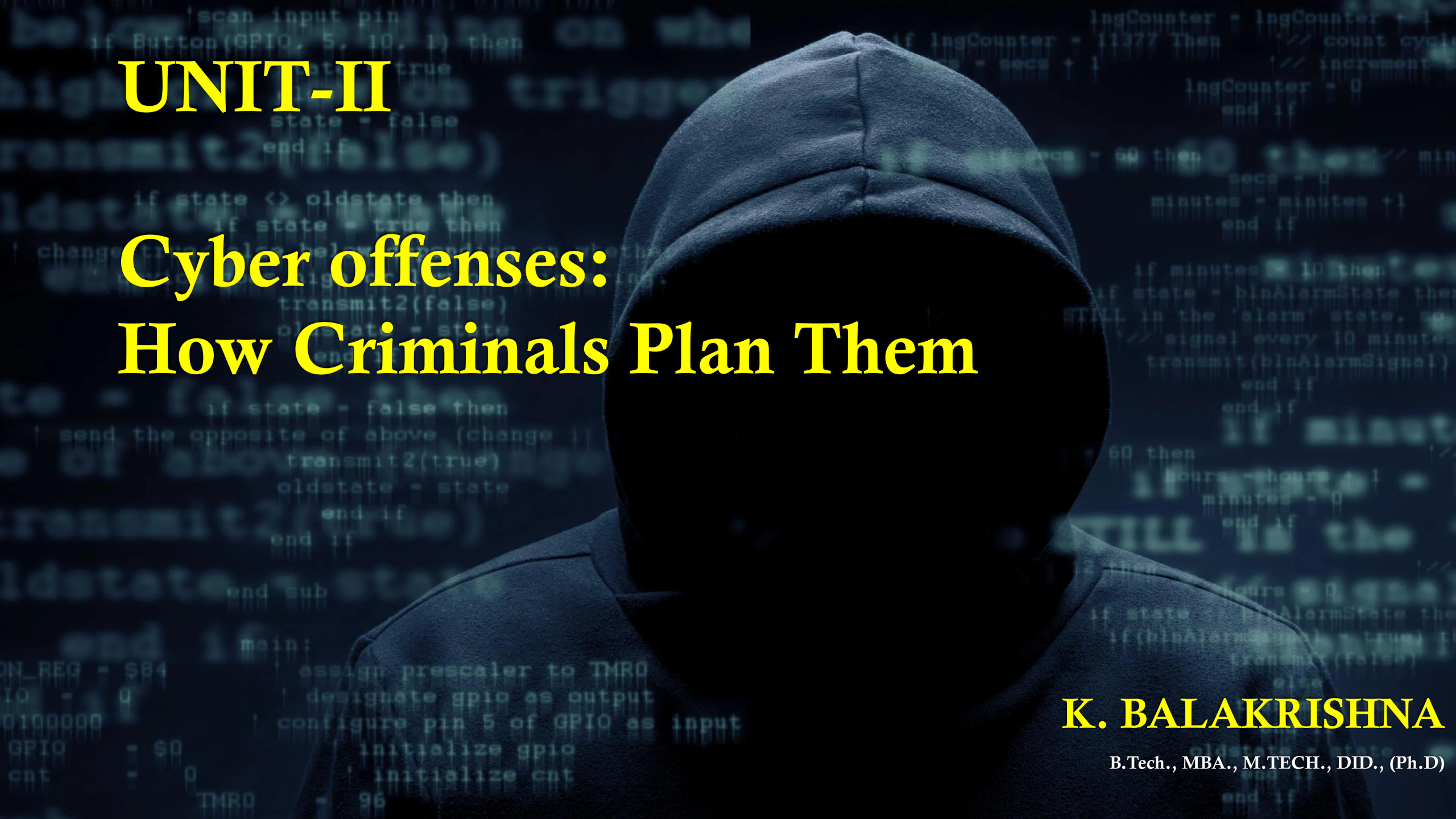


UNIT-II

Cyber offenses: How Criminals Plan Them

K. BALAKRISHNA

B.Tech., MBA., M.TECH., DID., (Ph.D)

1. Introduction

In today's world of Internet and computer networks, a criminal activity can be carried out across national borders with "false sense of anonymity". An attacker would look to exploit the vulnerabilities in the networks such as:

1. Inadequate border protection (border as in the sense of network periphery);
2. Remote access servers (RASs) with weak access controls;
3. Application servers with well-known exploits;
4. Misconfigured systems and systems with default configurations.

Categories of Cybercrime:

Cybercrime can be categorized based on the following:

1. The target of the crime and
2. Whether the crime occurs as a single event or as a series of events.

1. Introduction

The target of the crime:

1.Crimes targeted at individuals

2.Crimes targeted at property

3.Crimes targeted at organizations

4.Single event of cybercrime

5.Series of events

2. How Criminals Plan the Attacks

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.

2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.

3. Launching an attack (gaining and maintaining the system access).

Reconnaissance:

"Reconnaissance" is an act of reconnoitering – explore, often with the goal of finding something or somebody (especially to gain information about an enemy or potential enemy).

Reconnaissance begins with "Footprinting" – this is the preparation toward pre-attack phase

- involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.

Passive Attacks:

- A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge.
- It is usually done using Internet searches or by Googling an individual or company to gain information.

2. How Criminals Plan the Attacks

Active Attacks:

- An active attack involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase.
- It involves the risk of detection and is also called “Rattling the doorknobs ” or “Active reconnaissance”.
- Active reconnaissance can provide confirmation to an attacker about security measures in place.

Scanning and Scrutinizing Gathered Information:

The objectives of scanning are:

1. Port scanning: Identify open/close ports and services.

2. Network scanning: Understand IP Addresses and related information about the computer network systems.

3. Vulnerability scanning: Understand the existing weaknesses in the system.

2. How Criminals Plan the Attacks

Attack (Gaining and Maintaining the System Access):

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password;
2. Exploit the privileges;
3. Execute the malicious commands/applications;
4. Hide the files (if required);
5. Cover the tracks – delete the access logs,

so that there is no trail illicit activity.

