
CYBER
SECURITY

Objectives

To understand

- Definition of Cyber Crime
- Classification of Cyber crimes
- Computer Intrusions and Hacking
- Computer Security

Cyber Crime

- **Cybercrime** also known as **Computer crime**, refers to any crime that involves a computer/mobile and a network.
- The computer may have been used in the commission of a crime, or it may be the target.
- **Netcrime** is criminal exploitation of the internet.
- Experts defined Cybercrime as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".
- Such crimes may threaten a nation’s security and financial health.

Cyber Crime

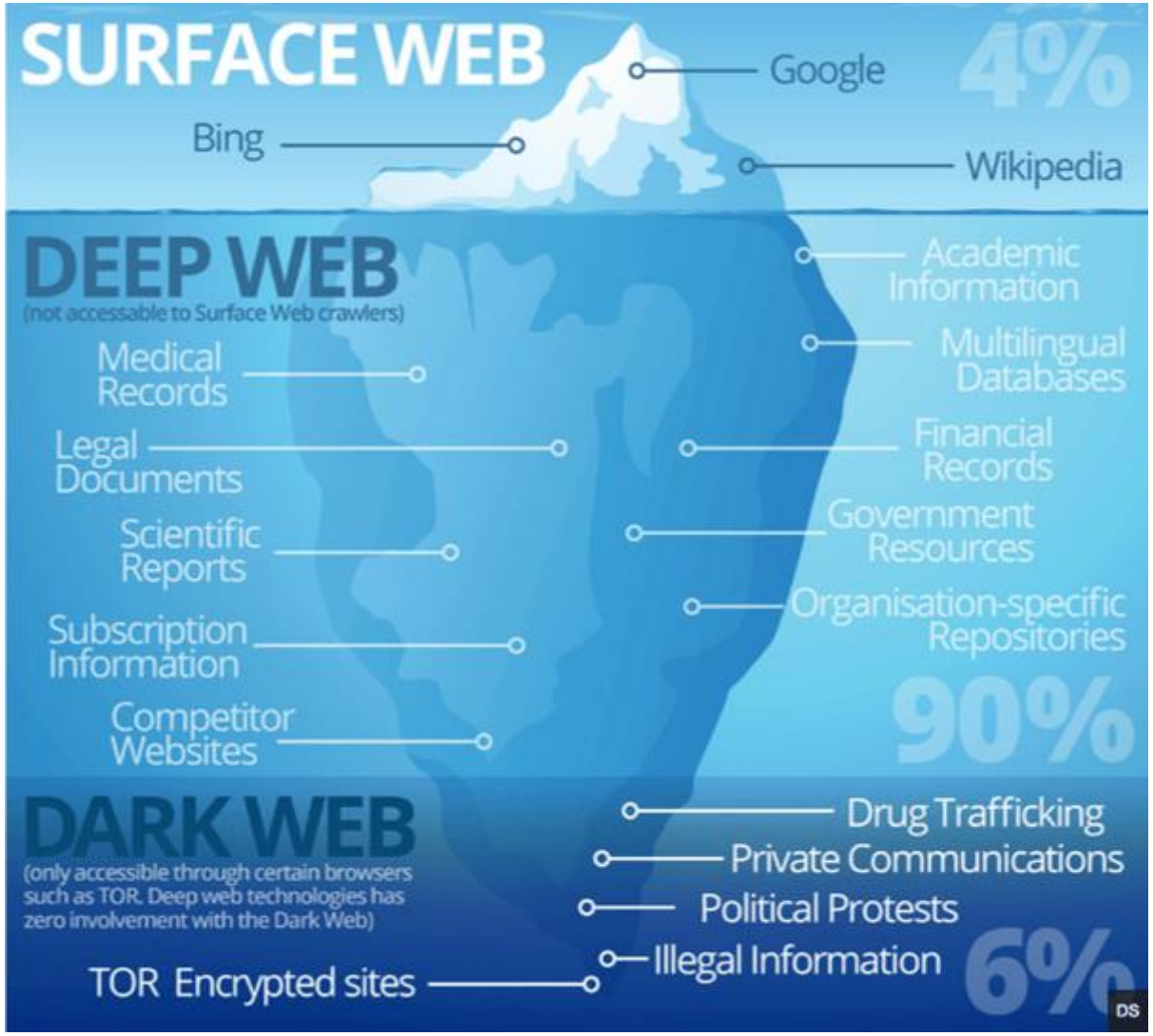
A simple yet sturdy definition of cyber crime would be

"unlawful acts wherein the computer is either a tool or a target or both".

