

COMPUTER MAINTENANCE, SECURITY AND PROBLEM SOLVING

WEEK 11

COMPUTER MAINTENANCE, SECURITY AND PROBLEM SOLVING



Objectives

At the end of this chapter you will learn:

- o how to maintain and protect computers
- o how to protect your files
- o basic security terminology
- o how to resolve computer-related problems
- o learn some security best practices.

COMPUTER MAINTENANCE

Definition

- Computer maintenance is a set of services or procedures performed to keep a computer in good working and robust condition.
- A well-maintained computer
 - Performs faster
 - Runs more efficiently
 - Crashes less
- Maintaining your computer will save your money and time, and protect your data.

COMPUTER MAINTENANCE

Why maintenance is important?

- Your computer could stop working.
- Your computer could slow down.
- Your computer could be marked as a virus-carrier.
- Spywares or viruses could reveal your personal information.

To avoid these problems you should know how to protect your files and computers.



FILE SECURITY

Protection of Your Files

- **File security** is a feature of your file system that
 - controls which users can access to which files,
 - brings limitations on what users can do with files.
- For instance:
 - A file may be viewed by everyone but can be changed only by specific people.
 - A file may be secured so that only the owner can view it.
- You can use a password to prevent others from opening or modifying your files.

FILE SECURITY

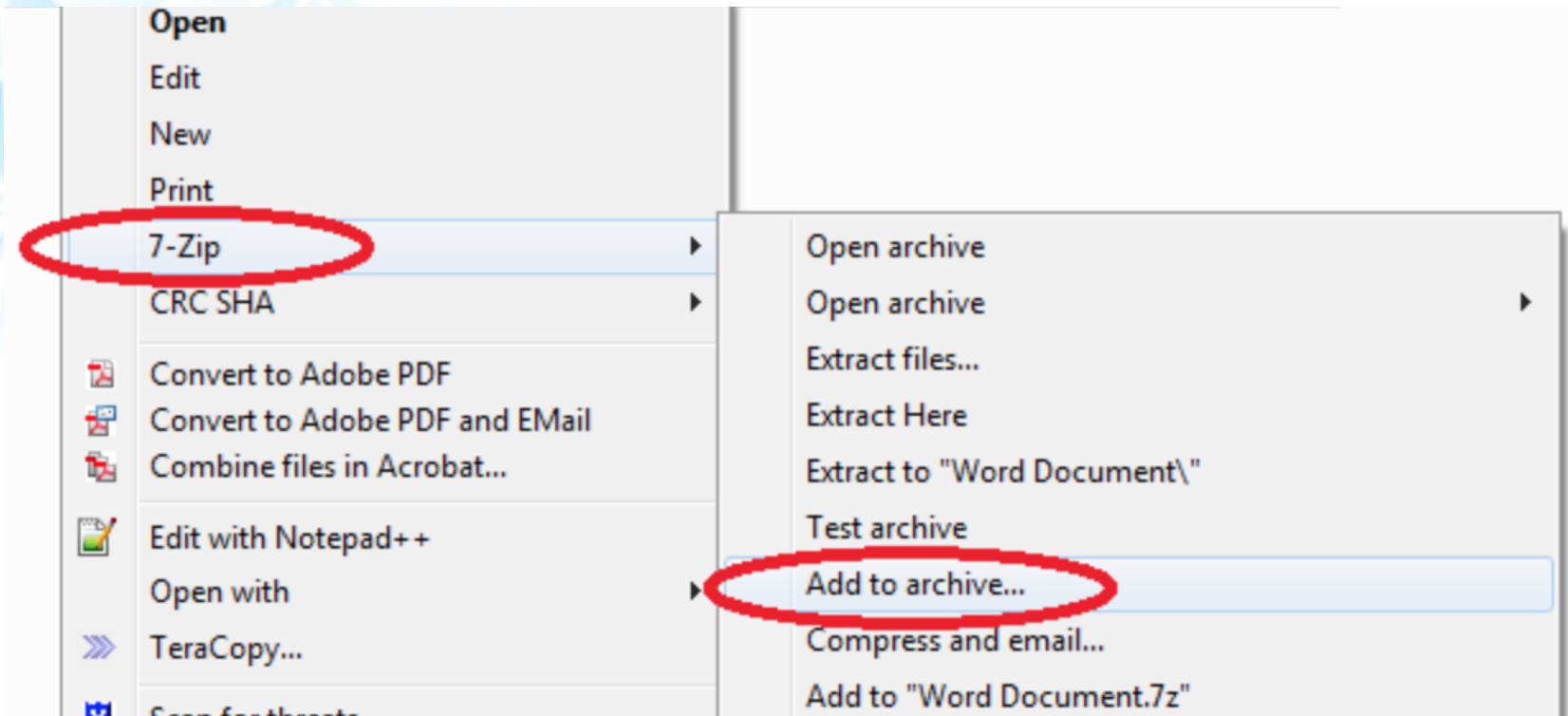
Encrypt and password protect a file on your computer

