

Lecture: #06
Securing Your Computers



Dr. Redhwan M. A. Saad

Head of Cybersecurity Department

Faculty of Informatics

Midocean University



CyberSecurity Fundamentals (CYB670)



Securing Your Computers

Introduction

Firewall Settings

Antivirus Software

Anti-spyware
Software

Anti-spam
Software

Security Updates

Secure Browser
Settings

Scan Devices
Before Data
Transfer

Social Engineering
Attack Precautions

Miscellaneous Tips



- Computers have become the most integral parts of our day to day life.
- We use computers so extensively that our **personal and public matters and activities are fully under the influence of computers.**
- We **communicate** through computers, we **buy** through computers, we **sale** through computers, we **travel** with the help of computer-based systems, we **work** through computers, we are **paid** through computers, and even we **order our food** through computers.





- The computers have drastically changed the way we lived our lives a few decades back.
- In the 1970s when the first microprocessor was developed, nobody thought of that chip to influence the way it has done in today's modern life.
- After the development of internet and worldwide web, the influence of computers has become eminent on all fields and activities of life.
- As the dependency of the people on computers increased, the issues with security of the computer expanded exponentially.
- No one was aware of the **dark side of the impact of computer** till the first malicious program hit the internet resulting huge losses to the public lives and businesses.





- The demand for the security of computers started increasing exponentially in the modern field of information technology.
- There are many kinds of **threats** to the computers, communication networks, and all physical infrastructures that use the power of computer for their operations.
- The **threats to the computers** can be divided into two major parts:
 - **Traditional physical security threats** (*Examples: Natural events (e.g., floods, earthquakes, and tornados) Other environmental conditions (e.g., extreme temperatures, high humidity, heavy rains, and lightning) Intentional acts of destruction (e.g., theft, vandalism, and arson)*)
 - **Cyber security threats** (*Examples: Malware, Social engineering, Ransomware, Phishing, Man-in-the-middle attacks, , Spyware, etc...*)





- The **physical threat** can be further classified into:
 - Overt physical threats (*e.g., floods, earthquakes, and tornados*)
 - Covert physical threat (*e.g., spilled drinks, overloaded electrical outlets, and bad plumbing*)
- Similarly, the **cyber security threat** can be classified into:
 - Computer security
 - Network security
 - Data Security





- In this chapter, we are going to talk about the how to secure your computer from the cyber threats?
- From the beginning of cyber security threats, the number of hackers is increasing very fast. Hundreds of thousand hacker attacks take place annually on the internet.
- The list of the FBI's most wanted cyber criminals is increasing continuously.
- The total number of cyber criminals included the most wanted list of the FBI expanded to 63 in the first month of 2019.





- The gravity of the cyber-attacks can be imagined by the latest statistics released by MacAfee Inc.
- According to the McAfee research, the total loss due to cybercrimes worldwide was estimated at about \$600 billion in 2017. **1 Trillion in 2019**
- With the advancement in the technology, the hackers are also becoming so sophisticated and advanced in attacking the computers.
- Newer ideas, tools, techniques are being **applied by the hackers** to damage the cyber environment.





Let's have a look at the major components used for securing our computers.

- Firewall Settings
- Antivirus Software
- Anti-Spyware Software
- Anti-Spam Software
- Security Updates
- Secure Browsing Settings
- Scan Devices before Data Transfer
- Social Engineering Attack Precautions
- Miscellaneous Tips





- **Firewall** is the first line of defense for the computer, when it is connected through the internet or other networks.
- A **firewall** is a type of security software that is able to check and monitor traffic coming from certain sources and leaving for a certain ports or destinations.
- **Firewall software** is used as the first line of defense for any kind of security threat originating from the external sources in a connected environment.
- It is also the last security check-post for any traffic originating from your computer.





- Many **firewall** software monitors both incoming and outgoing traffics, but some firewall software only focuses on the incoming traffic because the main threat normally originates from the external sources sitting on the other side of the firewall.
- The software applications that we use on our computers use the communication port numbers at transport layer of the OSI model.
- The **firewall** checks the port numbers of the traffic to make sure that the traffic originated from the authorized sources and terminating at the genuine port.





- If there is any kind of irregularity in the traffic, the firewall is able to detect the suspicious activities and to generate an alert for the same.
- It is also able to close the port for incoming traffic, if it is configured for the auto-blocking malicious activities.
- In most of the cyberattacks, the hackers use the un-trusted connections to access the vulnerable applications on the computer to launch some malicious software code to install on your computers using those unauthorized connections.
- **Firewall** is able to detect any un-trusted connection and stop it from intruding into the security of the system.