3. Social Engineering

- It is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- The sign of truly successful social engineers is that they receive information without any suspicion.

Classification of Social Engineering:

1. Human-Based Social Engineering:

Human-based social engineering refers to person-to-person interaction to get the required/desired information.

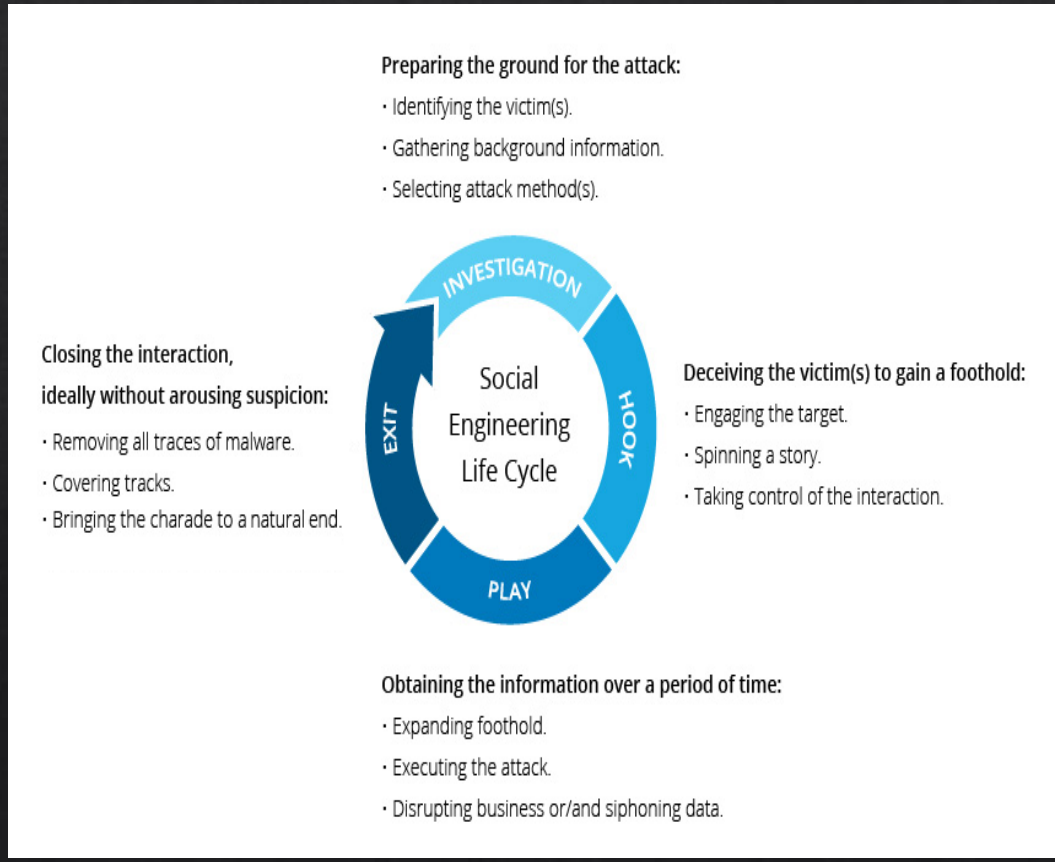
2. Computer-Based Social Engineering:

Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.

3. Social Engineering

There are many different ways to classify social engineering attacks, but some of the most common classifications include:

- ***Targeted vs. mass attacks:*** Targeted attacks are those that are specifically designed to target a particular individual or organization. Mass attacks, on the other hand, are those that are designed to reach a large number of people.
- ***In-person vs. remote attacks:*** In-person attacks are those that are carried out in person, such as a tailgating attack or a pretexting attack. Remote attacks, on the other hand, are those that are carried out over the internet, such as a phishing attack or a spear phishing attack.
- ***Technical vs. non-technical attacks:*** Technical attacks rely on the use of technology, such as malware or phishing emails. Non-technical attacks, on the other hand, rely on social skills and persuasion, such as pretexting or tailgating.



3. Social Engineering

Type of Attack	Description
Phishing	This is an email or text message that appears to be from a legitimate source, such as a bank or credit card company. The message will often contain a link or attachment that, when clicked, will install malware on the victim's computer.
Spear phishing	This is a type of phishing attack that is specifically targeted at a particular individual or organization. The attacker will often do research on the victim in order to make the attack more believable.
Pretexting	This is a technique in which the attacker pretends to be someone they're not in order to gain the victim's trust. For example, the attacker might call the victim and claim to be from their bank, asking for their account information to "verify their identity."
Baiting	This is a technique in which the attacker leaves a USB drive or other device in a public place, hoping that someone will pick it up and plug it into their computer. The device will often contain malware that will be installed on the victim's computer when they plug it in.
Quid pro quo	This is a technique in which the attacker offers the victim something in exchange for their personal information or other sensitive data. For example, the attacker might offer the victim a free gift or discount in exchange for their credit card number.
Tailgating	This is a technique in which the attacker follows someone who is authorized to enter a secure area. The attacker will often pretend to be a legitimate employee or contractor.
Physical impersonation	This is a technique in which the attacker impersonates a real person in order to gain access to a secure area or to obtain personal information.

4. Cyberstalking

- It is defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- It involves harassing or threatening behavior that an individual will conduct repeatedly.
- As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

Types of Stalkers:

There are primarily two types of stalkers as listed below:

1. Online stalkers: They aim to start the interaction with the victim directly with the help of the Internet.

2. Offline stalkers: The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.

4. Cyberstalking

Here are some of the ways cyberstalking works:

- ***Direct contact:*** The stalker may send emails, text messages, or social media messages to the victim. These messages may be threatening, harassing, or simply annoying.
- ***Indirect contact:*** The stalker may post information about the victim online, such as their address, phone number, or workplace. They may also create fake social media profiles or websites in the victim's name.
- ***Tracking:*** The stalker may use tracking software to follow the victim's online activity. This information can be used to learn about the victim's habits and movements.
- ***Impersonation:*** The stalker may impersonate the victim online. This can be done by creating fake social media profiles or websites in the victim's name.
- ***Threats:*** The stalker may make threats to the victim, either online or in person. These threats may be verbal, written, or implied.