Biggest Cyber Attacks 2017

1. Equifax Data Breach – 145.5 Million Accounts
2. Uber Data Breach – 57 Million Records
3. WannaCry Cyber Attack – 300,000 Systems
4. Yahoo! Makes History, Again – 3 Billion Accounts
5. Deep Root Analytics Data Breach – 198 Million U.S. Voters
6. Rasputin Attacks – 60 Universities and Federal Agencies

Surface Web vs Deep Web vs Dark Web



Surface Web vs Deep Web vs Dark Web

Dark Web vs Deep Web vs Surface Web	
Darknet/Dark Web	Restricted to special browsers Not indexed for Search Engines Large scale illegal activity Unmeasurable due to nature
Deep Web	Accessible by password, encryption, or through gateway software Not indexed for Search Engines Little illegal activity outside of Dark Web Huge in size and growing exponentially
Surface Web	Accessible Indexed for Search Engines Little illegal activity Relatively small in size

Cost of Information in Dark Web

- **Bank credential:** $1,000 plus (6% of the total dollar amount in the account)
- **U.S. credit card with track data (account number, expiration date, name and more):** $12
- **EU, Asia credit card with track data:** $28
- **Hacking into a website:** $100 to $300
- **Counterfeit social security cards:** $250 and $400
- **Counterfeit driver's license:** $100 to $150

Classification of Cyber Crimes

- Threatening email, assuming someone's identity, defamation, SPAM and Phishing are some examples where computers are used to commit crime.

- Where as viruses, worms and industrial espionage, software piracy and hacking are examples where computers become target of crime.

Classification of Cyber Crimes

Where computers are used to commit crime

- This category includes traditional offenses such as fraud committed through the use of a computer.
- Some examples are:

1. Financial Crime
2. Online Gambling
3. Intellectual Property Crimes
4. Email spoofing
5. Cyber defamation
6. Cyber stalking

1. Financial crimes

- This would include cheating, credit card frauds, money laundering etc.

2. Online gambling

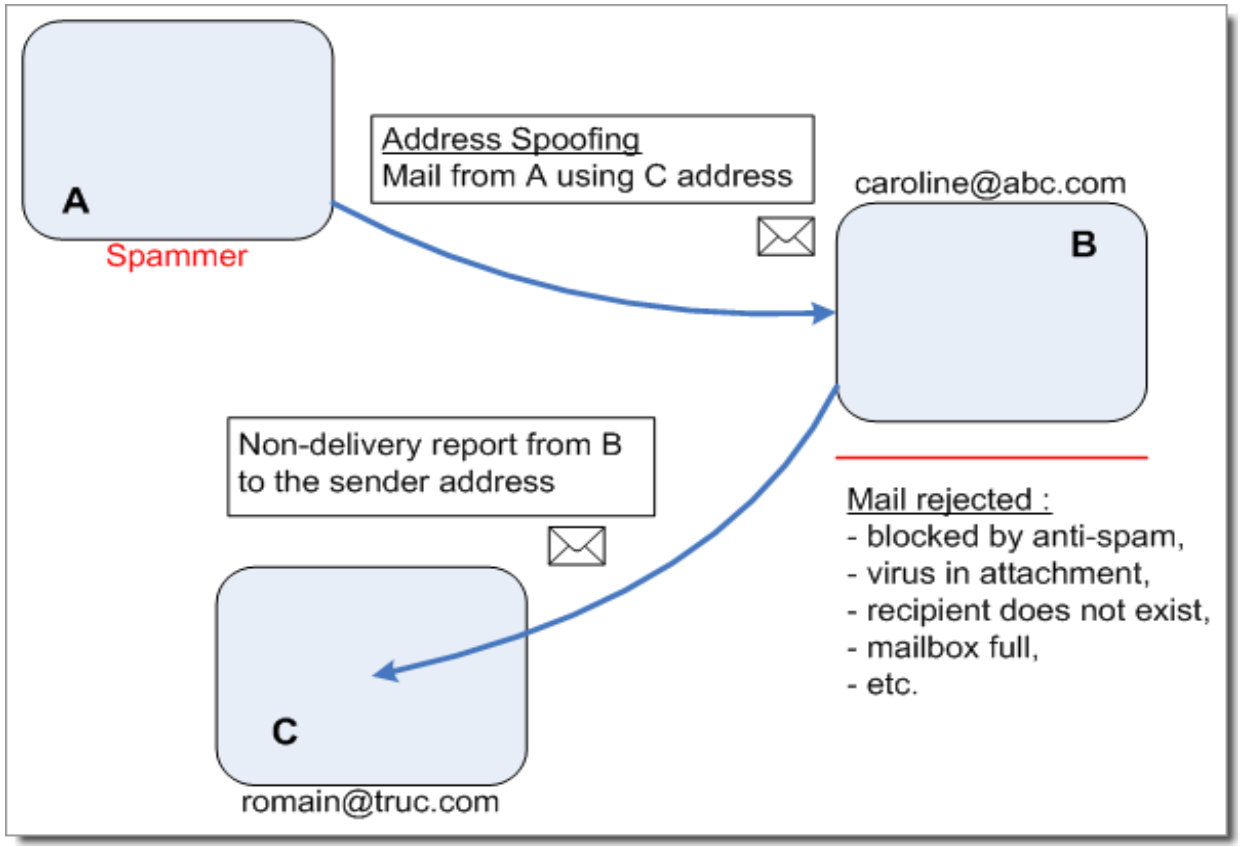
- There are millions of websites; all hosted on servers abroad, that offer online gambling.
- In fact, it is believed that many of these websites are actually fronts for money laundering.

