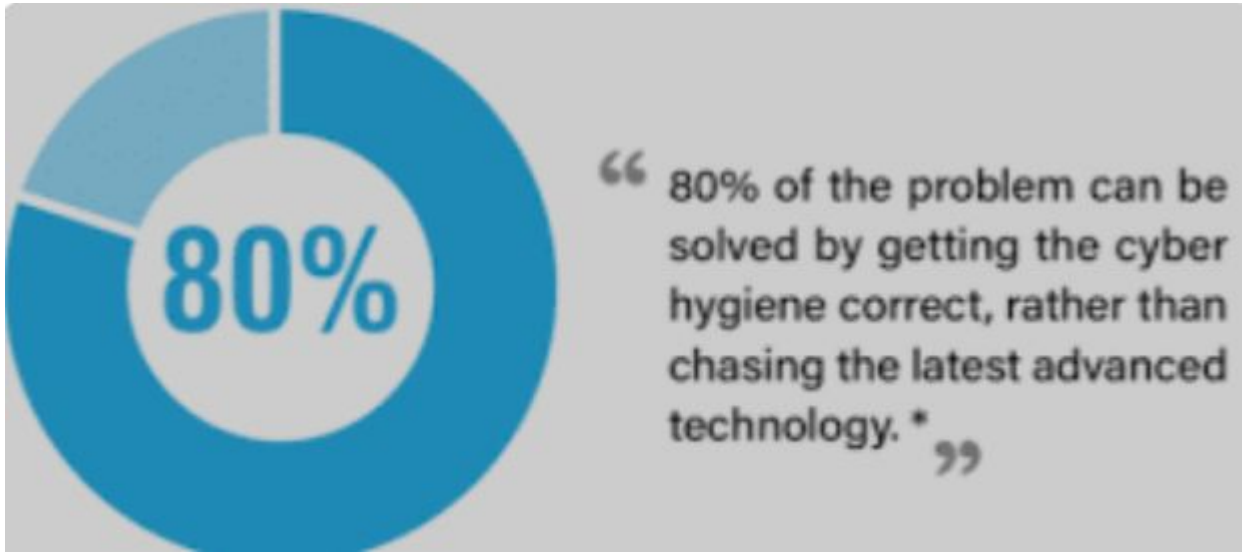
Unit-02 Cyber Offenses



“80% of the problem can be solved by getting the cyber hygiene correct, rather than chasing the latest advanced technology. *”

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:

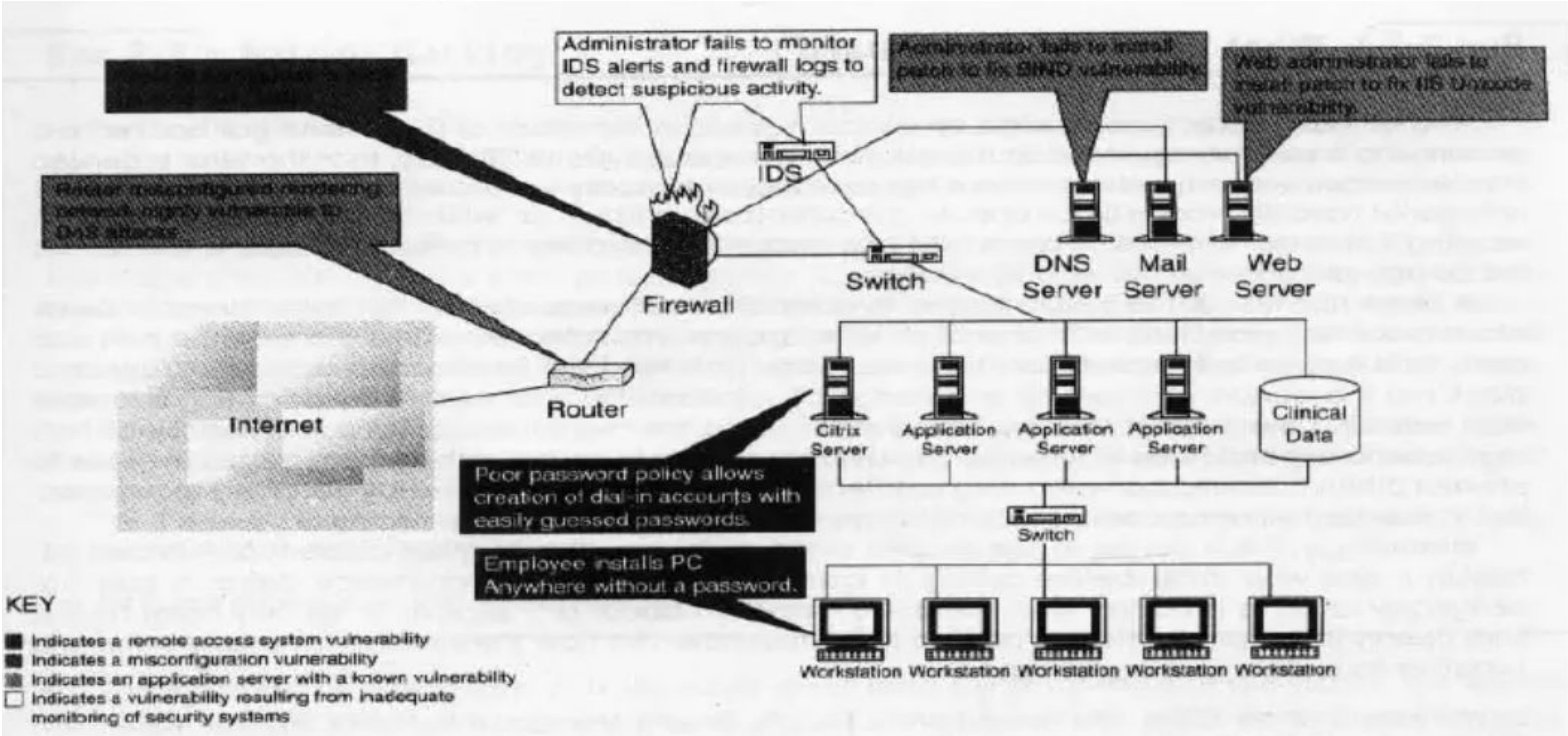
1. Inadequate border protection (border as in the sense of network periphery);

2. Remote access servers (RASs) with weak access controls;

3. Application servers with well-known exploits;

4. Misconfigured systems and systems with default configurations.

Introduction-Network Vulnerabilities-Sample network



Administrator fails to monitor IDS alerts and firewall logs to detect suspicious activity.

Administrator fails to install patch to fix BIND vulnerability.

Web administrator fails to install patch to fix IIS Unicode vulnerability.

Router misconfigured rendering network highly vulnerable to DoS attacks

Poor password policy allows creation of dial-in accounts with easily guessed passwords.

Employee installs PC Anywhere without a password.

KEY

- ■ Indicates a remote access system vulnerability
- ■ Indicates a misconfiguration vulnerability
- ▨ Indicates an application server with a known vulnerability
- □ Indicates a vulnerability resulting from inadequate monitoring of security systems

Terminologies

Hacker

Brute Force Hacking

Crackers

Cracking

Cracker tools

Phreaking

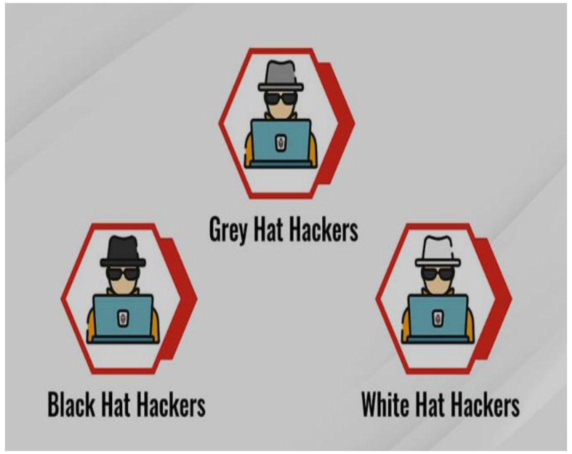
War dialer

Types of Hackers-----The Colour of Hat

- **White Hat Hackers** are the one who is authorized or the certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity.

- **Black Hat Hackers** can gain the unauthorized access of your system and destroy your vital data.

- **Gray Hat Hackers** fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. They work with both good and bad intentions; they can use their skills for personal gain. It all depends upon the hacker.



Other Hackers are:
->**Script Kiddies**
->**Green Hackers**
->**Blue Hackers**
->**Red Hackers**
->**Nation Funded Hackers**

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.