4. Cyberstalking

How Stalking Works? Steps:

1. Personal information gathering about the victim

2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.

3. Stalkers will almost always establish a contact with the victims through E-Mail. The stalker may use multiple names while contacting the victim.

4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.

5. The stalker may post the victim's personal information on any website related to illicit service such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details The stalker will use bad and/or offensive/attractive language to invite the interested persons.

6. Whosoever comes across the information, start calling the victim on the given contact details asking for sexual services or relationships.

7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

4. Cyberstalking

Examples of Cyberstalking:

Some of the common examples of cyberstalking are:

- Making rude, offensive, or suggestive online comments
- Joining the same groups and forums to follow the target online
- Sending the target threatening, controlling, or lewd messages or emails
- Making a fake social media profile to follow the victim
- Gaining access to the victim's online accounts
- Posting or disseminating real or fictitious photos of the victim
- Attempting to obtain explicit photographs of the victim
- Tracking the victim's online movements using tracking devices
- Mailing explicit photos of themselves to the victim on a regular basis, etc.

4. Cyberstalking

If you are being cyberstalked, it is important to take steps to protect yourself. Here are some things you can do:

Save evidence: Save all emails, text messages, social media messages, and other forms of communication from the stalker. This evidence can be used to help you get a restraining order or press charges.

Block the stalker: You can block the stalker on social media, email, and text messaging. This will prevent them from contacting you directly.

Change your passwords: Change your passwords for all of your online accounts. This will make it more difficult for the stalker to access your information.

Report the stalking: If you are being cyberstalked, you should report it to the police. They can help you get a restraining order and investigate the stalking.

5. Cybercafe and Cybercrimes

- Cybercafes, also known as internet cafes, are establishments that provide public access to computers and internet services for a fee. These venues are often equipped with multiple computer terminals, high-speed internet connections, and various software applications to cater to the needs of their customers.
- Cybercafes offer a range of services, including web browsing, email access, online gaming, document printing, and sometimes even food and beverages.
- They are popular in areas where individuals may not have personal computers or reliable internet connections at home, such as developing countries or regions with limited infrastructure.
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.
- Cybercafes have also been used regularly for sending obscene mails to harass people.
- Indian Information Technology Act (ITA) 2000 interprets cybercafes as “network service providers” referred to under the erstwhile Section 79, which imposed on them a responsibility for “due diligence” failing which they would be liable for the offenses committed in their network.