- In order to password protect or encrypt a file on your computer, you may need to install a third-party program that allows you to protect your files and folders.
- **7-zip** is one of the open source tools that you can use to encrypt and password protect your files.



FILE SECURITY

How to encrypt and password protect a file

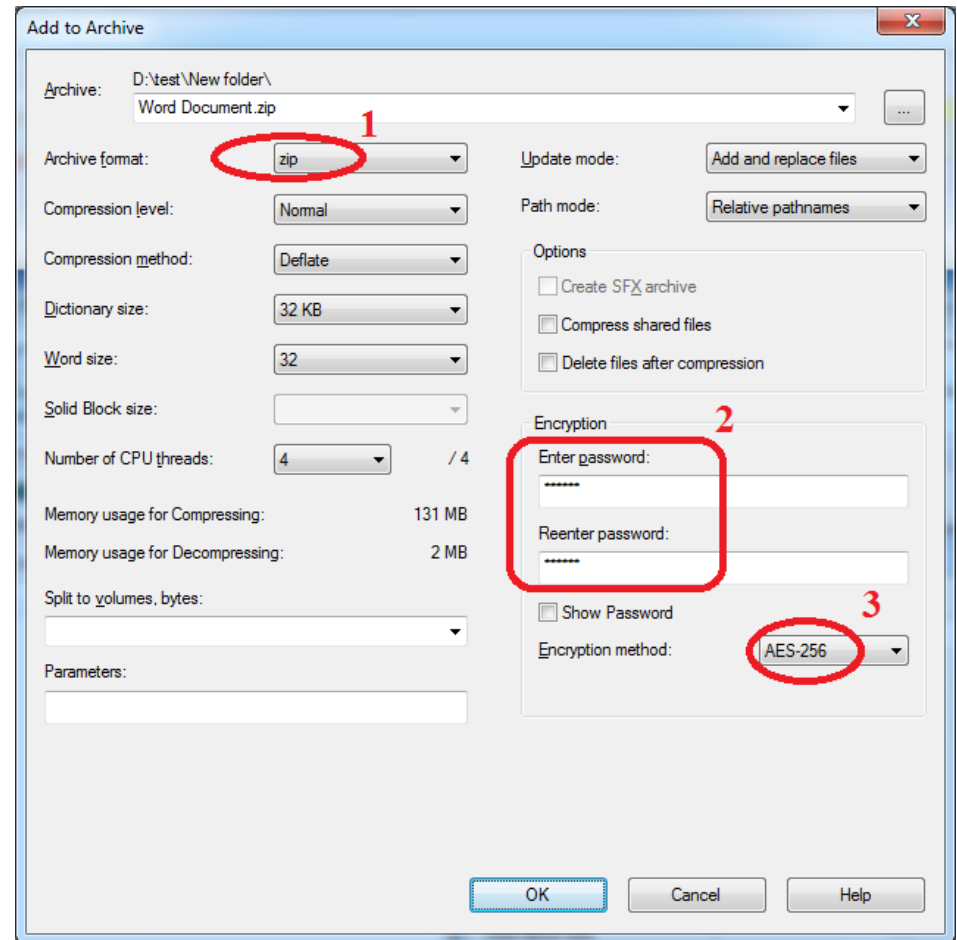


Select the file(s) you need to compress. Then right click the selection and choose "7-Zip" -> "Add to archive..." from the menu.