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

How Criminals Plan Their Attacks-Types

- Active attacks
- Passive attacks
- Inside attacks
- Outside attacks

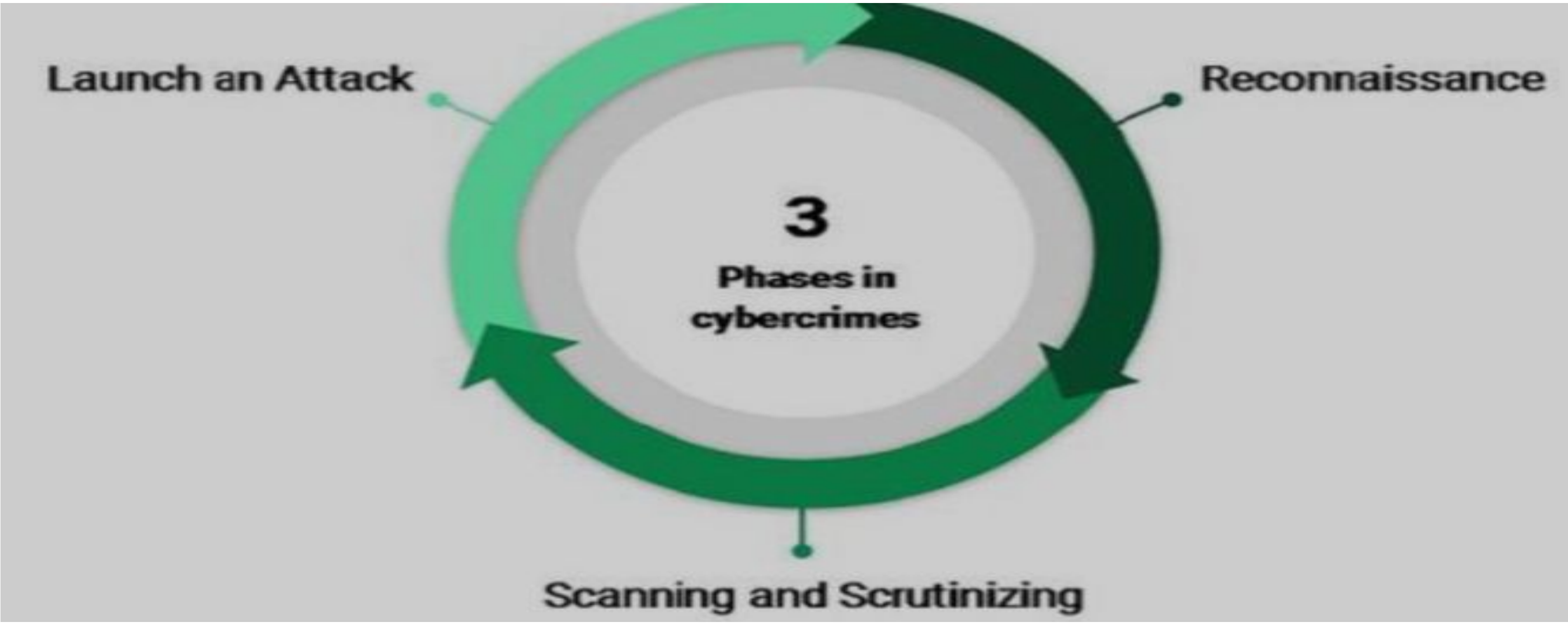
How Criminals Plan Their Attacks

Phases in Cybercrimes:

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).



How Criminals Plan Their Attacks

I. Reconnaissance

“Reconnaissance” is *an act of reconnoitering – explore, often with the goal of finding something or somebody.*

Reconnaissance begins with “*Foot Printing*” – 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.
- Organization’s website may provide personnel directory or information about key employees.
- Surfing online community groups like Facebook, insta etc…

Passive Attacks-Tools

Network Sniffing is another means of passive attack to yield useful information such as Internet Protocol(IP) address ranges, hidden servers or networks.

Google earth
It is a virtual globe, map and geographic information program.

http://earth.google.com/

Internet Archive:
It is an Internet library , with the purpose of offering permanent access for researches, historians and scholars.

It includes texts, audio, moving pages and software as well as archived webpages in our collections.

http://www.archive.org/index.php

Passive Attacks-Tools

Professional Community

Manage your professional identity. Build and engage with your professional network. Access knowledge, insights and opportunities.

http://www.linkedIn.com/

Passive Attacks-Tools

Domain Name Confirmation

The registered domain name can be found using .com, .net, .org, .edu and .biz etc

http://www.namedroppers.com/

http://www.binarypool.com/bytes.html

WHOIS

This is a domain registration lookup tool.

This utility is used for communicating with WHOIS servers located around the world to obtain domain registration information.

http://www.whois.com

Passive Attacks-Tools

Traceroute

- This tool is used to find the route to target system.
- It determines the route taken by packets across an IP network.

http://www.rjsmith.com/tracerte.com/

VisualRoute Trace:-

This is a graphical tool which determines where and how virtual traffic on the computer network is flowing between source and target destination.

http://www.visualware.com/

Passive Attacks-Tools

Nslookup(Name Server Lookup)

This tool is used on windows and Unix to query Domain Name System(DNS) servers to find DNS details, IP address, MX records.

http://nslookup.downloadsoftware4free.com/

Dnsstuff:-

Dnsstuff is used to extract information about IP addresses, mail server extensions, DNS lookup, WHOIS lookups etc.

http://www.dnsstuff.com/

Passive Attacks-Tools

emailTrackerPro

- It analyses the E-Mail header and provides the IP address of the system that sent the mail.

http://www.emailtrackerpro.com/

HTTrack

- This tool acts like an offline browser.
- It can mirror the entire website by being offline.

http://www.httrack.com/

How Criminals Plan Their Attacks

Active Attacks

- An active attack involves probing the network to discover individual hosts to confirm the information(IP address, OS type, services on network) 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.

How Criminals Plan Their 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;

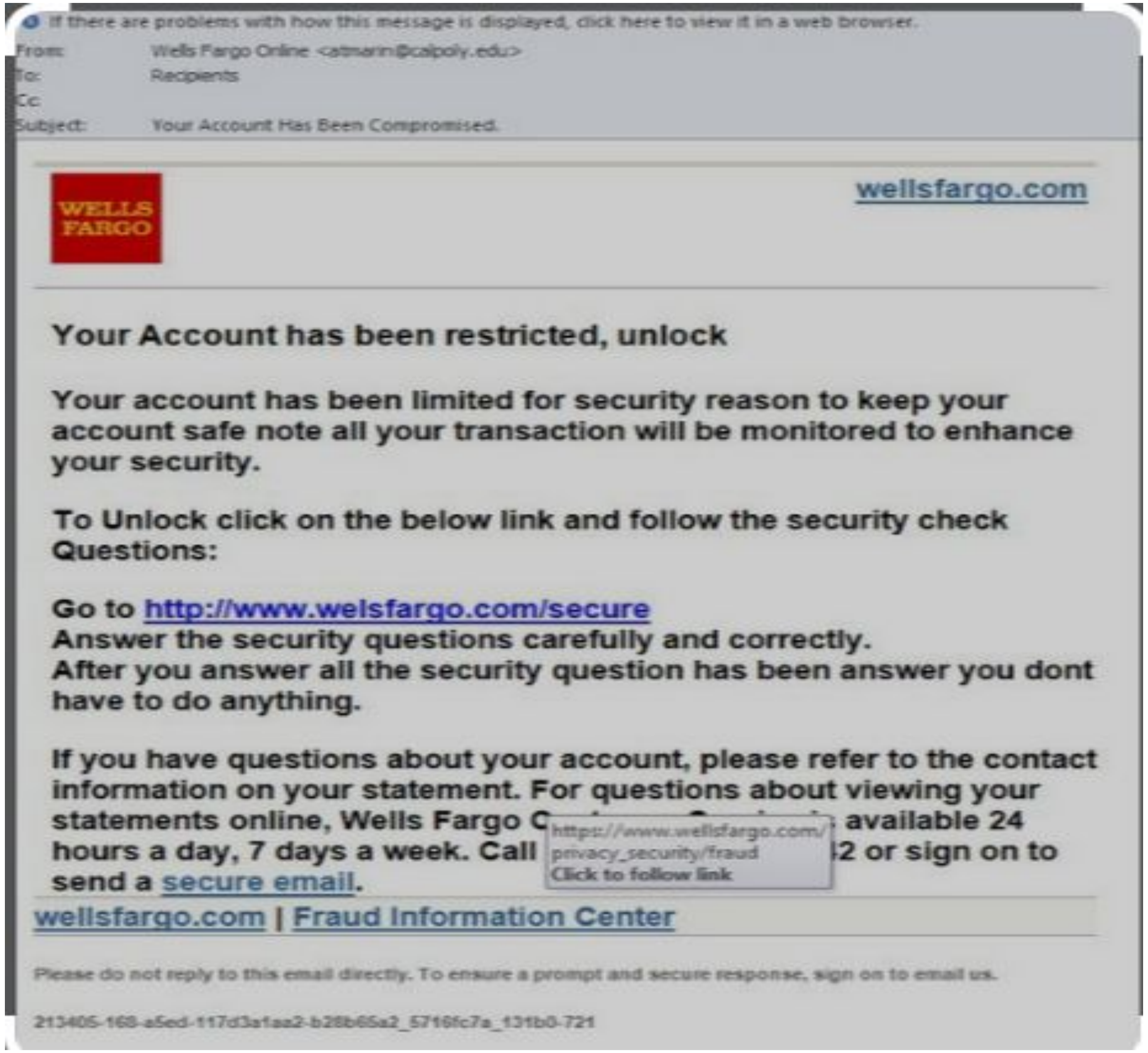
2. Exploit the privileges;

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.

Social Engineering



If there are problems with how this message is displayed, click here to view it in a web browser.

From: Wells Fargo Online <atmarin@calpoly.edu>
To: Recipients
Cc:
Subject: Your Account Has Been Compromised.

wellsfargo.com

Your Account has been restricted, unlock

Your account has been limited for security reason to keep your account safe note all your transaction will be monitored to enhance your security.

To Unlock click on the below link and follow the security check Questions:

Go to http://www.welsfargo.com/secure
Answer the security questions carefully and correctly.
After you answer all the security question has been answer you dont have to do anything.