5. Cybercafe and Cybercrimes

Safe Banking for online Services

icicibank.com/online-safe-banking

ICICI Bank | PERSONAL + | NRI | BUSINESS + | CORPORATE | GIFT CITY | CALL 1800 1080 | PERSONAL | LOGIN

Search for Products, Services

iPlay | Digital Banking | HELP & CONTACT

ACCOUNTS | CARDS | LOANS | INVEST | INSURE | PAY | OFFERS | CAMPUS POWER NEW | APPLY ONLINE

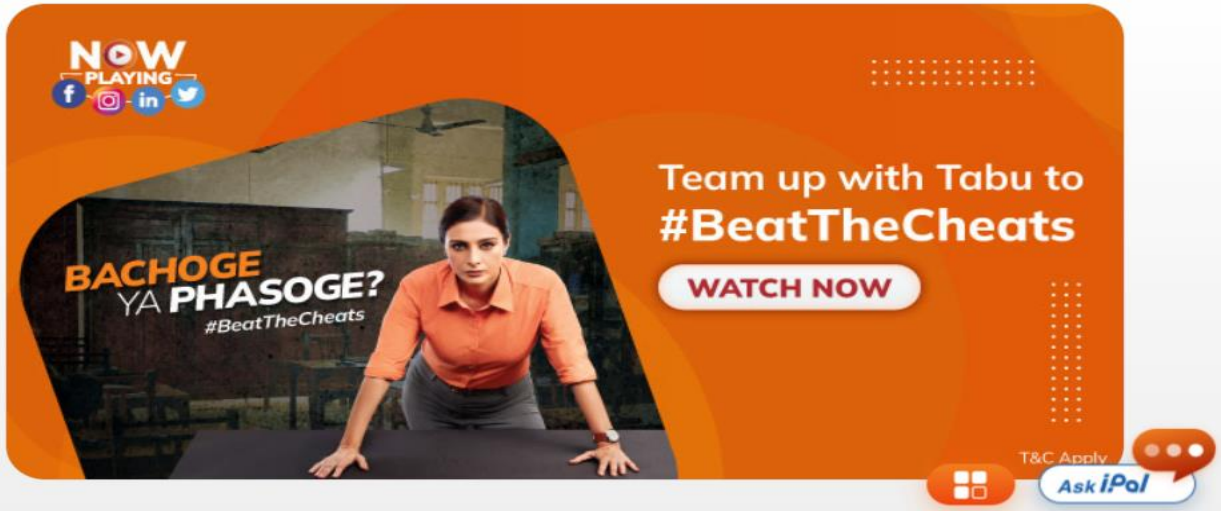
Home • Safe Banking

SAFE BANKING | ICICI BANK I-SAFE | REPORT AN UNAUTHORIZED TRANSACTION | MORE

Online Safe Banking

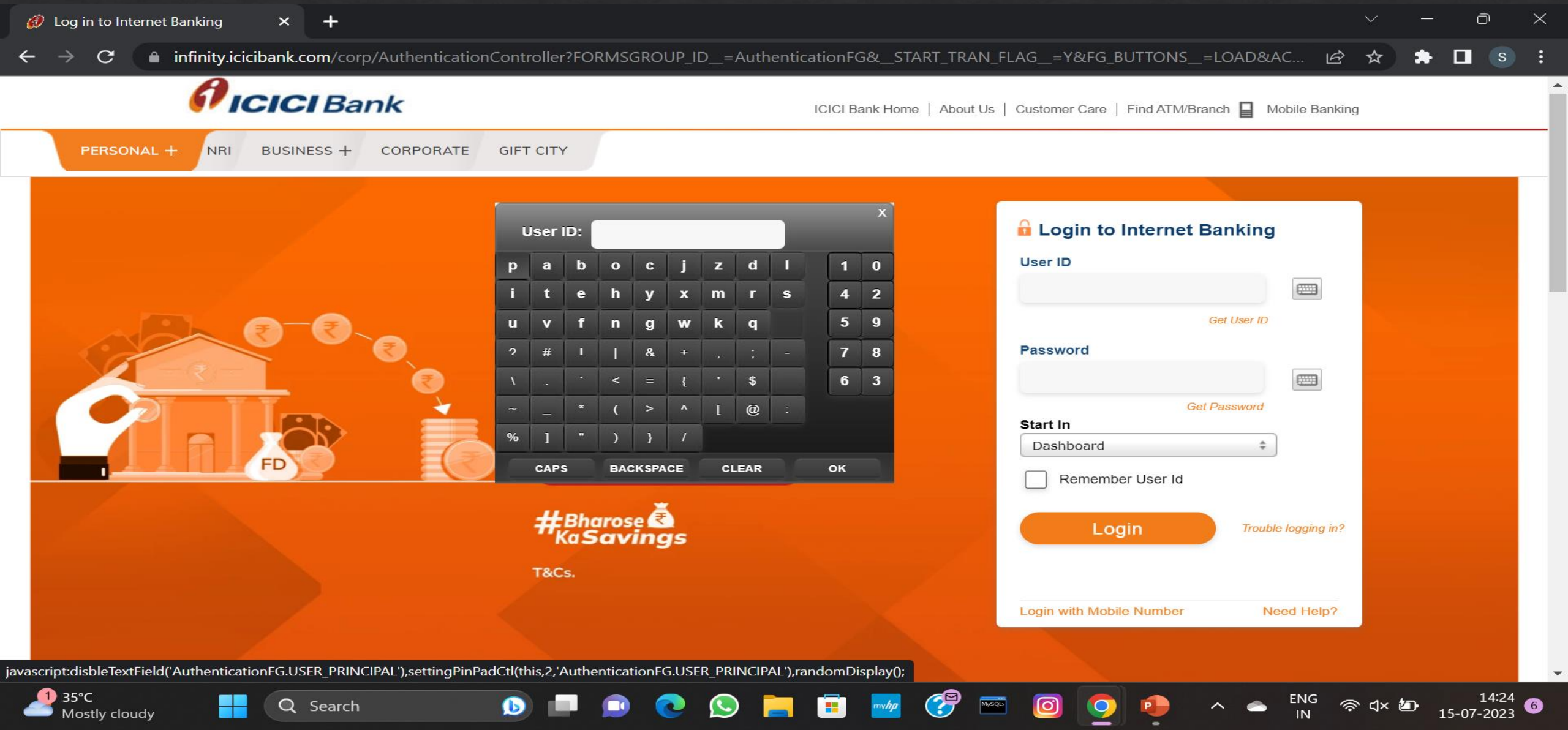
Bank employees will never ask for your Password/ PIN/ OTP/ CVV/ Card Number

Sharing your details can lead to transfer of money from your account.



35°C Mostly cloudy | Search | ENG IN | 14:22 15-07-2023

5. Cybercafe and Cybercrimes



5. Cybercafe and Cybercrimes

Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.

Here are a few tips for safety and security while using the computer in a cybercafe:

1. Always logout
2. Stay with the computer
3. Clear history and temporary files
4. Be alert
5. Avoid online financial transactions
6. Change passwords
7. Virtual keyboard
8. Security warnings