FILE SECURITY

How to encrypt and password protect a file

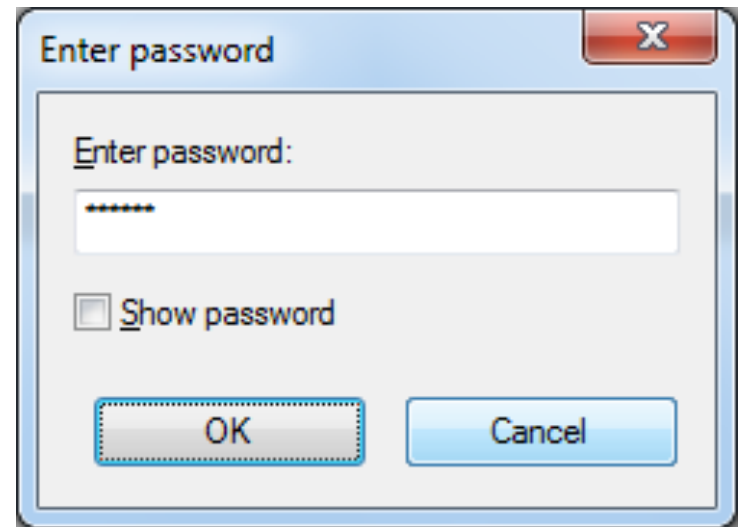
Make sure to choose "zip" for the archive format. Then enter your password (It is recommended to set password with more than 8 characters consisting of alphabets and numbers), and choose the "Encryption method" you prefer. Then click "OK".



FILE SECURITY

How to encrypt and password protect a file

In order to open the encrypted file, you will need to enter the password you set.



COMPUTER SECURITY

- You need to be careful about the protection of your computer when you
 - o connect to the Internet.
 - o allow other people to use your computer.
 - o share files with others.



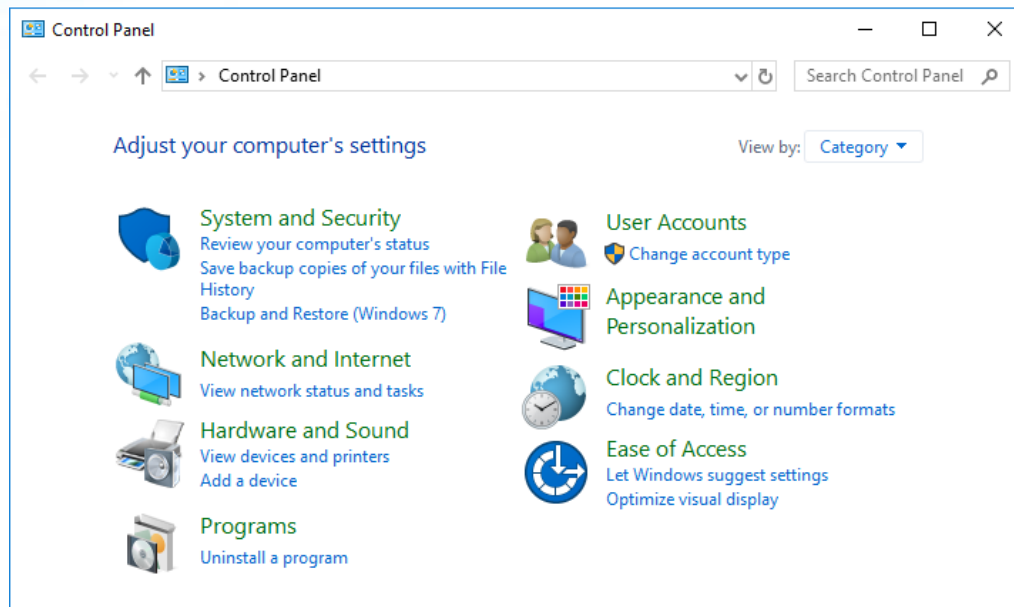
COMPUTER SECURITY

- Computer criminals (hackers or crackers) can attack
 - directly, by breaking into your computer through the Internet and stealing your personal information.
 - indirectly, by creating **malware** (MALicious softWARE).
- Malware is any software, such as a virus, spyware, Trojan, etc., designed to cause a damage to a single computer, server, or computer network.
- Fortunately, you can protect yourself by taking some simple precautions.

COMPUTER SECURITY

Windows Security Center

- Windows Security Center is your headquarters for computer security.
- It shows your computer's current security status and helps you to make your computer more secure.

