Cyber Security

Instructor : Saba Iqbal

Learning Objectives

After going through this lesson you would be able to:

- What is cyber security?
- Meaning of the word cyber
- Need of cyber security
- History
- Categories of cyber crime
- Major security problems
- ATM skimming and point of scale crimes

What is Cyber Security?

- Cyber security refers to the technologies and practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks via the Internet by cyber criminals.
- Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks.
- It's also known as information technology security or electronic information
- It is important for network, data and application security.

Need of Cyber Security

- Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.

History

- The first cyber crime was recorded in the year 1820.
- The first spam email took place in 1978 when it was sent over the Arpanet.
- The first Virus was installed on an Apple Computer in 1982.

Categories of Cyber Crime

We can categorize cyber crime in two ways:-

- **The computer as a target:** Using a computer to attacks other computer e.g., Hacking, Virus/Worms attacks, DoS attack etc.

- **The computer as a weapon:** Using a computer to commit real world crime e.g., credit card fraud etc.

Types of Cyber Crime

- Hacking
- Phishing
- Denial of Service (DOS)
- Spam Email
- Spyware, Adware
- Malware (Trojan, Virus, Worms etc.)
- ATM Skimming and Point of Scale Crimes
- Ransomware

Hacking

- Hacking in simple terms means an illegal intrusion into a computer system and/or network.
- It is also known as cracking.
- Government websites are the hot targets of the hackers due to the press coverage; it receives.

Phishing

- Phishing is a fraudulent attempt, usually made through email, to steal your personal information.

- Phishing is the attempt to obtain sensitive information such as username, password and credit card details, often for malicious reasons through an electronic communication (such as E-mail).

- A common online phishing scam starts with an email message that appears to come from a trusted source (legitimate site) but actually directs recipients to provide information to a fraudulent web site.

Denial of Service

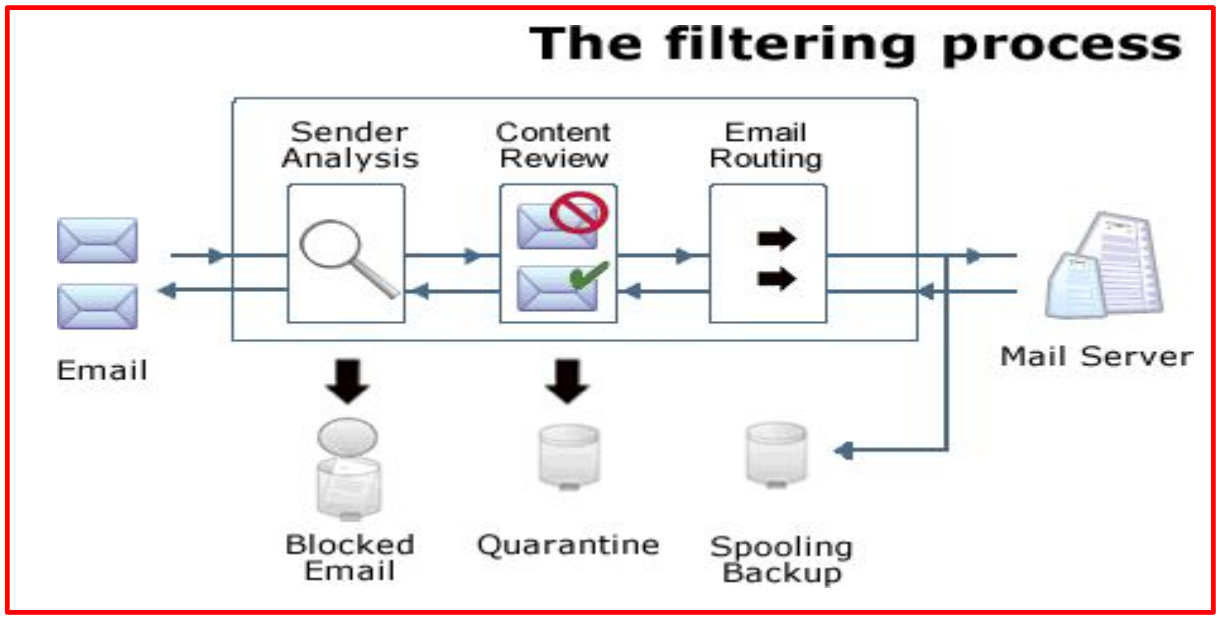
- A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic.