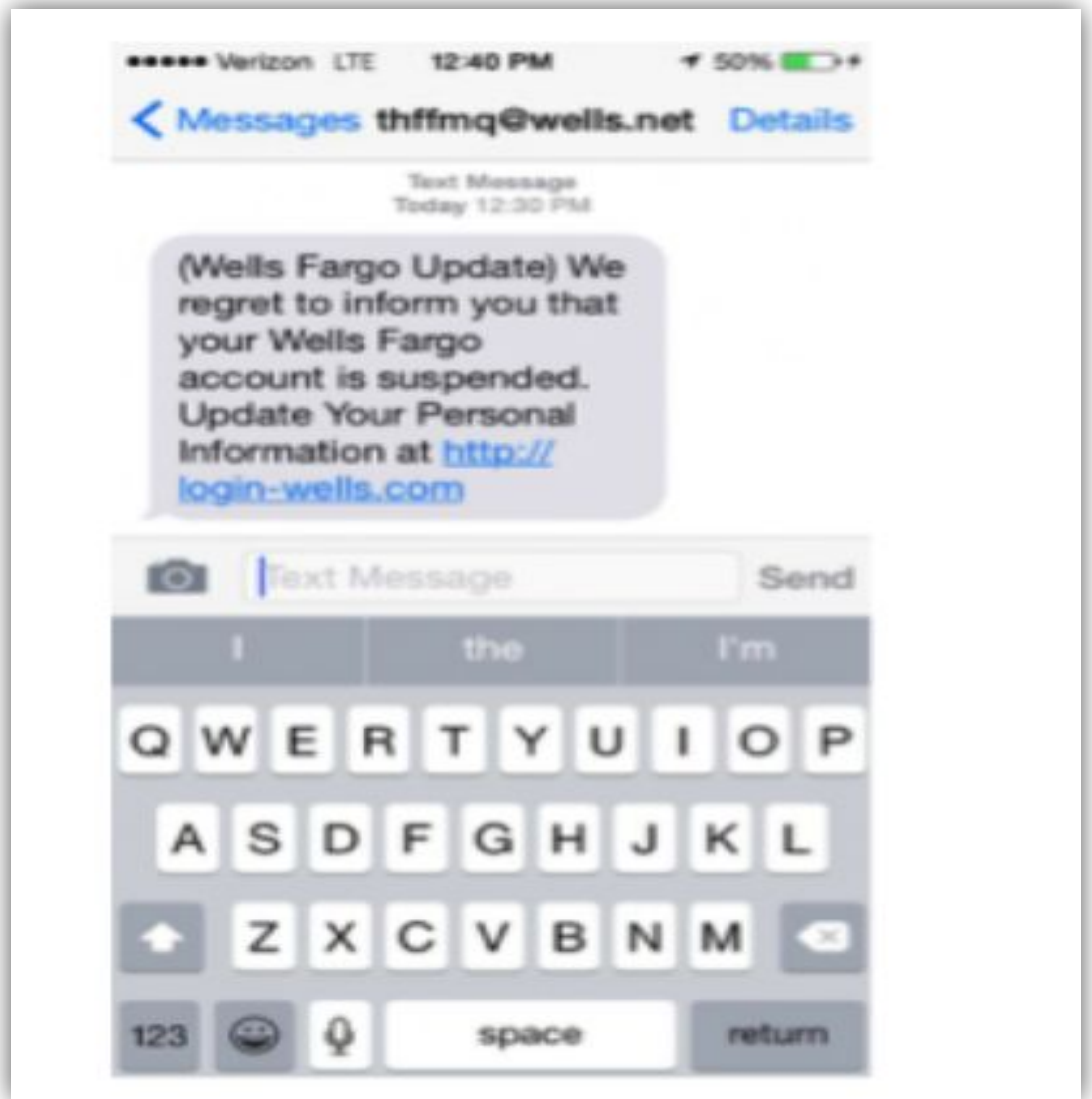
If you have questions about your account, please refer to the contact information on your statement. For questions about viewing your statements online, Wells Fargo C available 24 hours a day, 7 days a week. Call 2 or sign on to send a secure email.

https://www.wellsfargo.com/privacy_security/fraud
Click to follow link

wellsfargo.com | Fraud Information Center

Please do not reply to this email directly. To ensure a prompt and secure response, sign on to email us.

213405-168-a5ed-117d3a1aa2-b28b65a2_5716fc7a_131b0-721



thffmq@wells.net

Text Message
Today 12:30 PM

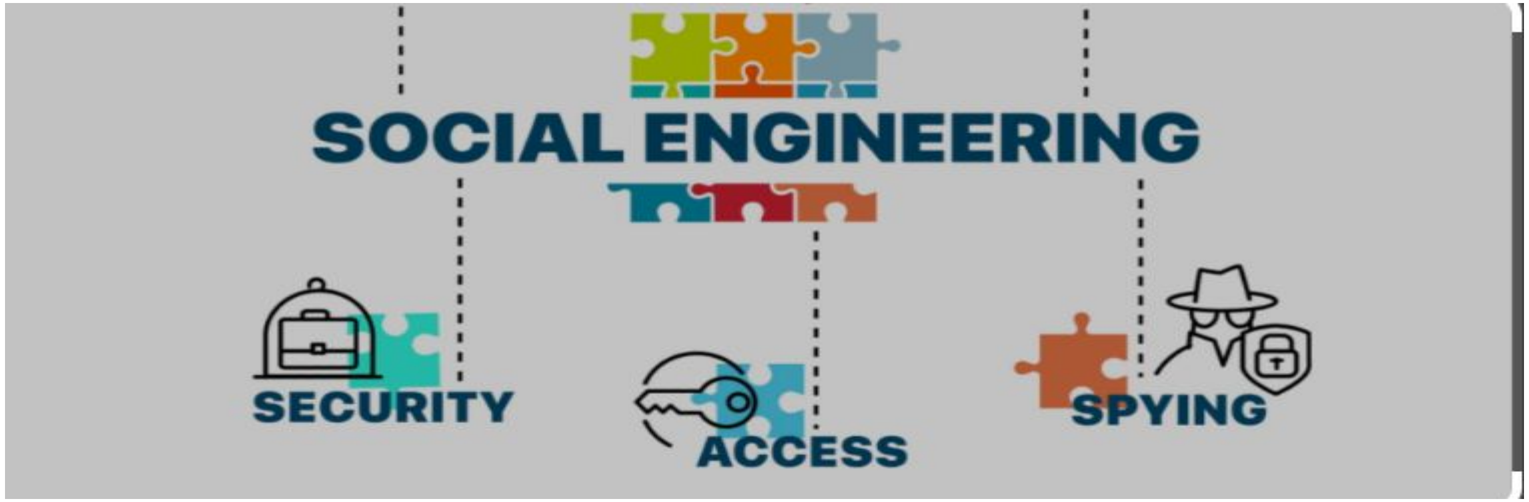
(Wells Fargo Update) We regret to inform you that your Wells Fargo account is suspended. Update Your Personal Information at http://login-wells.com

Social Engineering

“There is no patch for human stupidity.”

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.

Example:

1. Impersonating an employee or valid user
2. Posing an important user
3. Using a third person
4. Calling technical support
5. Shoulder surfing
6. Dumpster diving(people dumpster dive search items ,reclaim those….)