- Thus, the hacker is caught at the first defense of the computer before performing any malicious activity on the computers.
- There is numerous firewall security software available in the market.
- You can get so many firewalls for free too, but it is always not recommended to get the free security software for your computer with critical information.
- Always purchase the firewall security software by paying their price.
- The **paid software** is more robust and highly featured to capture numerous kinds of threats originating from the malicious users.





A few very important **firewall software** that are known for having many great features and capabilities are mentioned below:

- Zone Alarm Pro Firewall
- Comodo Firewall
- Norton Security Standard Firewall
- Kaspersky Internet Security with Firewall
- Bit Defender Security Firewall
- TinyWall Firewall Software

It is always a great idea to activate the high-level security settings on firewall, but it may irritate you with many warnings and alerts. So, always try to configure firewall settings to allow all programs and their connections to monitor.





Firewall Settings

- If you have many applications that you don't use, you should remove those applications from your computer to make your computer less prone to the external threats.
- **Windows operating system** comes with integrated firewall software. It is activated by default, and you need to configure your security firewall for stronger security settings.
- The Windows based firewall does **not monitor the outgoing** traffic from your computer, but it focuses mainly on the incoming traffic to monitor for any kinds of threats originating from the adversary sources.





- **Antivirus** is one of the fundamental security tools that are recommended for every computer whether that is connected to the external world through internet or even it operates standalone position or in the silos.
- **Antivirus software** is a security software utility that is able to detect different types of viruses and malwares on computers. It is also able to **remove, delete, and quarantine** a virus that has already affected the computer.
- There are many types of **viruses** that commonly spread on the internet at a very high rate; among such viruses, Trojan horses, worms, viruses, rootkits, and other forms are a few very common to name. These viruses are very dangerous for damaging your valuable data on your computer.



- **Viruses** use different types of application and system **vulnerabilities** to get them installed on the computer. Slowly and gradually, they start damaging, coping, or deleting your valuable data.
- At some point, you will lose your data completely without any remedy to the data recovery.
- **Hackers and malicious attackers** use different types of viruses for different purposes to launch some of the lethal cyberattacks on the networks and computers on the internet.
- So, you should always be very well aware of the damage those viruses can inflict on your computers.



- The **viruses** also start duplicating on the computer, and thus reducing the performance of your computer by filling up the free space on your disk, using the excessive memory, choking data bandwidth and other resources of the computer and networks.
- Many **viruses** create **backdoors** on the computers and start sending your valuable information and control to the handlers of the viruses through backdoor.
- Once the control of your computer is transferred to the hackers, your computer starts acting as a source of cybercrimes by attacking the other computers on the network. Your computer becomes a '**Zombie**' for hacker attacks.



- Numerous Good antivirus software programs, which are available in FREE as well as in paid versions.
- You can choose any of those versions from the **reputed antivirus software providers**.
- For computers with **critical** information and personal data, it is NOT recommended to use **free** antivirus software because those software programs offer **limited** capabilities and features.
- And those limited capabilities are **not sufficient** for stopping certain viruses that are more powerful and more dangerous to your computers.



- Almost all available **anti-virus software programs** have multiple **features** like **virus cleaner**, **spyware cleaner**, **Trojan horse detection**, **performance improvements** and other standard features required for keeping your computer clean.
- But, the **paid versions** of those antivirus software are more robust and have additional deeper features to cope with many dangerous of the cybercrimes.



- A few names of the top-notch **antivirus software programs** are mentioned below:
 - Kaspersky Internet Security
 - Panda Premium Antivirus
 - AVG Internet Security
 - Microsoft Security Essentials
 - McAfee Total Protection
 - Comodo Antivirus Software
 - Avira Antivirus Pro
 - Avast Security Ultimate
 - Norton Security
- Most of the antivirus are set to **update their versions automatically by default**, but in some cases if the antivirus software update is not turned on, activate it.





- You should also take of the following **important points for keeping your computer free from viruses.**



- Make sure your antivirus software automatically starts with the **starting** of your computer
- Antivirus is always **on** while the computer is **on**
- Always download and install the **latest updates** from the venders to update the virus definition **database**
- Regularly run quick **scans** on your computer
- Run full scans occasionally after a few weeks
- Always scan the **data transfer mediums** before copying any data
- Take notice of all **warnings and alerts** generated by the antivirus software



- **Spyware** is one of the most critical tools for launching cyberattacks on the targeted networks, services, or the computer servers.
- **Spywares** are the malicious code design to spy on the activities of the user for getting information about *the behavior of the internet user or steal the crucial information* from the computers and online user accounts.
- The advertisement campaigns can be started with proper focus on the targeted market segments suitable for their online marketing campaigns.