3. Intellectual Property crimes

- These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

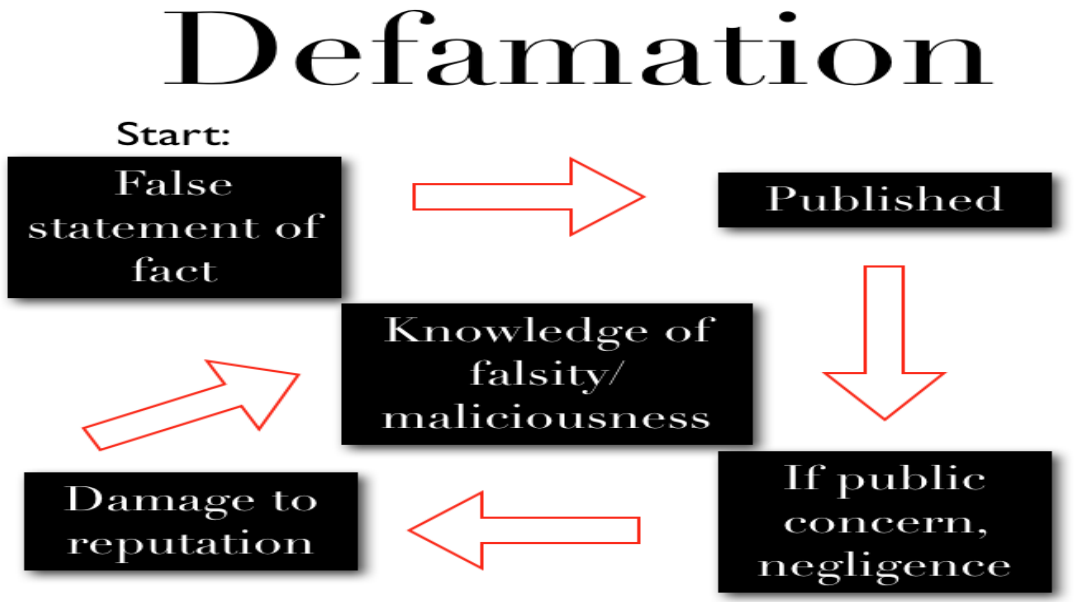
4. Email spoofing

- A spoofed email is one that appears to originate from one source but actually has been sent from another source.



5. Cyber Defamation

- This occurs when defamation takes place with the help of computers and / or the Internet.
- Example: Someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's contacts.



6. Cyber stalking

- Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly

  bombarding the victim with emails etc.

Classification of Cyber Crimes

Where computers become target of crime

- This category includes computer oriented cyber crimes.

- Some types are:

A. Unauthorized Access(Hacking)
B. Malicious Software(Viruses, Trojans- corrupts server)
C. Worm (Self-replicating programs)
D. Spyware – parasitic software, invades privacy,
E. Divulging details through tracking cookies.
F. Cyber terrorism

A. Unauthorized Access

- Also known as Hacking.