Classification of Social Engineering

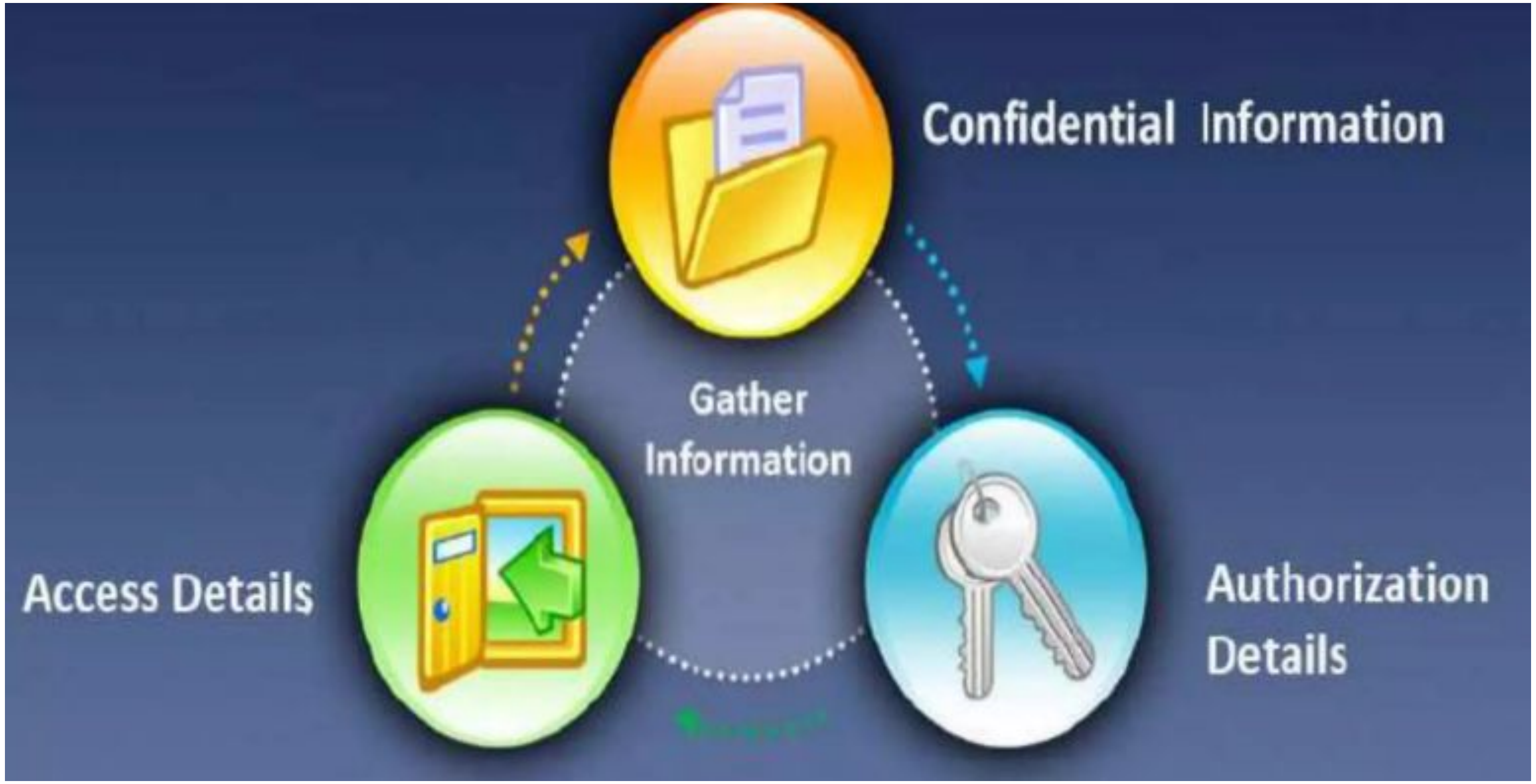
2. *Computer-Based Social Engineering*

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

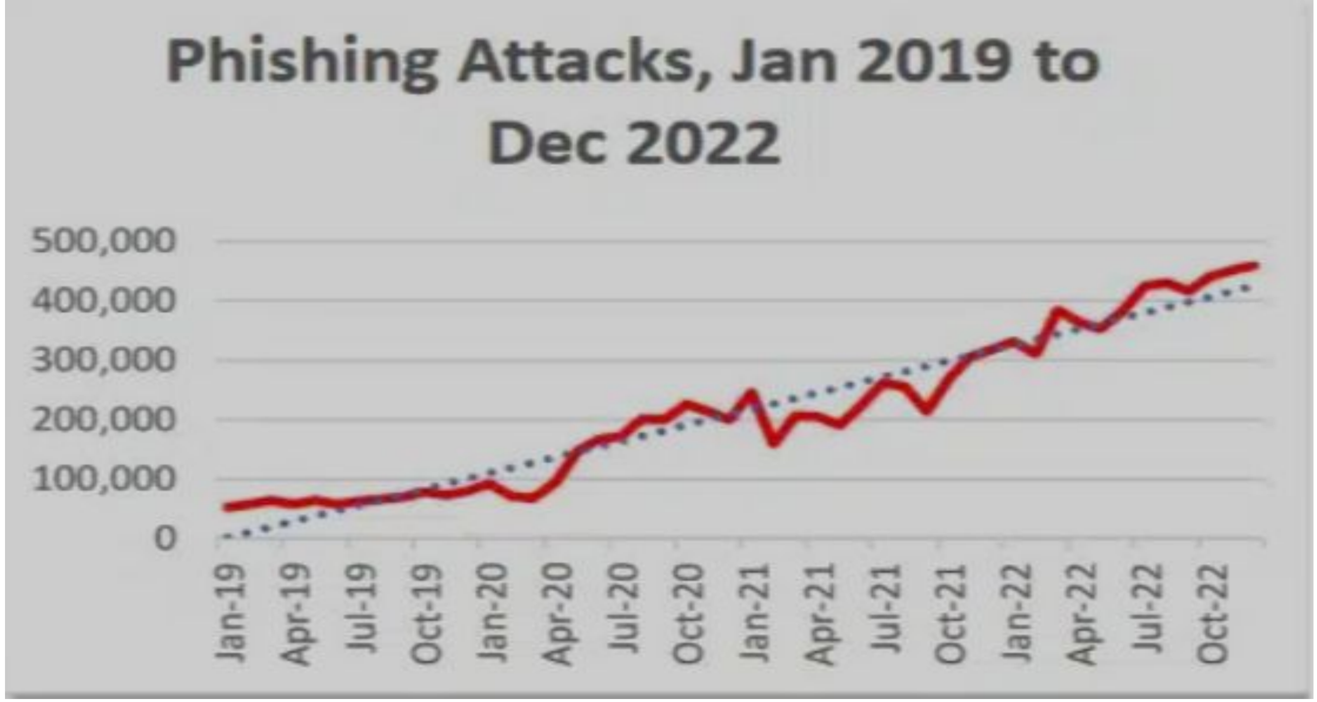
Example:

1. Fake E-mails
2. E-mail attachments
3. Pop-up windows

What they are Looking For?



Social Engineering-Phishing Statistics



Types of Social Engineering

Phishing: A scammer contacts victims posing as a reliable company or organization to collect sensitive data.

Spear phishing: A phishing scam that targets a specific individual within a company or organization.

Baiting: A scammer plants a digital storage device or link laced with malware where the target will find it.

Tailgating: An attacker gains physical access to a restricted area by posing as a trusted individual.

Social Engineering-How it is done?

- Attacks come in various forms:
  - On the phone, over e-mail, in person impersonation

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, cyber stalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

Types of Stalkers

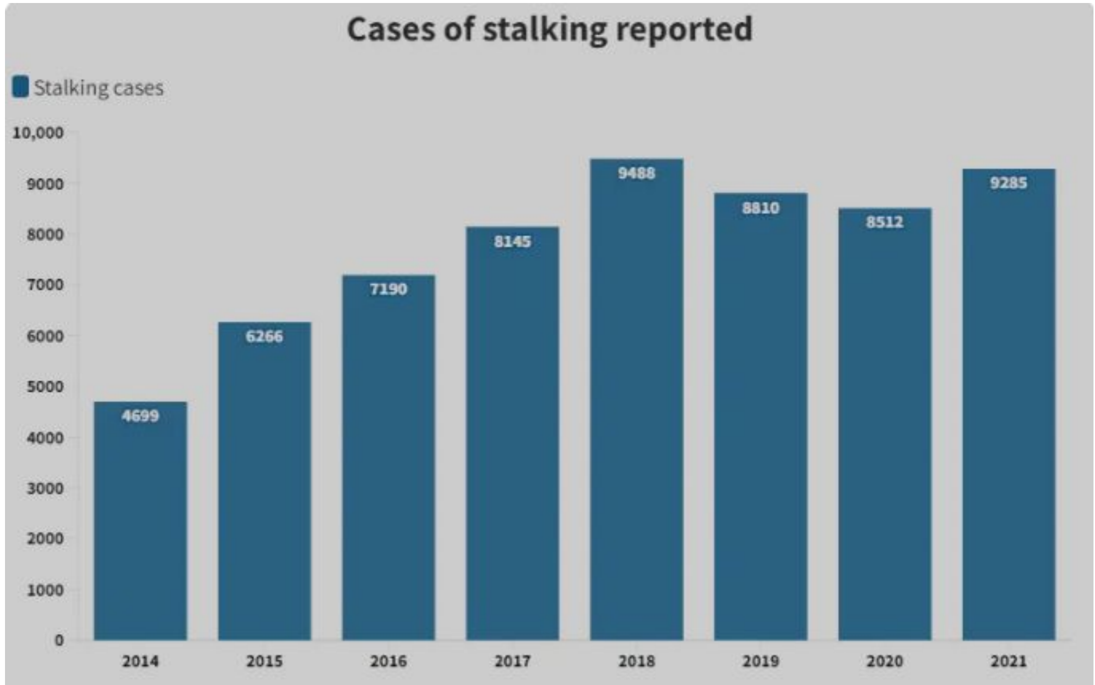
Online Stalkers:

They interact with victim directly through Internet. Email and Chat rooms are most popular communication medium.

Offline Stalkers:

The stalker may observe daily routine of victim, Searching on message boards/newsgroups, personal websites.

Cases Reported on Stalking



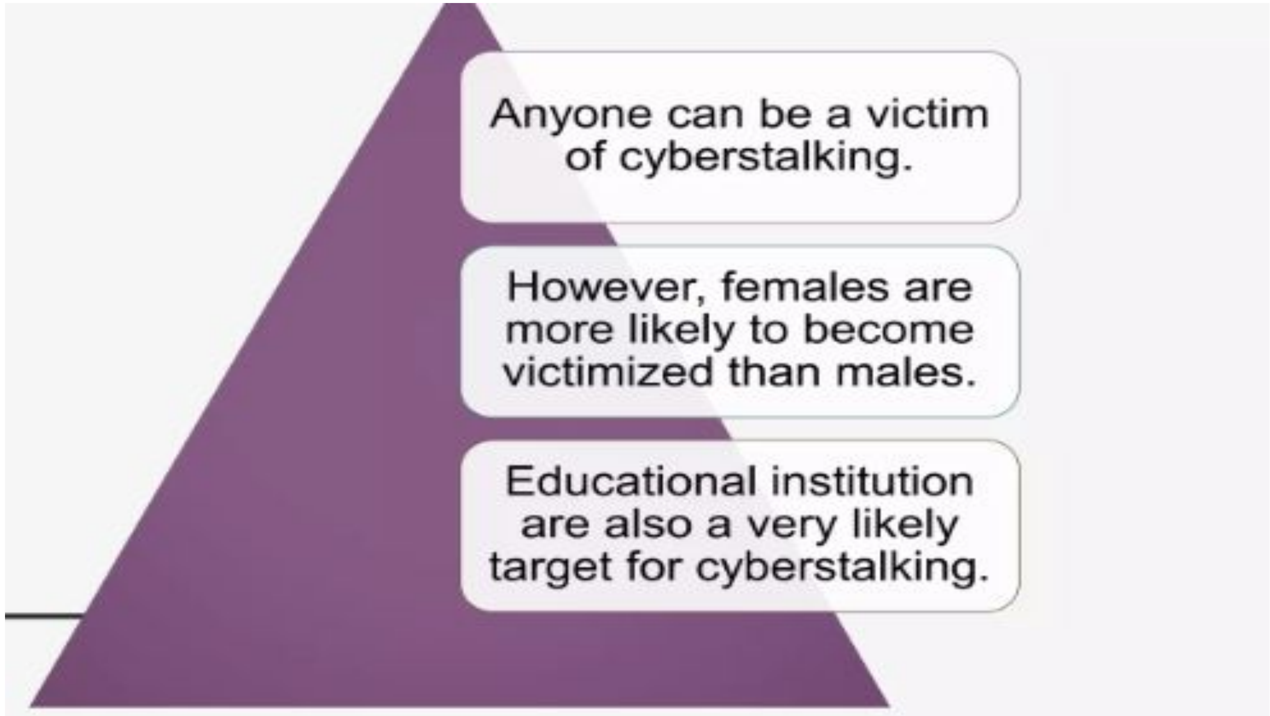
75 to 80% of stalkers are men stalking women.