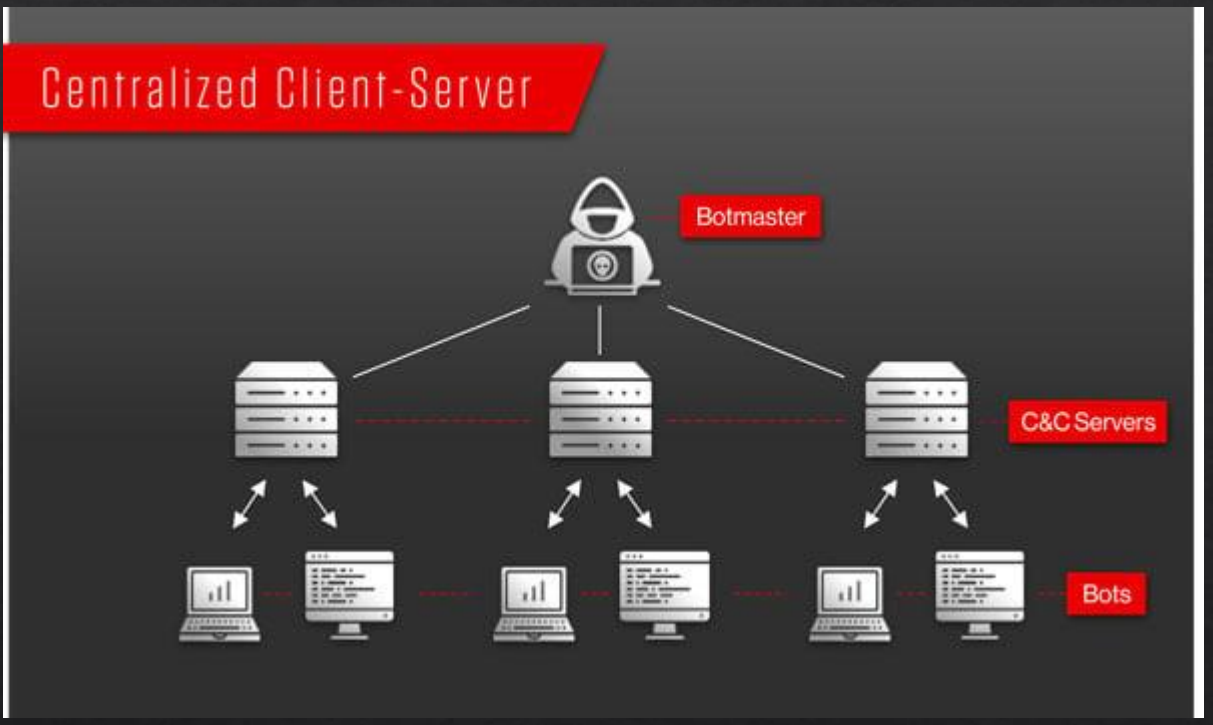
6. Botnets

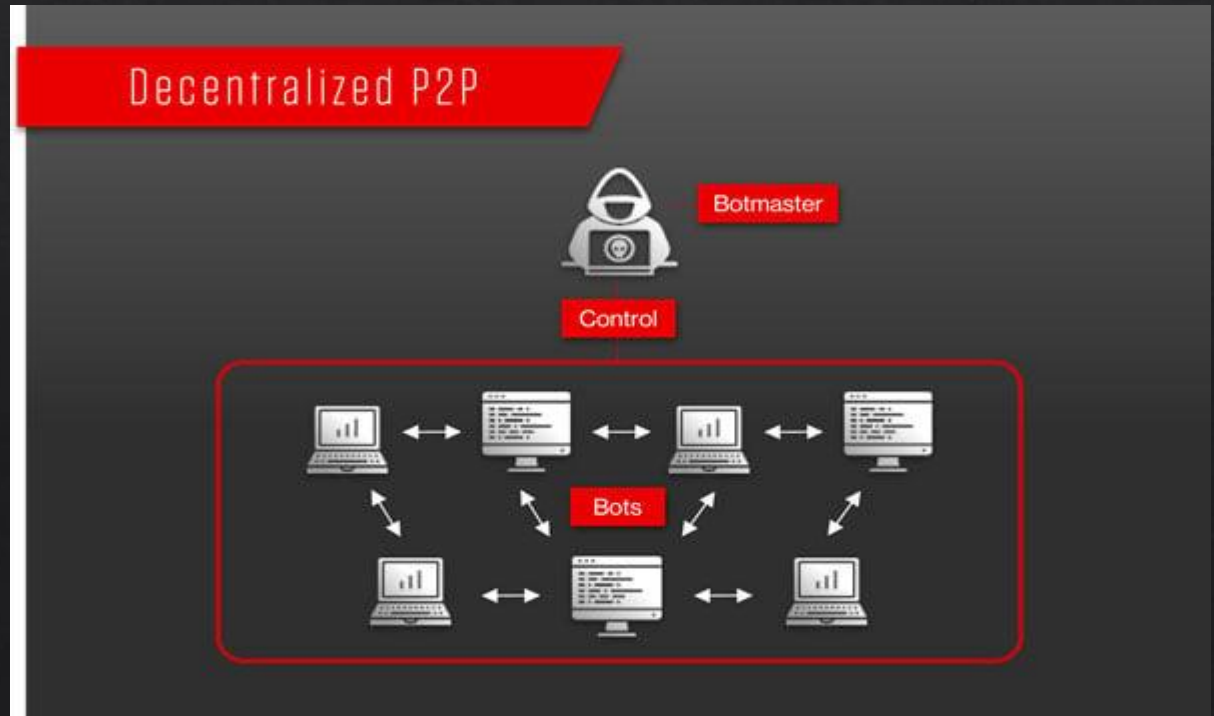
- ***Malware*** is currently the major source of attacks and fraudulent activities on the Internet. Malware is used to infect computers.
- ***Botnet*** is a network of zombies, i.e. compromised computers under control of an attacker.
- ***Bot*** is a program loaded on zombie computer that provides remote control mechanisms to an attacker.
  Bot - a small program to remotely control a computer
- ***Bot -*** Characterized by:
  - Remote control & communication (C&C) channels to command a victim (*For ex., perform denial-of service attack, send spam)*
  - The implemented remote commands (*For ex., update bot binary to a new version)*
  - The spreading mechanisms to propagate it further (*For ex., port scanning, email)*

C&C channel:

- Means of receiving and sending commands and information between the botmaster and the zombies.
- Typical protocols: IRC, HTTP, Overnet (Kademlia)
- Protocols imply (to an extend) a botnet's communication topology.
  - The topology provides trades-off in terms of bandwidth, affectivity, stealth, and so forth.

6. Botnets: The Fuel for Cybercrime





6. Botnets: The Fuel for Cybercrime

The client-server botnet:

- The traditional client-server model involves setting up a command and control (C&C) server and sending automated commands to infected botnet clients through a communications protocol, such as Internet Relay Chat (IRC).
- The bots are then often programmed to remain dormant and await commands from the C&C server before initiating any malicious activities or cyber attacks.

