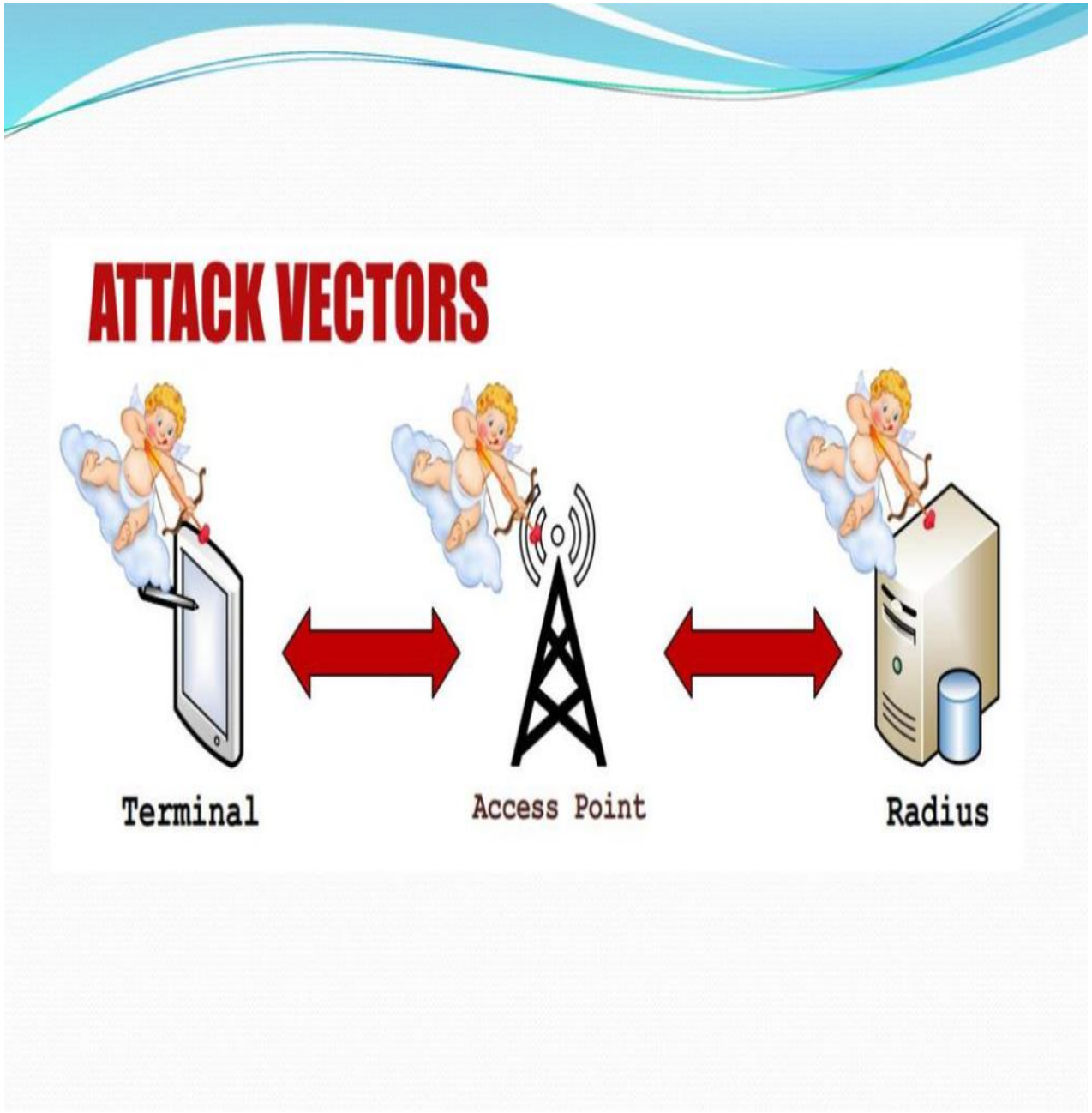
Spamdexing, also known as webspam and black-hat SEO, is an attempt to manipulate search engine rankings, so traffic is lured to a bad actor's domain. To do this, hackers gain access to a normal, healthy website, and then inject keywords and links to another web property they've set up for affiliate marketing, to monetize search traffic, or other malicious behavior.

Google's anti-spamdexing solution is called SpamBrain.

Ways to secure the system

- Use antivirus and anti-spyware
- Install updates
- Use firewall
- Disconnect internet when not in use
- Don't trust free downloads
- Check regularly inbox and sent items
- Take immediate action if system is infected

In computer security, an attack vector is a specific path, method, or scenario that can be exploited to break into an IT system, thus compromising its security



Attack vector

- An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome.
- Attack vectors enable hackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.

- To some extent, firewalls and anti-virus software can block attack vectors.
- But no protection method is totally attack-proof.
- A defense method that is effective today may not remain so for long, because hackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers.

- If vulnerabilities are the entry points, then attack vectors are the ways attackers can launch their assaults or try to infiltrate the building.
- In the broadest sense, the purpose of the attack vectors is to implant a piece of code that makes use of a vulnerability. This code is called the ***payload,*** and attack vectors vary in how a payload is implanted.
- The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan horses, worms, and spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

Different ways to launch Attack Vectors:

- Attack b y E-Mail
- Attachments
- Attack b y deception: social engineering/ haoxes
- Hackers
- Heedless guests (attack by webpage)
- Attack of the worms
- Malicious macros
- Foistware/ sneakware
- viruses

A zero-day attack

- A **zero-day** (or **zero**-hour or **day zero**) **attack** or threat is an **attack** that exploits a previously unknown vulnerability in a computer application or operating system, one that developers have not had time to address and patch.
- Software vulnerabilities may be discovered by hackers, by security companies or researchers, by the software vendors themselves, or by users.
- If discovered by hackers, an exploit will be kept secret for as long as possible and will circulate only through the ranks of hackers, until software or security companies become aware of it or of the attacks targeting it.
- ZERT

- This is how hackers hack you using simple social engineering - YouTube

What is social engineering? - YouTube