I am a woman, My stalker is a woman,
How weird is that?

How Stalking Works??

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 services 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.

Cyber Stalking-Who are the Victims

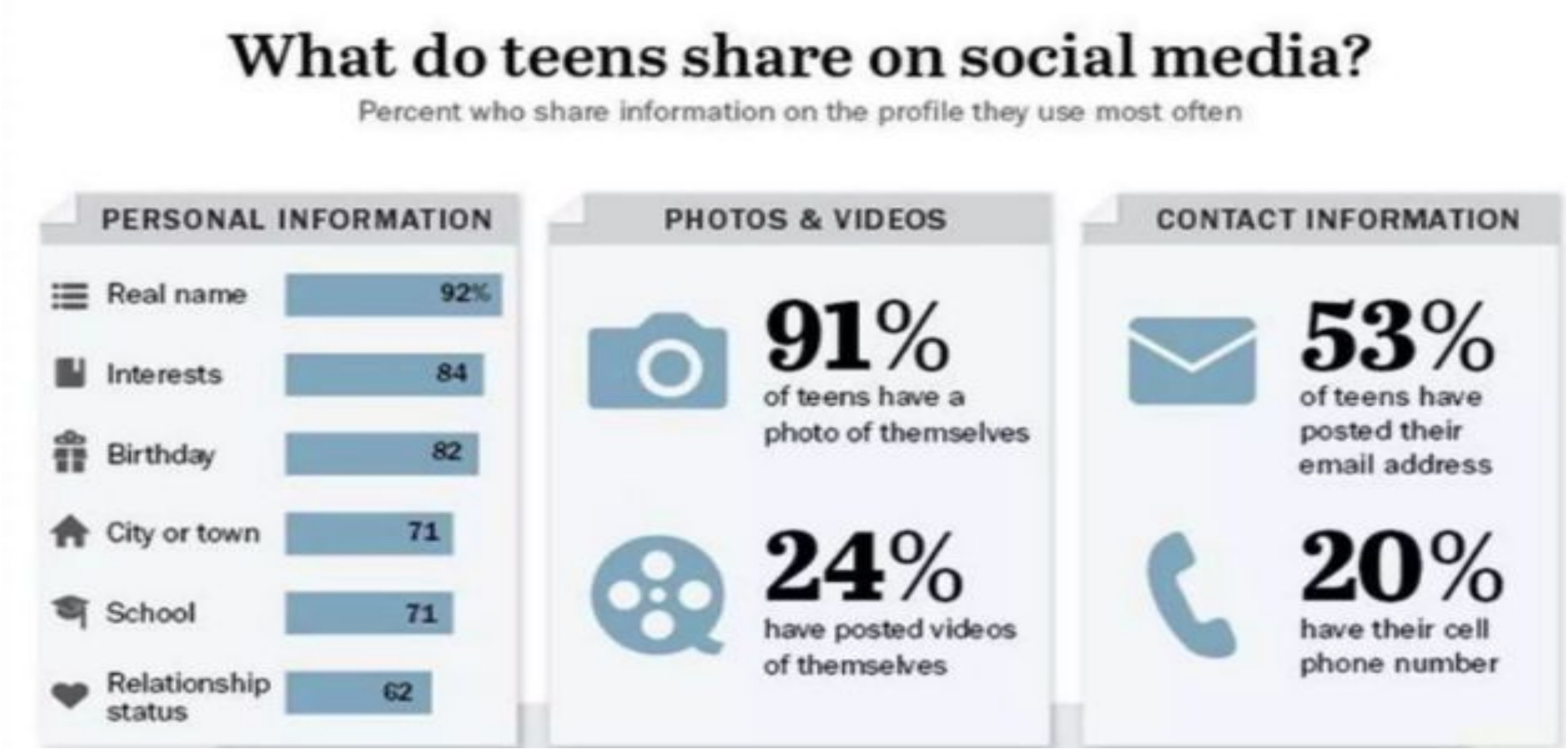


Anyone can be a victim of cyberstalking.

However, females are more likely to become victimized than males.

Educational institution are also a very likely target for cyberstalking.

Cyber Stalking-What do they share



What do teens share on social media?