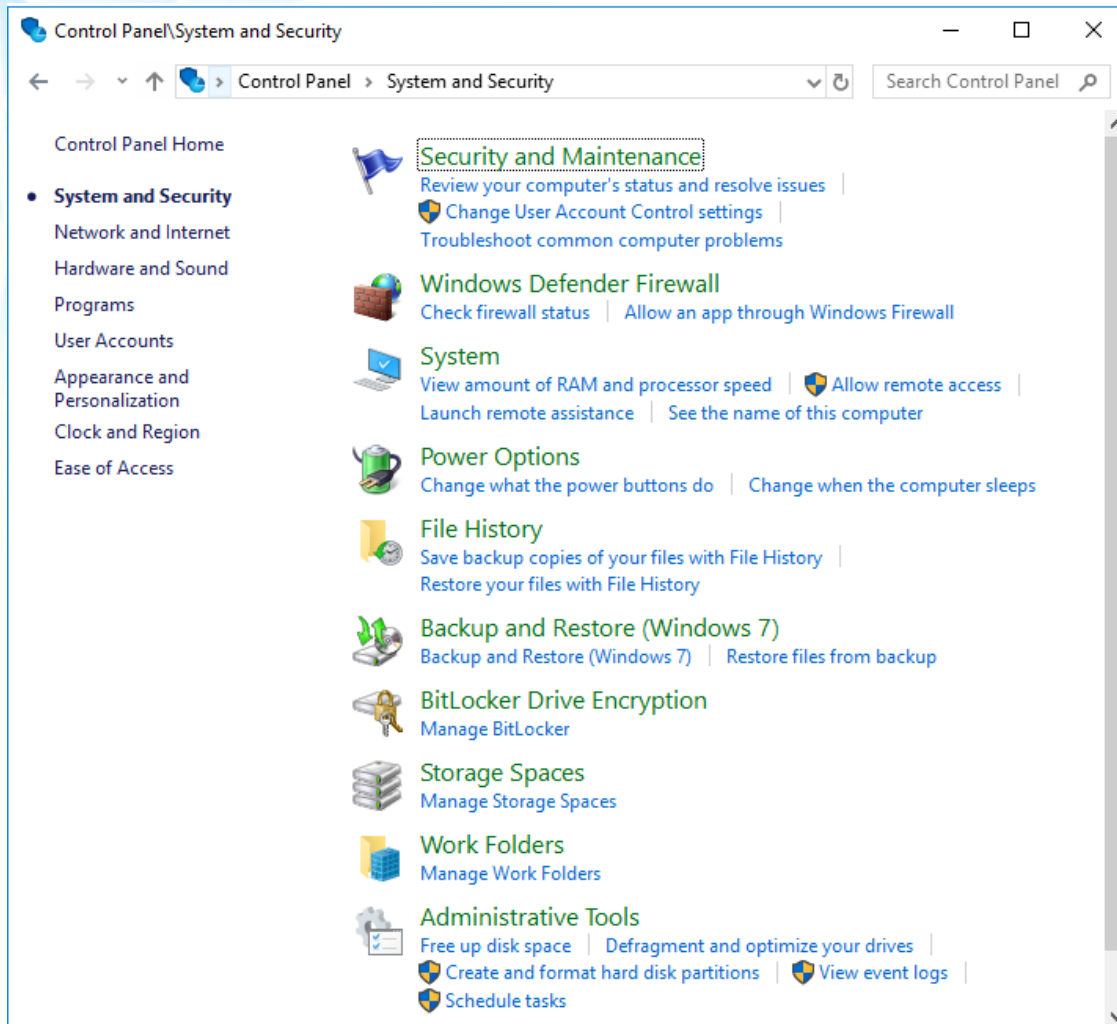


Windows Control Panel

- To open it:
 - In the search box on the taskbar, type **control panel**, and then select **Control Panel**.