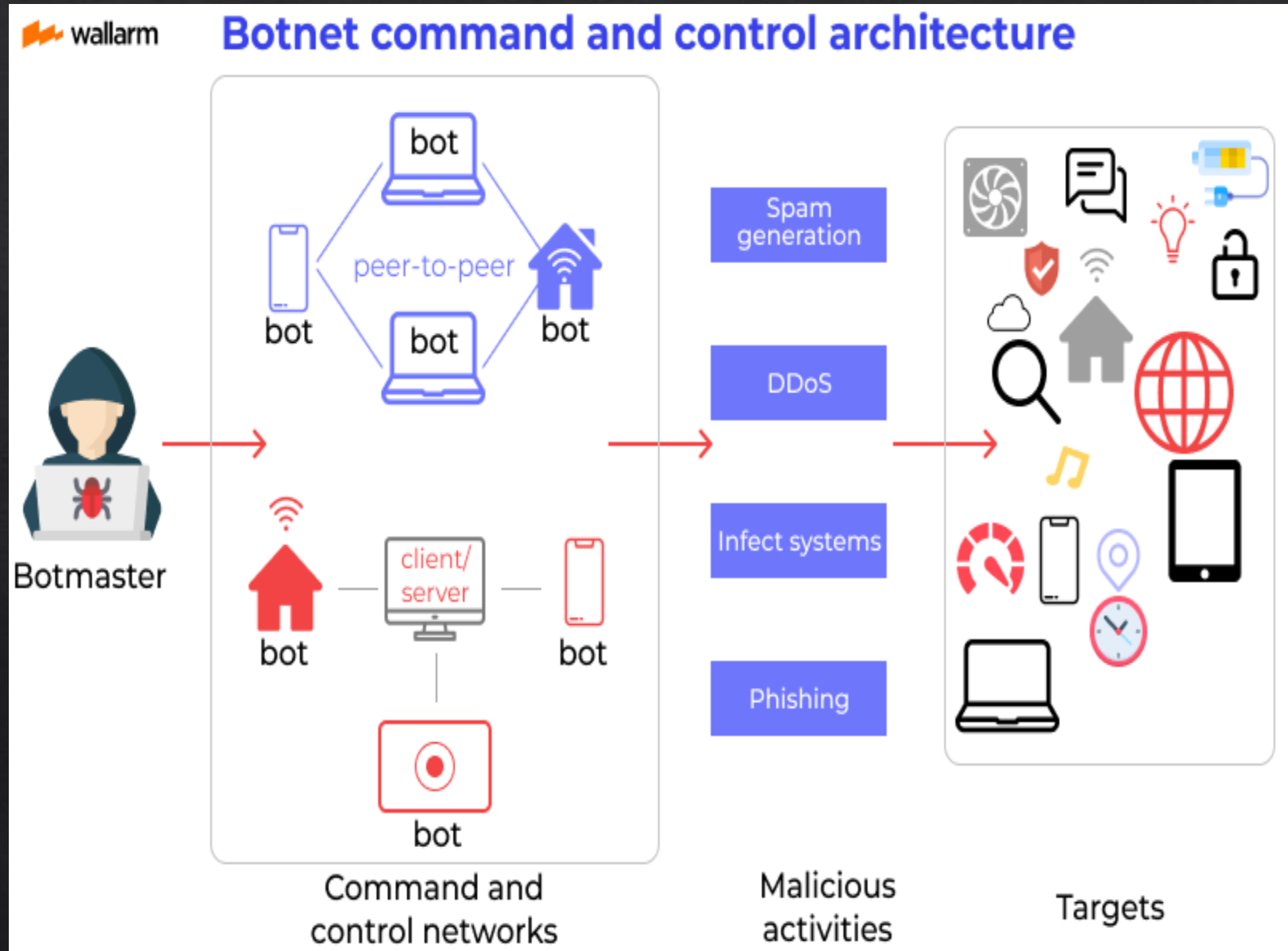
The P2P botnet:

- The other approach to controlling infected bots involves a peer-to-peer (P2P) network. Instead of using C&C servers, a P2P botnet relies on a decentralized approach. Infected devices may be programmed to scan for malicious websites or even for other devices that are part of a botnet. The bots can then share updated commands or the latest versions of the malware.
- The P2P approach is more common today, as cybercriminals and hacker groups try to avoid detection by cybersecurity vendors and law enforcement agencies, which have often used C&C communications to locate and disrupt botnet operations.

6. Botnets: The Fuel for Cybercrime

The Architecture of a Botnet:

- Botnet infections are usually spread through malware or spyware. Botnet malware is typically designed to automatically scan systems and devices for common vulnerabilities that haven't been patched in hopes of infecting as many devices as possible.
- Once the desired number of devices is infected, attackers can control the bots using two different approaches.