- One form of the dangerous spyware code is known as the **keylogger**, which is used to track and record the keys pressed. **And sends it to the command-and-control center.**
- The hackers **steal the information** such as usernames, passwords, and other codes or pin numbers used for your financial activities and other valuable transactions through the internet.





- If you have already installed a **full version of any antivirus software** on your computer, you might have purchased the **antispyware** already. Many modern antivirus packages are also **included** with the **spyware tools**.
- If there is no such security software on your computer, download one from the reputed companies to secure your computer from malicious spying on your computer, data, and your internet using behavior while browsing the internet.
- **Spyware codes** normally spread through free downloads, free websites, and other such free sources available on the internet.
- So, it is highly recommended to use the paid version of the software from the **trusted security companies**. Those software are not piggybacked with the spyware or other malicious codes.





- A few very well **trusted antispyware software companies** are listed below, you can choose any one of them to download the antispyware security software.
 - SuperAntispyware software
 - Spybot – Search and Destroy
 - Adaware Software
 - SpywareBlaster
 - AVAST Antivirus (embedded)
 - AVG Antivirus (embedded)
 - MalwareBytes Spyware
 - Emsisoft Emergency Kit





- Take the following measures to **make your spyware protection more robust** and effective:
 - Use reliable and dedicated **antispyware** software.
 - Always keep your antispyware software **up to date**
 - **Scan** your computer regularly for any kind of spyware on your computer
 - Always be vigilant while visiting the unknown websites
 - Major source of spyware spreading is infected websites
 - Deal strictly with the **pop ups** and alluring offers by clicking “x” on it
 - Set your browser settings to **block popup ads**
 - Don’t open emails from the **unknown** senders





- **Spamming** is one of the major sources of spreading malwares on the internet.
- Many spammers send malicious code like spyware, malwares, and viruses through different kinds of **unsolicited** emails from different sources.
- A huge **time was consumed** on reading those unsolicited emails, which caused a huge loss to the company productivity.



- At that time two IT engineers started working on this problem by sorting out the IP addresses, servers, locations, company names and other information from where the spamming emails were originating.
- That list was later used on the routers to filter the spamming emails through the boarder gateway protocol (BGP) on the internet.
- They named it as the Mail Abuse Prevention System (**MAPS**). The name was a bit difficult so they reversed the order of the words to make it SPAM.
- This list was later converted as real time black-hole list precisely referred to as RBL.



- A large majority of the **public email servers** like **Google, Yahoo, Hotmail and others** have successfully tracked and identified more than 99% of the spam emails and send them directly to their spam or junk folders.
- Thus, **a huge time and energy of the email users is saved.**
- But this problem is still a matter of concern for many small and big organizations across the world.
- They **use different anti-spam services and software tools** to stop this menace. This cost them money and manpower substantially.



- According to the latest research released by digital trends website suggest that the strike rate of spam emails has increased from 13.4% in 2017 to 14.2% in 2018. If this trend persists for a few years, the nuisance of spamming emails will soar again.
- The **spammers** are becoming more sophisticated and start sending personalized emails and other phishing techniques to make the spamming more dangerous in years to come.
- **A large ratio of over 31% of the spam emails contain the malicious links**, if the strike rate of clicking continues to increase the threat of cyberattacks will also increase substantially. The increase in the cyberattacks will inflict damages to the global economy exponentially.



The major anti-spamming software and services include the following:

- Hornet Security Spamfilter Service
- SpamTitan anti-spam software
- MailCleaner anti-spam software
- SpamPhobia anti-spam
- Spambrella anti-spam service provider
- FireTrust MailWasher Service

You can also use **customized services** and **software tools for safeguarding** your company employees from the nuisance of spam emails.





- As mentioned earlier, the **success rate of the anti-spam software tools** or anti-spam email cleaning services is about 99% or so. Still there is a chance of the spam emails to pass through to the inbox of the users. Therefore, you need to take care of your emails too.
- Other than using the anti-spamming emails solutions, you should also take care of the following points while using emails.
 - ***Never open emails from unknown users***
 - ***Never click on the links or attachments of spam emails***
- Always keep the volume of spam emails in mind; if there is any spike in the emails consult with your cyber security person or service provider



- Computers perform different types of functions and activities based on the software code that runs not only the hardware of the computer, but also the software utilities that we use.
- **No software code is 100% perfect.** There may be some flaws, bugs and other vulnerabilities in all types of software programs.
- These bugs or vulnerabilities in the software programs may be **present** in the operating system, drivers, application software, utilities software, and network software.
- The vulnerabilities in the websites and web-based applications can also be a major issue that can pose security threat.