COMPUTER SECURITY

Windows Security Center

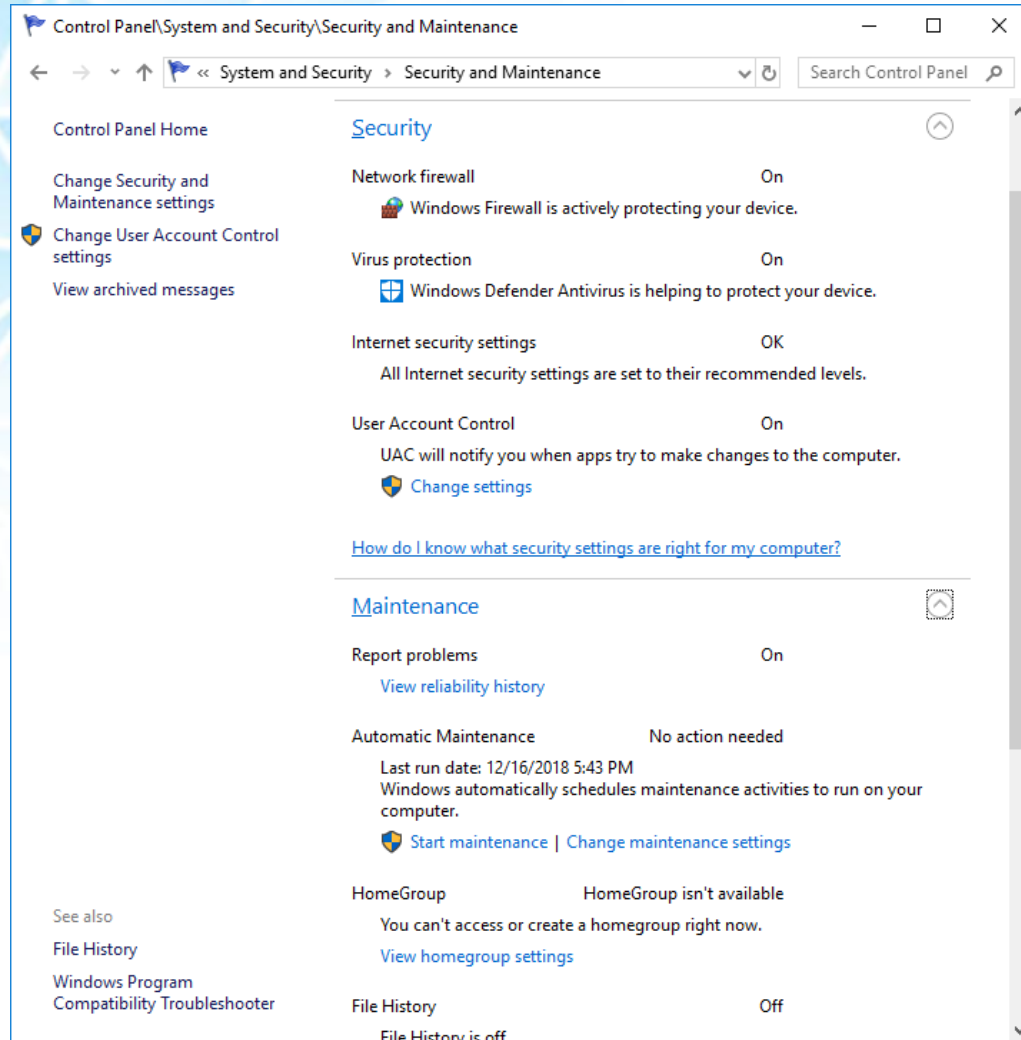


Click **System and Security**, and then click **Security and Maintenance**.

System and Security window of Control Panel

COMPUTER SECURITY

Windows Security Center



Windows Action Center

- Security and Maintenance checks your computer for these security essentials:
 - o Firewall
 - o Virus protection
 - o Internet security
 - o User controls
 - o Other security settings

COMPUTER SECURITY

Viruses, Worms and Trojan Horses

- Viruses, worms, and trojan horses are malicious programs.
- They can
 - cause damage to your computer and to the files on the computer.
 - slow down your computer and Internet connection.
 - use your computer to spread themselves to others.
- Malicious programs can reach your computer via email attachments or files downloaded from the Internet.
- If you receive an email with an attachment from someone you don't know, or about to download any file from the Internet, be cautious about the file before downloading it to your computer.

COMPUTER SECURITY

Viruses

- A **virus** is a piece of computer code that attaches itself to a program or a file so it can spread from computer to computer.
- It infects as it travels.
- Viruses can damage your software, hardware, and files.
- A true virus **does not spread** without human action.



COMPUTER SECURITY

Viruses

- **Programs and documents:** Programs and documents that you share can be infected with viruses.
- **E-mail:** E-mail can include infected attachments. Some emails even include malicious scripts that run as soon as you preview the mail or read the body.
- **The internet:** You may download programs or documents that are infected. Security vulnerabilities in your operating system can also allow viruses to infect your computer via the internet connection, though you are not aware of it.
- **CDs and USB Flash Drives:** They can hold infected programs or documents. Floppy disks can have a virus in the boot sector.

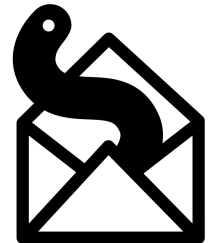


COMPUTER SECURITY

Worms

A **worm**, like a virus, is designed to **copy itself** from one computer to another, but it does so **automatically**.