- This renders the system unusable, preventing an organization from carrying out vital functions.

Spam Email

- **Email Spam** is the electronic version of junk **mail**. It involves sending unwanted messages, often unwanted advertising, to many recipients.

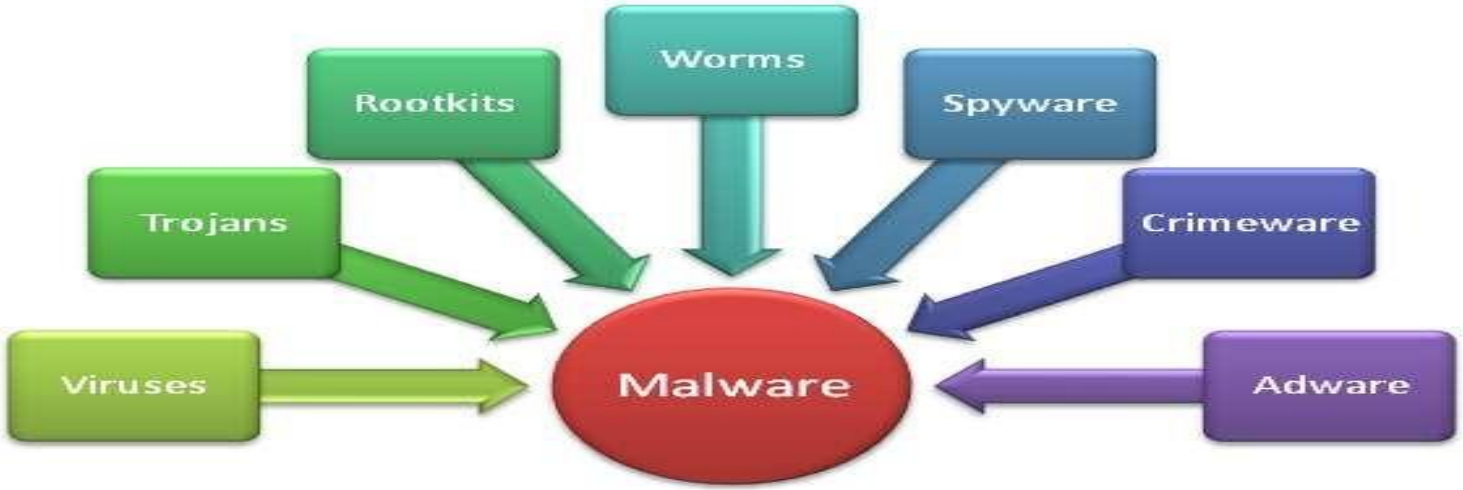
- **Spam** is a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks.



Malware

The word "malware" comes from the term "Malicious software."

Malware is any software that infects and damages a computer system without the owner's knowledge or permission.



Differentiate between Various Types of Malware

Malware: Pick Your Poison – Spam and Cookies

- Malware is malicious software
- Includes different types of programs designed to be harmful or malicious