Percent who share information on the profile they use most often

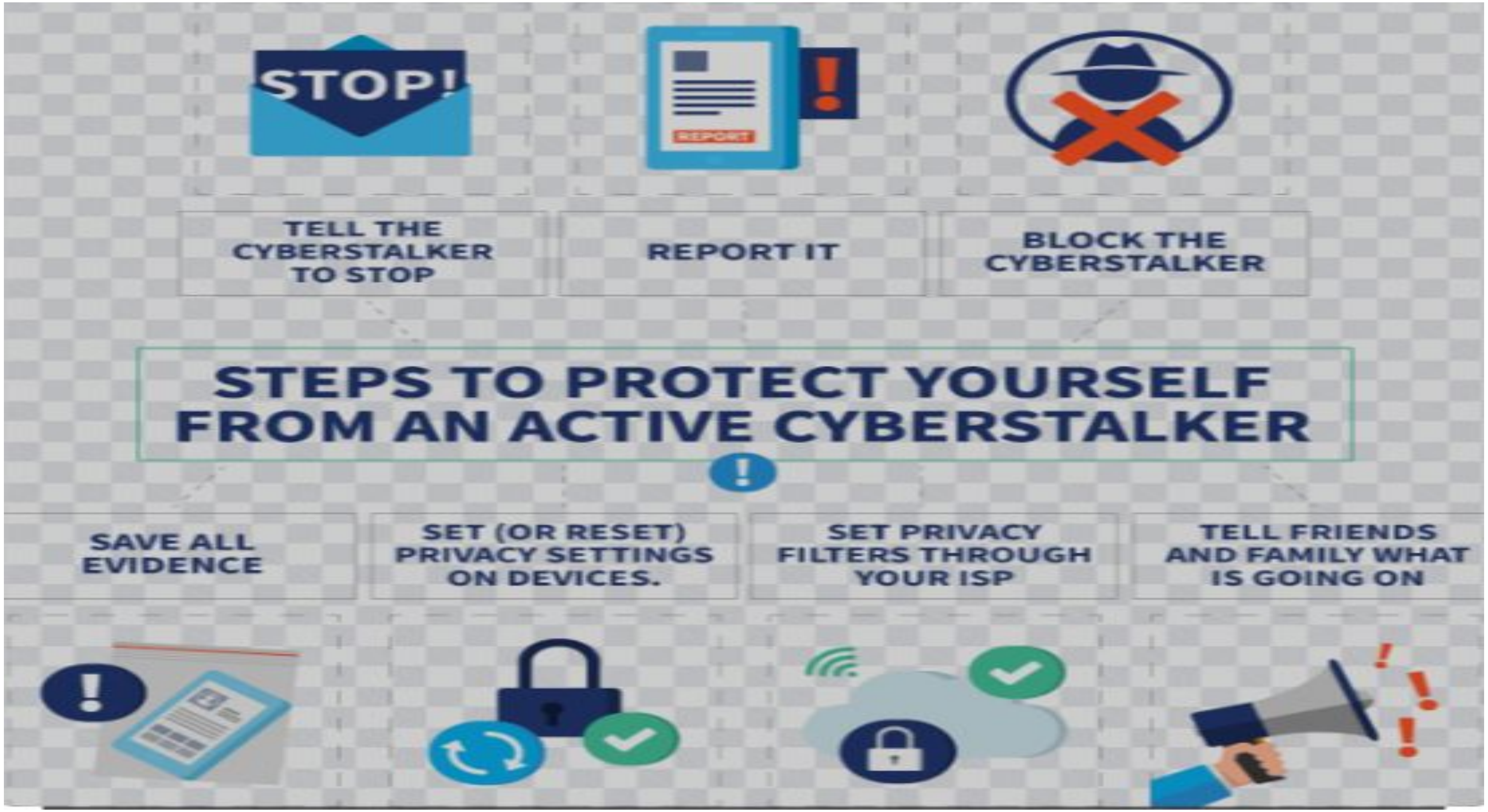
91% of teens have a photo of themselves

24% have posted videos of themselves

53% of teens have posted their email address

20% have their cell phone number

Cyber Stalking-How to protect from stalking



STEPS TO PROTECT YOURSELF FROM AN ACTIVE CYBERSTALKER

TELL THE CYBERSTALKER TO STOP

REPORT IT

BLOCK THE CYBERSTALKER

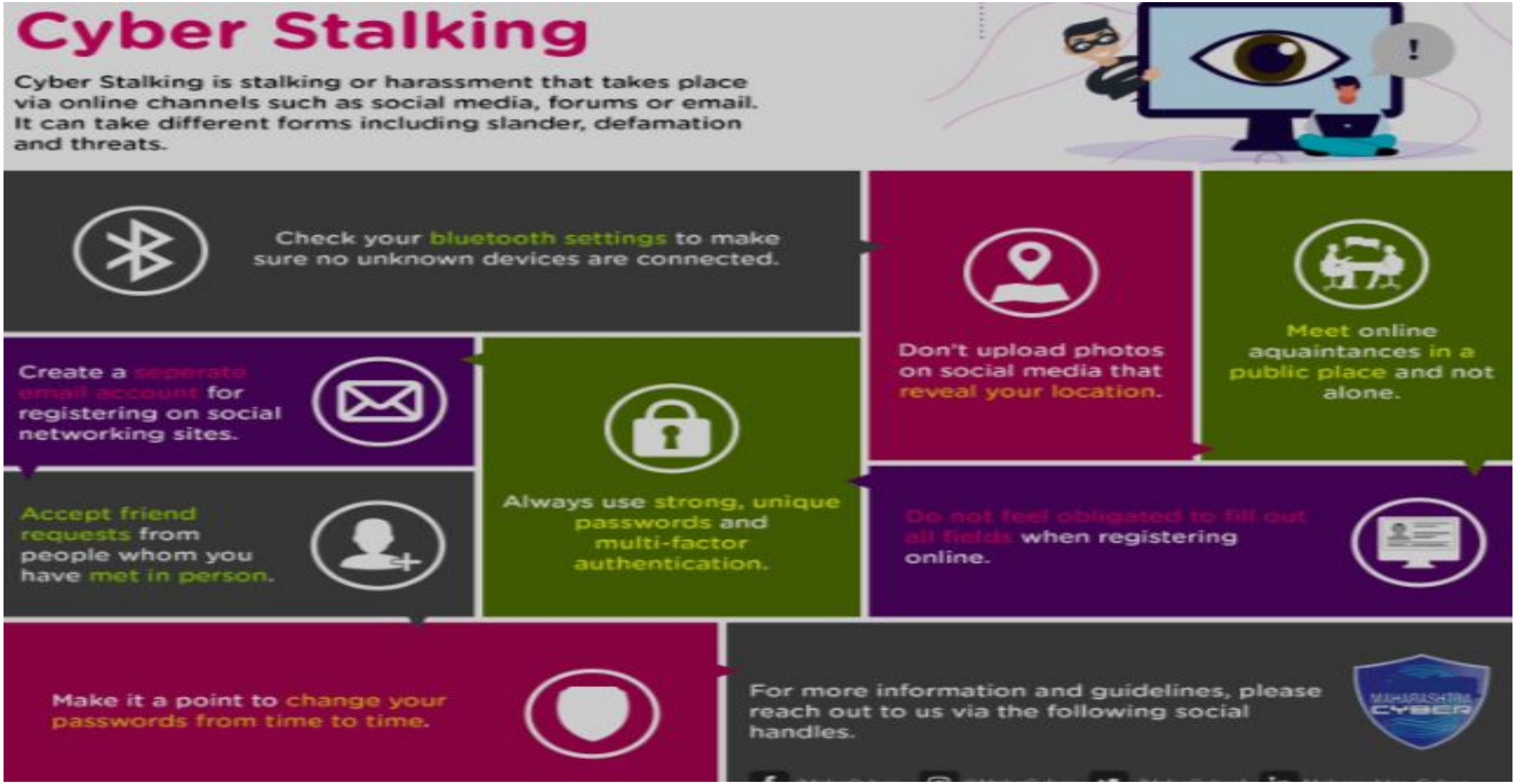
SAVE ALL EVIDENCE

SET (OR RESET) PRIVACY SETTINGS ON DEVICES.

SET PRIVACY FILTERS THROUGH YOUR ISP

TELL FRIENDS AND FAMILY WHAT IS GOING ON

Cyber Stalking-How to safeguard from it



Cyber Stalking

Cyber Stalking is stalking or harassment that takes place via online channels such as social media, forums or email. It can take different forms including slander, defamation and threats.

Check your bluetooth settings to make sure no unknown devices are connected.

Don't upload photos on social media that reveal your location.

Meet online aquaintances in a public place and not alone.

Create a seperate email account for registering on social networking sites.

Always use strong, unique passwords and multi-factor authentication.

Accept friend requests from people whom you have met in person.

Do not feel obligated to fill out all fields when registering online.

Make it a point to change your passwords from time to time.

For more information and guidelines, please reach out to us via the following social handles.

Cybercafe and Cybercrimes

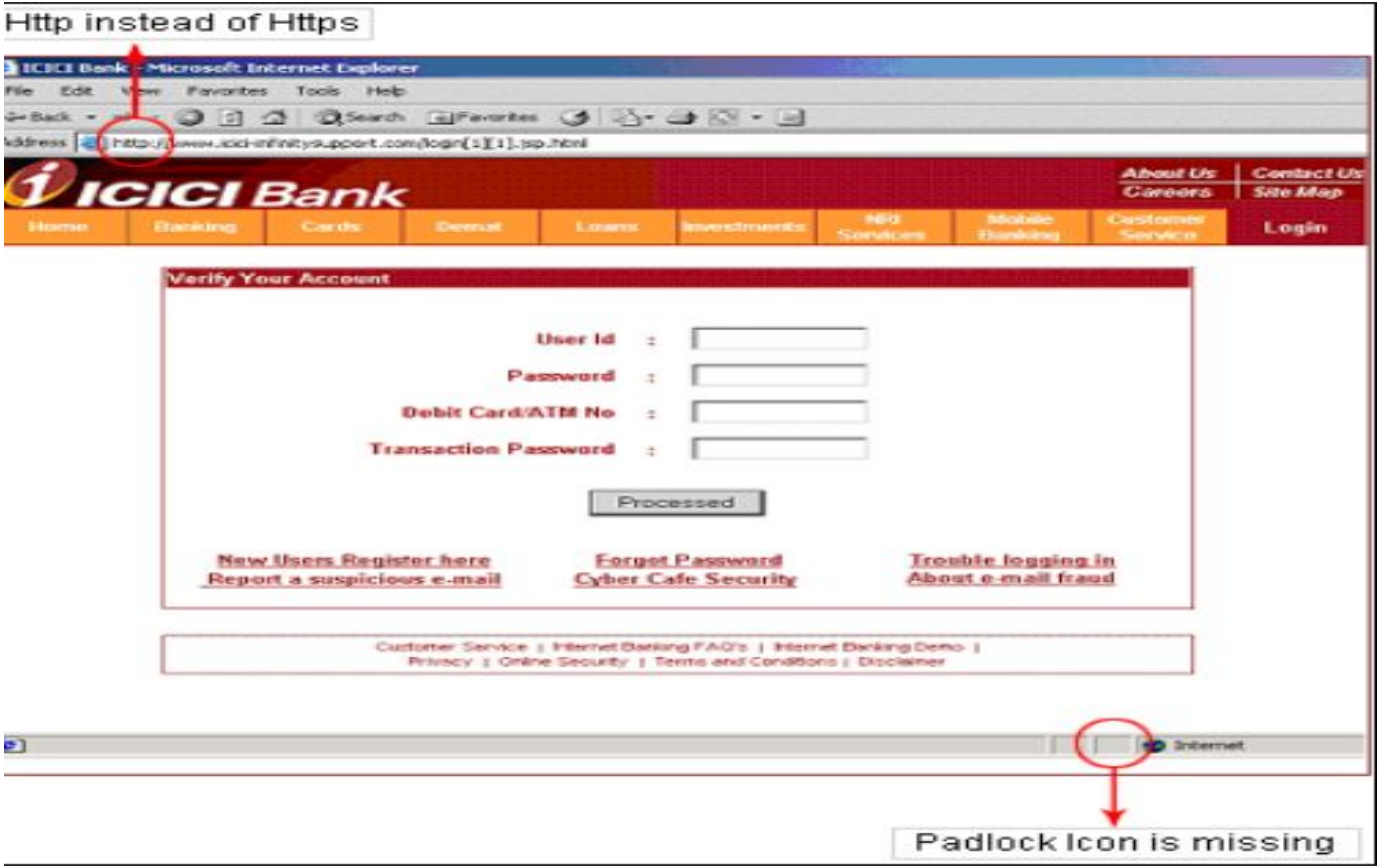
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.

- 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”.