- Involves gaining access illegally to a computer system or network and in some cases making unauthorized use of this access.

- Hacking is also the act by which other forms of cyber-crime (e.g., fraud, terrorism) are committed.

A. Theft of information

- Theft of any information contained in electronic form such as that stored in computer hard disks, removal storage media, etc.

- Can extend to identity theft.

A. Email Bombing

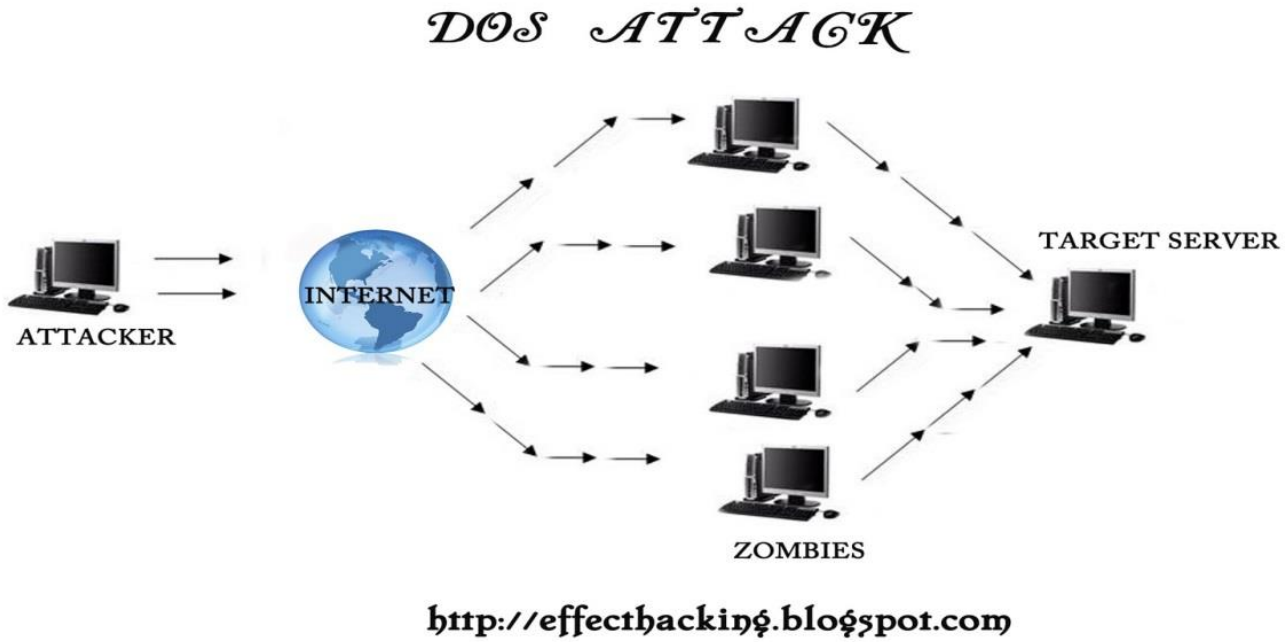
- This refers to sending large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

A. Salami Attacks

- These attacks are often used in committing financial crime and are based on the idea that an alteration, so insignificant, would go completely unnoticed in a single case.
- E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say 5 cents a month) from the account of every customer. This unauthorized debt is likely to go unnoticed by an account holder.

A. Denial of Service (DoS) Attack

- This involves flooding a computer resource with more requests than it can handle, causing the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.