✔ Spam

✔ Adware and spyware

✔ Viruses

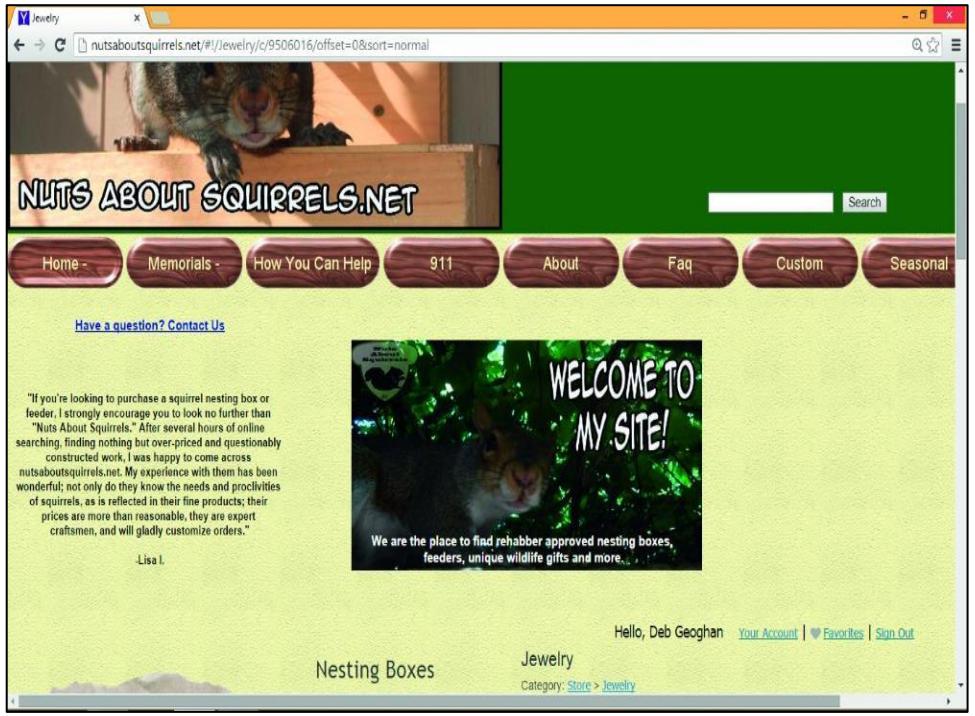
✔ Worms

✔ Trojan horses

✔ Rootkits

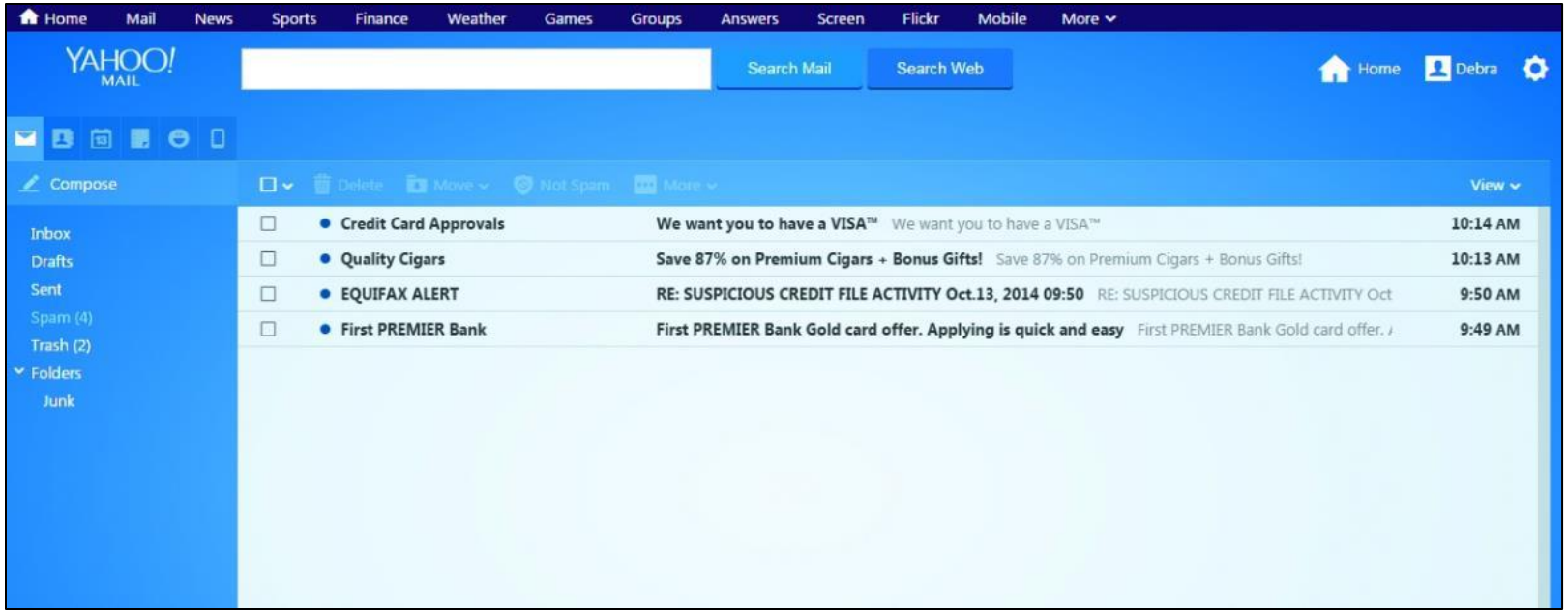
Malware: Pick Your Poison – Spam and Cookies