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

Cybercafe and Cybercrimes



Http instead of Https

ICICI Bank - Microsoft Internet Explorer

Address http://www.icici-infinitysupport.com/login[1][1].jsp.html

Verify Your Account

User Id :

Password :

Debit Card/ATM No :

Transaction Password :

Processed

Padlock Icon is missing

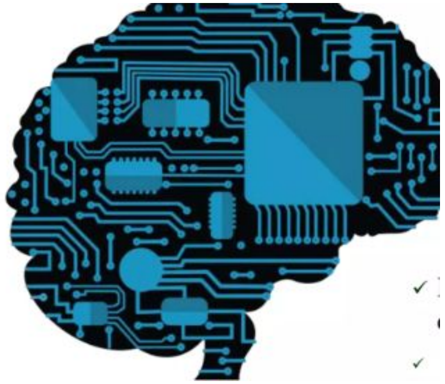
Cybercafe and Cybercrimes

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

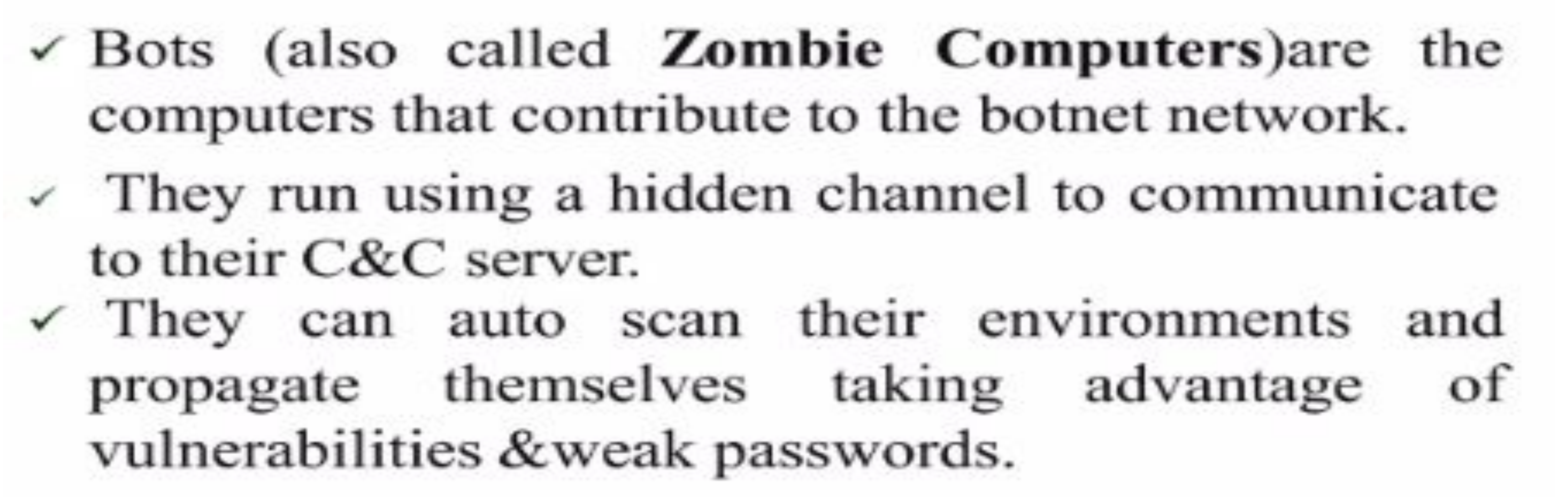
1. Always logout
2. Stay with the computer
3. Clear history and temporary files
4. Be alert
5. Avoid online Financial transactions
6. Change passwords
7. Virtual keyboard
8. Security warnings

Botnets

- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- Your computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.