- **Hackers and cyber criminals use those vulnerabilities**, flaws, bugs, and obsolete features to **attack the computers and the networks**. The security professionals always keep a close eye on the code, features of the code, bugs, possible vulnerabilities and other security related aspects to make improvements in the system and application software.
- The modification and improvement in the software tools with new software **patches** or new version releases are known as the **updates**.
- The updates are very critical not only for the security of your computer, data, and network, but also for the other people connected with you and your computer network.





- If you don't update your software regularly, you would definitely remain at the risk, but your computer once infected, will also pose the threats for the other users on the internet because your computer may turn a **zombie** and spread security threats to other computers of the people known to you and the people connected on your network.
- For keeping your computer updated with the security patches, **you should need to install patches** and **install newer versions** of the following applications:
 - Use the latest version of the operating system of your choice
 - Always install operating system software updates regularly without any delay





- Always use genuine security software programs
- Avoid to use free programs, which may bring some malware accompanied with them
- Always put your security applications on auto updating option
- Update every software application that you use on your computer
- Remove all applications that you don't use
- Always use the latest versions of the software utilities and applications on your computer
- Don't use the cracked version of software applications, it may be very dangerous for your data and computer security
- Never delay in installing downloaded updates





- By taking all of the above-mentioned measures carefully, you can save your data, computer, and applications from big dangers.
- Meanwhile, you also help in making the internet more secure for the people you know and the other people connected on your network.





- The **vulnerabilities in the browsers** are extensively exploited by the hackers and malicious attackers **to** intrude into the computer systems for carrying out cybercrime activities like data theft, identity theft, data corruption, ransom attacks, spamming, and other activities.
- Many browsers are used by the internet users; among such commonly used browsers Google Chrome, Windows Explorer, **Mozilla Firefox**, and Netscape are a few very important ones to name.
- **Every browser has its own capabilities and security features.**
- Presently, Google Chrome is one of the most popular browsers used in the internet surfing and accessing the other online web services.



- Google and Mozilla Firefox are releasing their security patches and software features more frequently as compared to the other browsers.
- That is the reason that many people prefer using these two very important browsers for majority of the operating systems including Linux, Windows, Mac, and others.
- Every browser has numerous settings that relate performance, security, privacy, and other plugins and functions.
- While using the browsers, you should take special care of all those features and capabilities, especially the security settings.
- You should **configure your browsers with high level of security** and **privacy settings** to make sure that hackers would not be able to exploit the possible vulnerabilities in low secure settings of a browser.



- You should set the browser to safe browsing mode. Meanwhile, the settings should also not allow the tracking of the traffic request and turn on the **SSL** and **HTTPs** certificate settings.
- All these security related settings would help you stay away from the malicious attacks of the hackers.
- Your browser should be configured for automatic installation of plugins.
- You should install plugins only when you are 100% sure about that plugin and you trust that vendor.



- The privacy settings of the browser should also be restricted to high-level of privacy.
- **Your location, personal information, login and passwords and other information** should also be **not** configured to show or save for every user on the computer. You should also set separate user group for accessing the computer resources.
- **It is always recommended not use the administrator account for normal activities** like emailing, internet surfing, normal home or office work or other such routine activities.
- If you are **not logged in as administrator**, then any malicious attempt to install some code on your computer would be difficult for the hackers.
- The malicious program will be prompted with logging in as administrator to install any new program.



- Thus, your computer will remain safe from hidden attempts to install some malicious programs on your computer, and you will also be alerted for any attempt to alter the settings of your computer or any attempt to install some malicious programs on your computer.
- Let's summarize the main **settings of your browser to keep your computer safe** from any malicious attempt to alter your computer resources and settings.
 - Setup privacy settings to high level
 - Use separate strong password-based user groups
 - Don't save passwords on browsers



- Don't **login** as an **administrator** until you really need it
- Activate the safe **browsing settings** on the browser
- Your browsing traffic should be attached with '**Do Not Track**' request
- Activate **SSL** and **HTTPS** settings
- All popup, plugin, and other activities should be denied or should be asked to get **permission** from the computer **admin**
- Computer resources and content access settings should be very strong
- Always check for harmful software installed on your browser or computer



- **Data travelers** or **other devices** to run or transfer data from one point to another one have been the major transporter of viruses, worms, Trojans, and other malicious codes.
- Among such devices flash drive, CDs, DVDs, external hard drive, and any other data transferring devices.
- All those devices should be properly **scanned with the updated antivirus and anti-malware** software to detect and kill any malicious programs attached to the data.
- After scanning the devices fully, you can copy or transfer data between the devices; this will reduce the threat of viruses to infect your computer.