- Cookies
  - ✓ Installed without your permission
  - ✓ Help websites identify you when you return
    - Track websites and pages you visit to better target ads
    - May collect information you don't want to share



Malware: Pick Your Poison – Spam

- Spam
  - ✓ Spamming is sending mass unsolicited emails
  - ✓ Messages are called spam
  - ✓ Other forms:
    - Fax spam
    - IM spam
    - Text spam



Different Types of Malicious Programs

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 and mobile device either by altering or deleting it.

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

- **Trojan** is a type of malware that pretends to be something useful, helpful, or fun while actually causing harm or stealing data. Trojans are often silently downloading other malware (e.g. spyware, adware, ransomware) on an infected device as well.

- Trojans can infect you in places where you might not expect it, such as emails, downloads and more. It's always better to be safe than sorry when it comes to avoiding this type of malware.

Spyware

- Spyware is a type of malware that hackers use to spy on you in order to gain access to your personal information, banking details, or online activity. We should protect ourselves by an anti-spyware tool.

Adware

- Adware is a type of malware that bombards you with endless ads and pop-up windows that could potentially be dangerous for your device. The best way to remove adware is to use an adware removal tool.

Ransomware

- Ransomware is as scary as it sounds. Hackers use this technique to lock you out of your devices and demand a ransom in return for access.
- Ransomware restricts access to your computer system and demands that a ransom is paid in order for the restriction to be removed.
- The most dangerous ransomware attacks are caused by Wannacry, Petya, Cerber and Locky ransomware.
- The money which suppose to be paid to remove ransomware from your system which is called ransom money.

Rootkit

- Set of programs, install themselves as part of some other download, backdoor, or worm.
- They then take steps to prevent the owner from detecting their presence on the system. -- **Nearly impossible to detect**
- Once installed, Rootkits provide a bad actor with everything they need to take control of your PC and use it for as a zombie computer.
- Rootkits operate near the core of OS, which means they have low-level access to instructions to initiate commands to the computer.

SOLUTION OF THE MAJOR SECURITY PROBLEMS

1. Virus
2. Hacker
3. Malware
4. Trojan Horses
5. Password Cracking

Viruses/Trojan Horses, Malwares

"program that is loaded onto your computer without your knowledge and runs against your wishes

Solution

Install a security suite that protects the computer against threats such as viruses and worms.

Hackers

In common a hacker is a person who breaks into computers, usually by gaining access to administrative controls.

How To Prevent Hacking

It may be impossible to prevent computer hacking, however effective security controls including strong passwords, and the use of firewalls can helps.

WINDOWS DEFENDER

SECURE YOUR COMPUTER

- Download an anti-malware program that also helps prevent infections.

- Activate Network Threat Protection, Firewall, Antivirus.

Password Cracking

Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

Securing Password

- Use always Strong password.
- Never use same password for two different sites.

Cyber Security Is Everyone's Responsibility

ATM Skimming and Point of Scale Crimes

- It is a technique of compromising the ATM machine by installing a skimming device a top the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine.
- Additionally, malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number codes that are later replicated to carry out fraudulent

How can we protect?

- **BE CAREFULL!!**

  - Read Privacy policy carefully when you submit the data through internet.
  - Encryption: lots of website uses SSL (secure socket layer)to encrypt a data.
  - Disable remote connectivity.

Safety Tips to Cyber Crime

- Use Antivirus Software.
- Insert Firewalls.
- Uninstall unnecessary software.
- Maintain backup.
- Check security settings.
- Never give your full name or address to strangers.
- Learn more about the internet privacy.

Advantages of Cyber Security

- It will defend us from hacks and virus. It helps us to browse the safe website.
- Internet Security process all the incoming and outgoing data on our computer.
- The cyber security will defend us from critical attacks.
- The application of cyber security used in our PC needs update every week.
- The security developers will update their database every week once. Hence the new virus also detected.