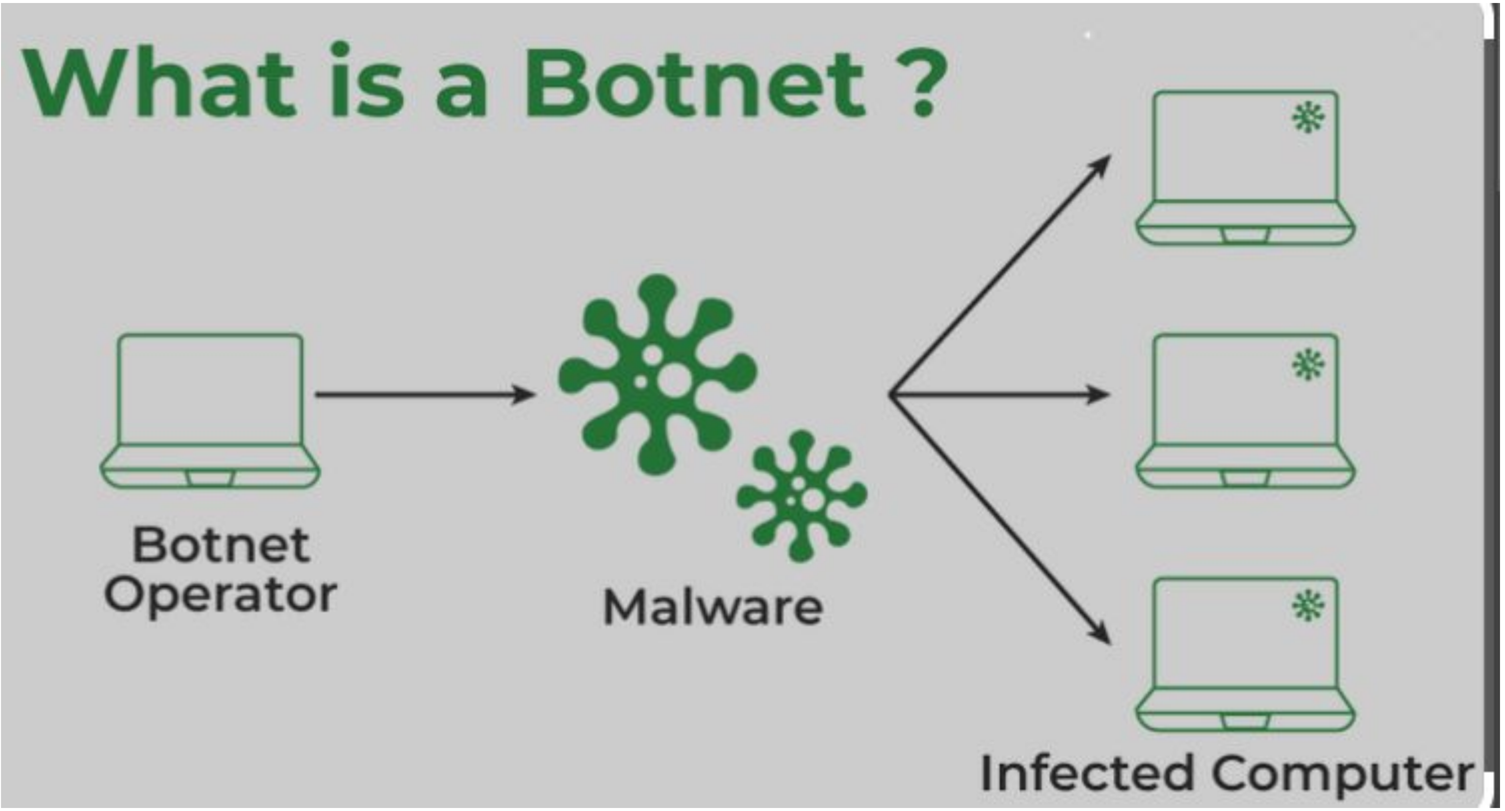


Botnets

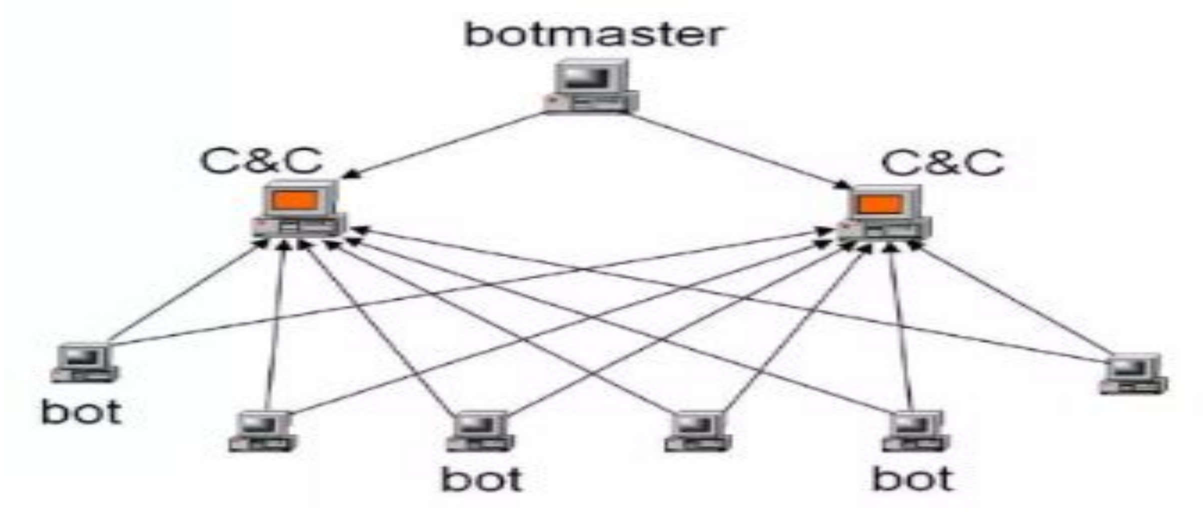


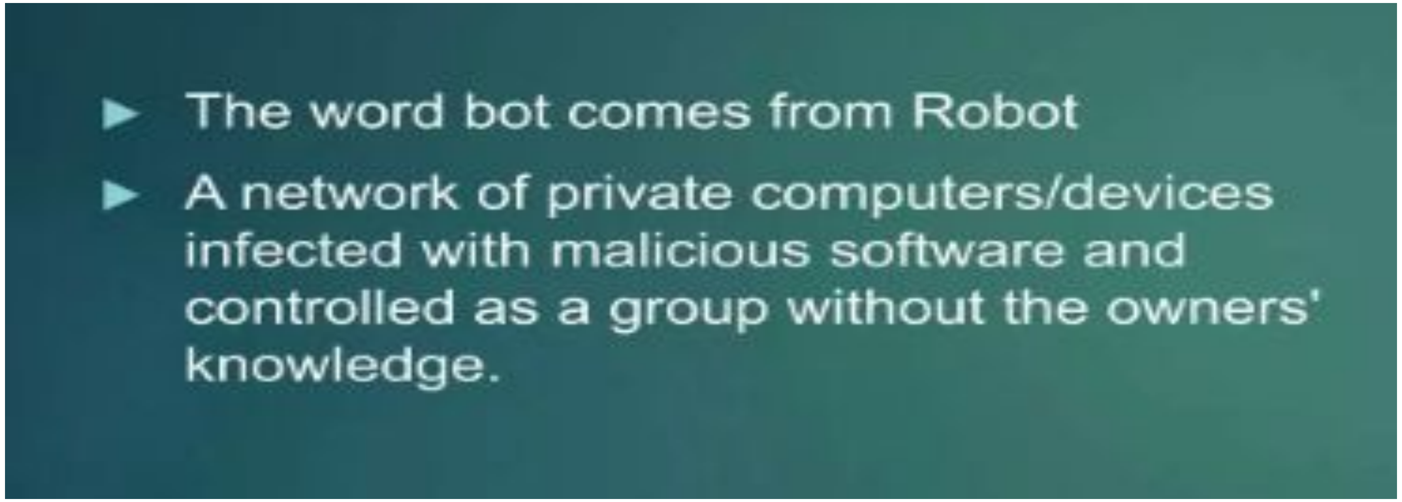
- ✓ Bots (also called **Zombie Computers**)are the computers that contribute to the botnet network.
- ✓ They run using a hidden channel to communicate to their C&C server.
- ✓ They can auto scan their environments and propagate themselves taking advantage of vulnerabilities &weak passwords.

Botnet


What is a Botnet ?
Botnet Operator
Malware
Infected Computer

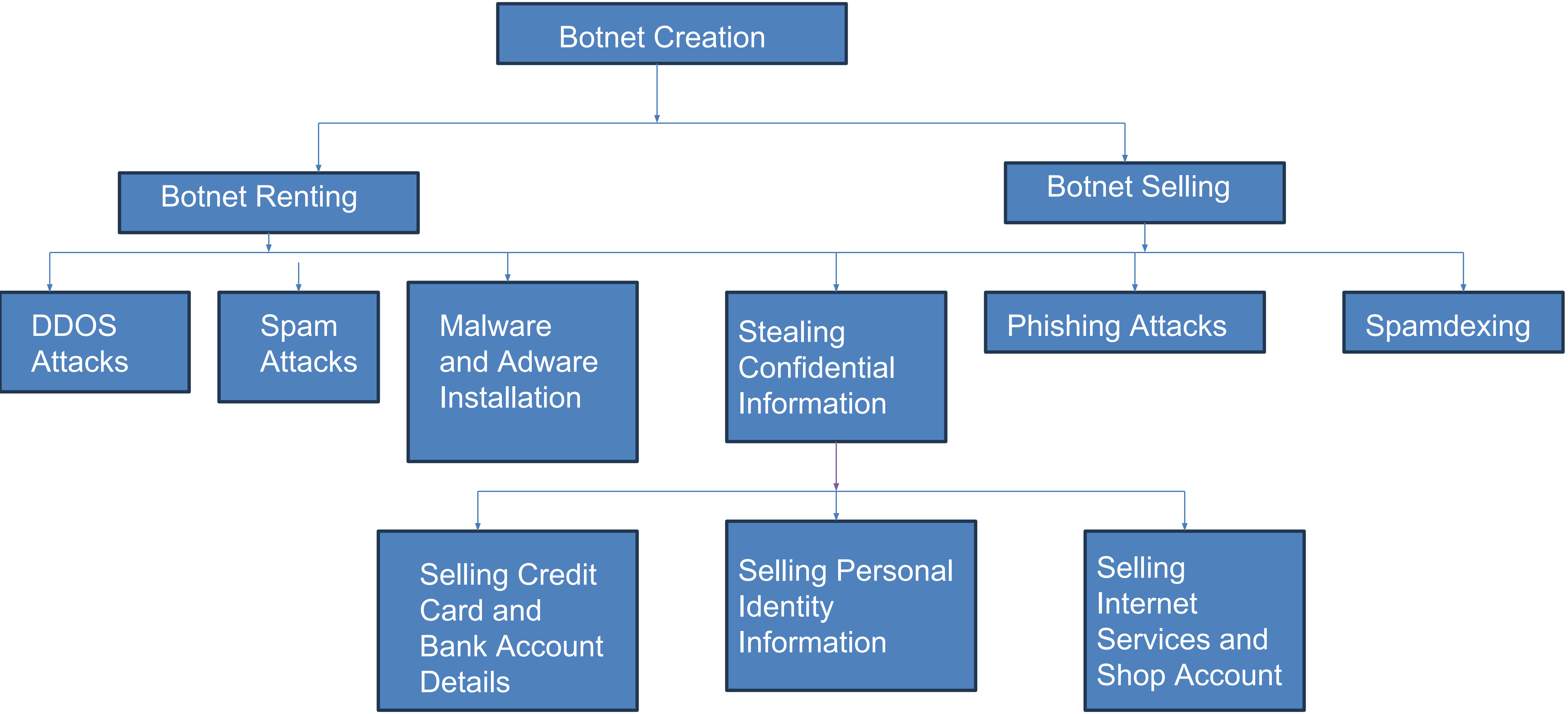
Botnet





- The word bot comes from Robot
- A network of private computers/devices infected with malicious software and controlled as a group without the owners' knowledge.

Botnet



Botnet Creation

Botnet Renting

Botnet Selling

DDOS Attacks

Spam Attacks

Malware and Adware Installation

Stealing Confidential Information

Phishing Attacks

Spamdexing

Selling Credit Card and Bank Account Details

Selling Personal Identity Information

Selling Internet Services and Shop Account

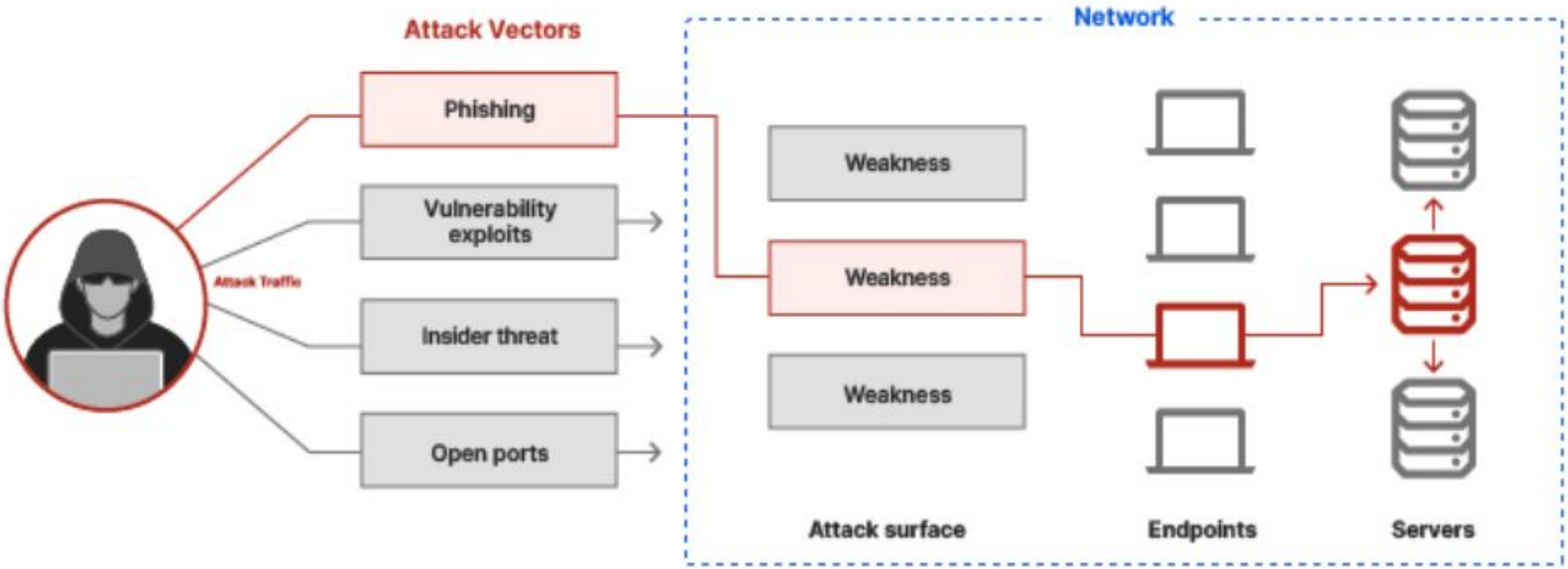
Secure the System from Botnets

1. Use antivirus and anti-Spyware software and keep it up-to-date.
2. Set the OS to download and install security patches automatically.
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet.
4. Disconnect from the Internet when you are away from your computer.
5. Downloading the freeware only from websites that are known and trustworthy
6. Check regularly the folders in the mail box – “sent items” or “outgoing” – for those messages you did not send.
7. Take an immediate action if your system is infected.

Attack Vector

- An “attack vector” is a path or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception.
- The most common malicious payloads are viruses, 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.
  - ✔ Payload means the malicious activity that the attack performs.
  - ✔ It is the bits that get delivered to the end-user at the destination.

Attack Vector



Attack Vectors

- Attack by E-mail
- Attachments(and other files)
- Attack by deception
- Hackers
- Heedless guests(Attack by Webpage)
- Attack of the worms
- Malicious macros
- Foist ware
- Viruses