- **Social engineering** is very important source for unleashing a cybercrime on your data, personal information, and bank account information.
- In this form of cyber-attacks different mediums like text messages, chatting, group discussion, telephone call, and emails are *used to communicate with you to exploit your innocence or ignorance*. This is also a part of **cyber frauds**.
- You might have noticed that you get an email from a legitimate looking source that you got a prize through a **lucky draw** or you **got a big job opportunity in a big organization**. That email looks like it has been sent from a legitimate company and you will be lured by the presentation of the content.





- The **hacker** on the other end of the communication tries to use the social behavior to influence your thoughts and asks you to provide your personal information including the bank account and other information.
- When they receive this information, they request you for some processing fee and may ask for credit card information.
- If you provide this information, they use it maliciously to damage you to steal money from your banks or from your credit card.
- If you send the money they ask for, they will go away and will not appear again.





- The **main objective of such social engineering attacks** is to achieve the financial benefits from the innocent people.
- They also use the text messages, phone calls and other mediums for the same purpose.
- In those cases, the in-person communication is used so efficiently that you will not doubt on their sincerity at any point of time.
- They use very professional manners to talk with you so politely and effectively that you start believing in their conversation and provide the information they like to get from you.





- Hackers use the social engineering tactics **to spread malware in your mobile and computer device** through emails, attached documents, and messages.
- Once you click the emails and its attachments, the viruses embedded in those emails download and install on your computer or mobile device. Thus, those viruses start carrying out the activities that they are designed for by the hackers sitting at the remote site.
- So, never open emails, text messages or other messages from unknown people.
- If you **see any kind of such alluring message from the unknown**, just delete it without any second thoughts!





- All of the above-mentioned items are the major components of keeping your computer free from the viruses and other cyber-attacks.
- There are many other factors that are also very important for keeping your computer free from the viruses.
- All those factors should be considered carefully other than the above-mentioned items. Those miscellaneous tips play very crucial role in your personal behavior towards the computer security.
- As we known, **the security is a continuous process** and **it is not possible to achieve by acting once**.
- You will have to adopt different recommendations and industry guidelines in your behavior so that you can make your habit 100% in compliant with the computer security standards and procedures.



The main tips for keeping your **computer free from viruses** are listed below:

- Never use the cracked software
- Never use free software because free software tools are normally embedded with some additional codes and advertisements, which can spy on the users and take the information and send to the company servers.
- Never save your passwords on your computer or browsers because if your computer is compromised, then your passwords and other information will at direct risk
- Don't provide critical information on telephone, email, or SMS
- Don't open files sent by unknown people



- Don't visit faulty websites
- Set your browser settings at high security and privacy
- Always create separate users for a computer
- Create a guest account with minimum privileges, if required
- Uninstall all Apps that are not in use
- Don't install unknown applications
- Always install the plugins that you deem necessary for your use
- Avoid to use free applications
- Always update your applications
- Use latest versions of OS
- Use latest versions of applications



- Never miss a security patch or update at all
- Daily check for the security updates
- Turn off your computer if you are not using it
- Turn off the internet router, if not used for a certain period of time
- Take security as a serious matter in your life
- Regularity check for the security guidelines
- Always make a copy of your valuable data
- Create check-points on your computer
- Run schedule virus scans regularly
- Always download something from the reliable websites
- Never try to use the public data sharing websites for exchanging data



- Use highly secure and reliable data sharing and collaboration platforms for data transfers
- Use strong passwords. The strong passwords should contain different combinations of the lower and the upper-case letters, symbols and numeric
- Encrypt your important data files through regular encryption options available with the operating systems or through any other tools available in the market

By taking all of the above-mentioned standard guidelines and tips for keeping your computer safe from viruses and other malware threats, you can avert big data losses and enjoy smooth internet browsing without incurring any damage to your computer.



1. In the,the hacker tries to use the social behavior to influence your thoughts and asks you to provide your personal information including the bank account and other information.
 - A. social engineering attack.
 - B. MITM.
 - C. DoS.
 - D. DDoS.

2. The first microprocessor was developed In the.....
 - A. 1970s.
 - B. 1990s.
 - C. 1980s.
 - D. 1950s.



Thank You