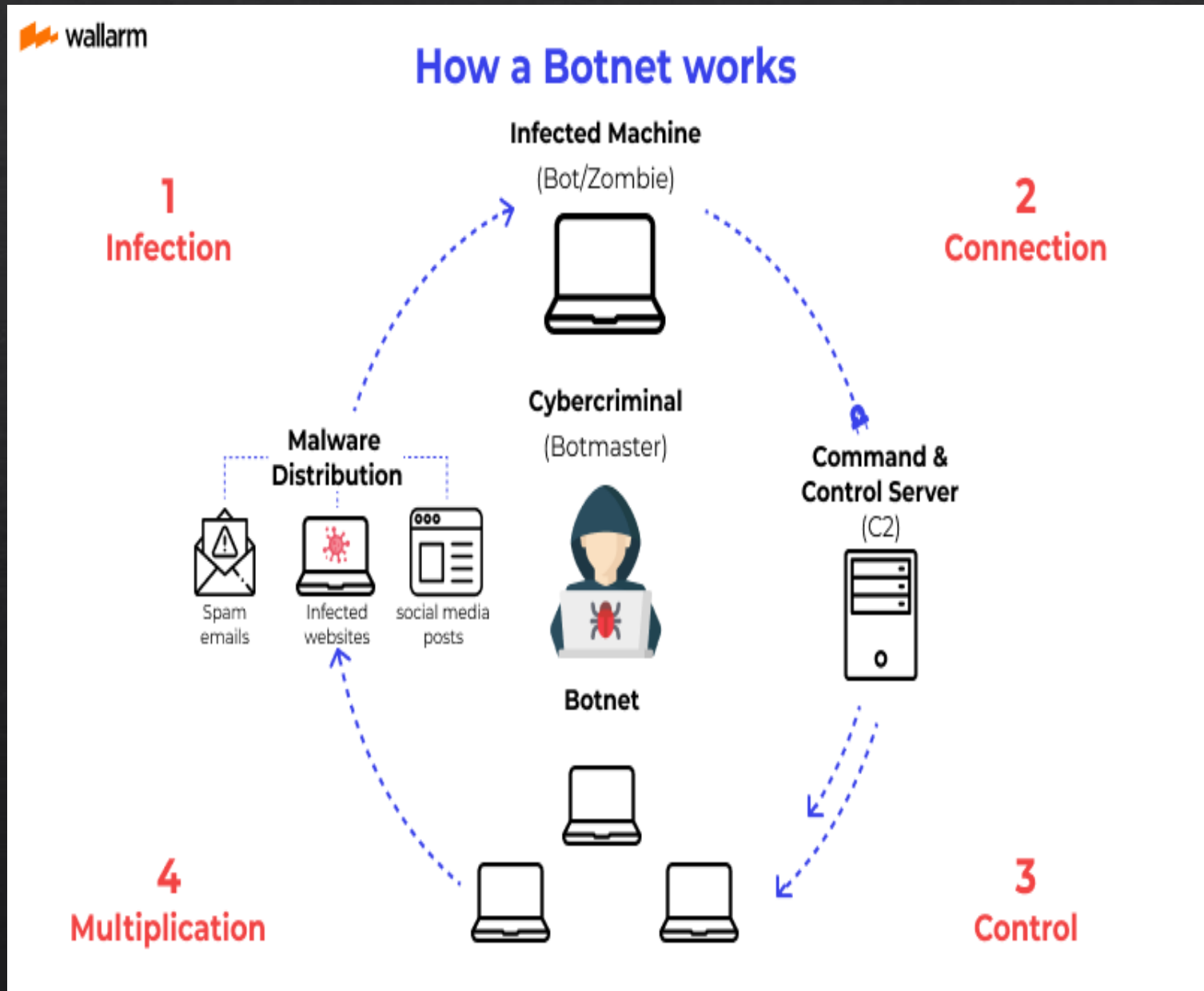


6. Botnets: The Fuel for Cybercrime

Stages of Botnet Building - The procedure involves three steps:

Stage 1 - Prepare and Expose:

- At this stage, the bad actor figures out the vulnerability to introduce into the user's device.
- The vulnerability hunting takes place in the website, human behavior, and application. By doing so, the hacker prepares a set-up to lure the target to get exposed to malware, knowingly or unknowingly.
- Most commonly, hackers figure out the vulnerabilities in websites and the software. Additionally, malware is delivered via emails or random messages.



6. Botnets: The Fuel for Cybercrime

Stage 2 - Infecting the user via malware:

- The next action that the botnet performs is activating the malware so that the end-user is infected and has compromised security. The process of infecting the device usually takes place via the Trojan virus or social engineering method.
- Some attackers adopt a more hostile approach and deploy drive-by-download techniques to infect the device. Using all these methods, attackers corrupt the targeted device with botnet malware.

Stage 3 - Controlling the targeted devices:

- The last stage of botnet working methodology is gaining control over each device. Hackers systematize the involved infected machines in the botnet and design a methodology to manage them remotely. In general, around thousands of devices are controlled in the process via a huge zombie network. Once the stage is successfully completed, the bad actor is able to gain admin-like access to the targeted devices or computers.
- The fruitful activation of the botnet allowed hackers to read or write the data stored in the system, capture any personal information, share the data from targeted devices, keep an eye on all the activities happening on the targeted device, and search other hidden vulnerabilities.

6. Botnets: The Fuel for Cybercrime

How to Protect Your Computer from Botnets?

Botnet attacks can be too damaging, if not handled properly. The below-mentioned ways can keep botnet attacks at bay.

- Updated OS
- Download from trusted resources
- No accessibility to suspicious links
- Paying attention to website security
- Stay away from P2P downloads
- Changing login details while introducing new devices
- Using the protection of firewall
- Strong password and 2FA (two–factor authentication)
- Deployment of anti-virus software
- Dependable security tool

7. Attack Vector

An *attack vector, or threat vector*, is a way for attackers to enter a network or system. Common attack vectors include social engineering attacks, credential theft, vulnerability exploits, and insufficient protection against insider threats.

Most common attack vectors:

Phishing: Phishing involves stealing data, such as a user's password, that an attacker can use to break into a network. Attackers gain access to this data by tricking the victim into revealing it.

Email attachments: One of the most common attack vectors, email attachments can contain malicious code that executes after a user opens the file.

Vishing: we define vishing as the practice of eliciting information or attempting to influence action via the telephone. Vishing, also known as voice phishing, is a dangerous attack vector. The goal of vishing is to obtain valuable information, contributing to the direct compromise of a target. Attackers may “spoof,” or fake, their outgoing phone number to add authenticity to their attack. Additionally, some bad actors may use voice changers to conceal their identity. They may also use artificial-intelligence based software to mimic authentic voices. In their attacks, bad actors may pose as an authority figure, technician, or fellow employee.

7. Attack Vector

Mishing: It is a type of social engineering attack that uses a fake email or text message to trick the victim into clicking on a malicious link. The link will typically take the victim to a website that looks like a legitimate website, but is actually controlled by the attacker. Once the victim clicks on the link, they will be infected with malware that can steal their personal information or give the attacker access to their computer.

The Mishing attack vector is named after the fact that the emails or text messages often contain misspellings or grammatical errors. This is done to make the messages look more authentic, as scammers know that many people will be more likely to click on a link if they think it is from a legitimate source.

Smishing: is a type of phishing attack that uses text messages (SMS) to trick victims into clicking on malicious links or providing personal information. The term SMISHING is a portmanteau of "SMS" and "phishing."

Smishing attacks often look like they are from a legitimate source, such as a bank or a shipping company. The messages may say that there is a problem with your account, or that you have a package that is waiting for you. The messages will often include a link that, when clicked, will take the victim to a fake website that looks like the legitimate website. Once the victim enters their personal information on the fake website, the attacker can steal it.