B. Virus

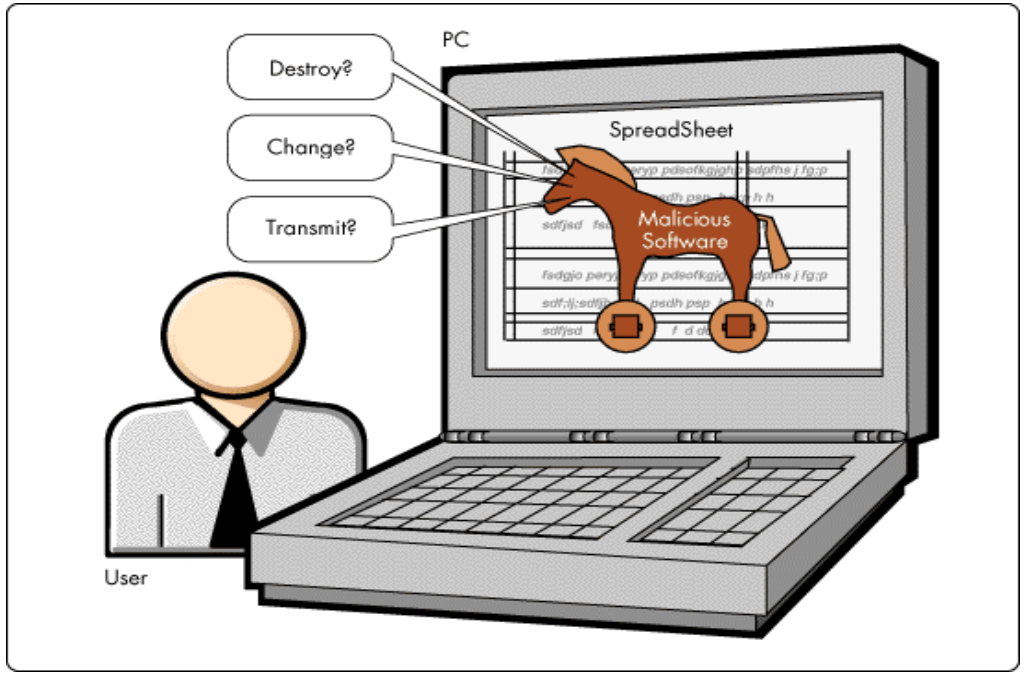
- Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it.

B. Logic Bombs

- These are event dependent programs where programs kick into action only when a certain event (known as a trigger event) occurs.
- Some viruses may be termed logic bombs because they lie dormant throughout the year and become active only on a particular date (e.g. Chernobyl virus).

B. Trojan Attacks

- An unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.



C. Worm

- Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

D. Web Jacking

- This occurs when someone forcefully takes control of a website (by cracking the password and later changing it).

E. Cyber-Terrorism

- Hacking designed to cause terror. Like conventional terrorism, `e-terrorism' utilizes hacking to cause violence against persons or property, or at least cause enough harm to generate fear.

Computer Security

- Computer security (also known as cyber security or IT security) is information security as applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the Internet as a whole.

- Computer Security is the protection of computing systems and the data that they store or access.

Computer Security

- Computer Security covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction.

- Computer security also includes protection from unplanned events and natural disasters.

Why is Computer Security Important?

- Enabling people to carry out their jobs, education, and research.
- Supporting critical business process.
- Protecting personal and sensitive information.

Why do I need to learn about Computer Security?

- Good Security Standards follow the "90 / 10" Rule:
- 10% of security safeguards are technical.
- 90% of security safeguards rely on the computer user ("YOU") to adhere to good computing practices
- Example: The lock on the door is the 10%. You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. You need both parts for effective security.

What Does This Mean for Me?

- This means that everyone who uses a computer needs to understand how to keep their computer and data secure.

- Information Technology Security is everyone's responsibility

Simple measures to be followed…

- Many cyber security threats are largely avoidable. Some key steps that everyone can take include:

—Use good, cryptic passwords that can't be easily guessed and keep your passwords secret

—Make sure your operating system and applications are protected with all necessary security patches and updates

—Make sure your computer is protected with up-to-date antivirus and anti-spyware software

Simple measures to be followed…

—Don't click on unknown or unsolicited links or attachments, and don't download unknown files or programs onto your computer

—Remember that information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept

- To help reduce the risk, look for https in the URL and the little padlock that appears in the URL bar or in a corner of the browser window before you enter any sensitive information or a password.
- Also avoid standard, unencrypted e-mail and unencrypted Instant Messaging (IM) if you are concerned about privacy

What are the consequences for security violations?

- Risk to security and integrity of personal or confidential information
  - e.g. identity theft, data corruption or destruction, unavailability of critical information in an emergency, etc.
- Loss of valuable business information
- Loss of employee and public trust, embarrassment, bad publicity, media coverage, news reports
- Costly reporting requirements in the case of a compromise of certain types of personal, financial and health information
- Internal disciplinary action(s) up to and including termination of employment, as well as possible penalties, prosecution and the potential for sanctions / lawsuits

Summary

- Definition of Cyber Crime
- Classification of Cyber crimes
- Computer Intrusions and Hacking
- Computer Security