7. Attack Vector

COMPROMISED CREDENTIALS

describe a case where user credentials, such as usernames and passwords, are exposed to unauthorized entities.

WEAK AND STOLEN CREDENTIALS

Weak passwords and password reuse make credential exposure a gateway for initial attacker access and propagation.

MALICIOUS INSIDERS

an employee who exposes private company information and/or exploits company vulnerabilities.

POOR ENCRYPTION

leads to sensitive information including credentials being transmitted either in plaintext, or using weak cryptographic ciphers or protocols.

MISCONFIGURATION

Misconfiguration is when there is an error in system configuration. Misconfigured devices and apps present an easy entry point for an attacker to exploit.

RANSOMWARE

is a form of cyber-extortion in which users are unable to access their data until a ransom is paid.

PHISHING

is a cybercrime tactic in which the targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data

TRUST RELATIONSHIPS

an attacker exploits the trust between two entities to gain unauthorized access to a system or network.

Balbix

7. Attack Vector

Bluetooth: As wireless devices have become popular, the use of Bluetooth technology has become a common scenario. From earphones to smart watches everything is connected with a simple Bluetooth technology, but if there are upsides to the technology, there are downsides too.

Bluetooth Hacking?

Bluetooth hacking is a technique used to get information from another Bluetooth enabled device without any permissions from the host. This event takes place due to security flaws in Bluetooth technology. Bluetooth hacking is not limited to cell phones, but is also used to hack laptops, mobiles and desktop computers.

Below are the three common hacking:

BlueBorne: As the name suggests, borne means spread through air, BlueBorne is an attack virus that spreads through air and gets into a device via Bluetooth and can then take full control of the device. The targeted device does not need to be paired to the attacker's device or even to be set on discoverable mode, only if the bluetooth is on the phone can be hacked.

7. Attack Vector

Bluesnarfing:

Bluesnarfing is when the hacker pairs with users' device without the user being aware about it and steals or compromises your personal data. The attackers use tools like bluediving, which can be used for testing Bluetooth devices for known vulnerabilities and major things to hack into the device.

BlueBugging :

As discoverable mode is a default setting in many devices, hackers can take control of the device i.e could listen to calls, read and send messages, and steal contacts,this is BlueBugging. It is done by pairing the device through Bluetooth.

How to know that the device is hacked?

- Unrecognized software installation, text messages one didn't send, purchases one didn't make, suspicious phone calls.
- Device works slower, uses way more resources and battery power and becomes hotter than usual. Malware working in the background might reduce its power significantly.

7. Attack Vector

- Mysterious data usage spikes without any changes in usage on the individual's part. Malicious processes might consume mobile data in the background.
- Apps that don't run the way they should, switch on and off unexpectedly, or that crash or fail to load.
- If one notices lots of pop-ups appearing on your screen, then probably there is spyware or malware.

Tips to safeguard Bluetooth devices:

- Turn off Bluetooth and Wi-Fi when it is not needed, especially in public places.
- Do not accept pair requests from unknown devices
- Make sure you always have the latest system software
- Ensure that one purchases device has adequate security features
- Change Bluetooth settings to not discoverable
- Always unpair with other devices after sharing
- Use Two step authentication
- Secure Bluetooth with password & Stay away from open Wi-Fi and always use Virtual Private Network.

8. Cloud Computing

Cloud computing is a method of delivering computing services over the internet, including servers, storage, networks, software, and analytic data. Companies choose cloud computing to reduce costs, gain agility, and improve cloud security. As cloud services, including cloud security, are easily scalable, it is a way to support continuity even during times of rapid growth.

Cloud computing services: These three are SaaS, PaaS, and IaaS.

- ***Software as a Service (SaaS)*** is a cloud application service. Organizations frequently use this to deliver their applications to the end-user, while a third party manages the application through a private cloud.
- ***Platform as a Service (PaaS)*** is a cloud platform service that allows developers to work on their applications through the cloud. This simplifies their development management process and allows them to solely focus on development while the organization or a third party manages the server, storage, and networking.
- ***Infrastructure as a Service (IaaS)*** offers organizations a complete working infrastructure, from storage, networking, monitoring, and other services, all on a private cloud. This simplifies the management practices of an organization and frees resources that would have otherwise been used in the case of legacy infrastructure.

Most Common Security Threats for Cloud Services

Malware & Rouge Software

- Unwanted software running in the system: Embedded software & Apps
- Designed to steal information – leading cause of data loss

DDoS

- Targeted attacks to consume cloud resources to deny services to users
- Slows down performance and results in customer dissatisfaction

Brute Force Password Attack

- Continuous login attempts, attacks on insecure interfaces & APIs
- If successful, accounts are hijacked & used for nefarious activities

Man in the Middle Attack

- Pretends to be a legitimate destination, copies all data and passes it on to actual users
- Very difficult to detect

Advanced Persistent Threats

- Parasitical form of cyber attack that infiltrates systems to steal data
- Usually a malware that resides within the data center

Phishing

- Uses Social Engineering to get access into system

System Vulnerabilities

- Exploits all known system vulnerabilities such as Spectre, Meltdown
- Race against time to exploit known vulnerabilities

8. Cloud Computing

7 Ways to protect the data that drives your business:

1. Adapt the principle of least privilege
2. Use a password manager
3. Embrace two-factor authentication
4. Implement encryption in the cloud
5. Control access for third-party apps
6. Arm yourself with knowledge:
   - Verify suspicious emails and texts with the sender by sending a new email or by picking up the phone and giving them a call.
   - Ignore and delete unsolicited emails or texts from people outside the organization.
   - Do not open or click suspicious documents or links in an email or text. Always verify with the sender in a different channel before taking action.
   - Be suspicious; always be alert when receiving unsolicited instructions via email. If you are unsure, best to leave it.
7. Back up cloud data