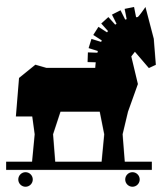
- Once a worm is in your system, it can travel alone.
- Takes control of features on the computer that can transport files or information.
- A great danger of worms is their ability to replicate themselves in great volume.
- A worm could send out copies of itself to everyone listed in your email address book.
- They can also tunnel into your system and allow somebody else to take control of your computer remotely.



COMPUTER SECURITY

Trojan Horses

- **Trojan horses** are computer programs that appear to be useful software, but instead they compromise your security and cause a lot of damage.
- Unlike viruses and worms, Trojans **do not** reproduce by infecting other files nor do they self-replicate.
- Trojans can
 - create a **backdoor** on your computer.
 - destroy or modify data the moment they launch such as erase a hard drive.
 - attempt to ferret out and steal confidential information such as credit card numbers and passwords.
- A Trojan horse can come in the different ways such as from email attachments or software that is downloaded from the Internet.



COMPUTER SECURITY

Antivirus Software

- Antivirus programs scan email and other files on your computer for viruses, worms, and Trojan horses.
- Some of security software products that you can use for your computer or mobile phones are **McAfee, Norton, AVG, Kaspersky** etc.
- Don't forget to update your antivirus software to its latest version to get the best security.



COMPUTER SECURITY

Antivirus Software

- If you don't have an antivirus program installed on your computer, you can only detect a virus when it displays its harmful effects.
- Followings are the some of the symptoms of an affected computer:
 - The computer slows down abnormally.
 - Unexpected error messages appear while running Windows applications ("application error", "system fault", "missing files" etc.).
 - The computer may not respond to your commands.
 - DOS operating system opens randomly.
 - Files cannot be opened.
 - Abnormal audio/visual behaviors take effect.
 - The computer performs other unwanted operations.

COMPUTER SECURITY

Spywares

- **Spyware** secretly gathers user information through user's Internet connection, usually for advertising purposes.
- For example, spyware can
 - install unwanted toolbars, links, or favorites in your web browser.
 - change your default home page.
 - display pop-up ads frequently.
 - secretly collect sensitive information.



COMPUTER SECURITY

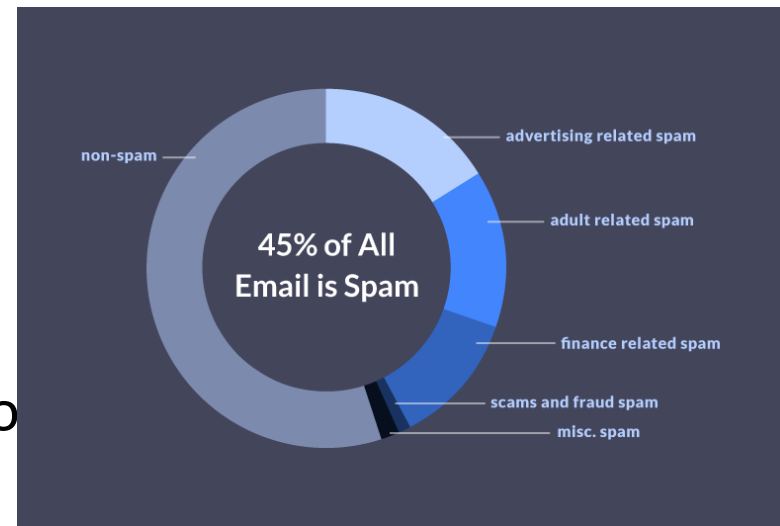
Protection from Spywares

- To protect your computer from spyware, use an antispyware program.
- Windows has a built-in antispyware program called Windows Defender, which is turned on by default.
 - Windows Defender alerts you when a spyware tries to install itself on your computer.
 - It also can scan your computer for existing spyware and then remove it.
- **Ad-Aware** and **Spyware Doctor** are two examples of anti spyware programs that you can use freely.
- Since new spywares appear every day, antispyware programs should be regularly updated.
- For the highest level of protection, set Windows to install updates automatically.

COMPUTER SECURITY

Spam

- **Spam** is an unsolicited commercial e-mail (UCE), also known as junk email.
- If you receive junk e-mail,
 - Do not click any links in the message.
 - Do not reply to it in any way and add the sender's e-mail address to the Blocked Senders list.
- You should know that one can not receive a cash reward for forwarding messages or filling forms.

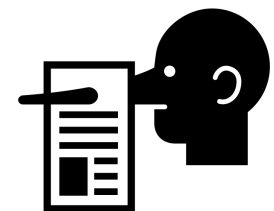


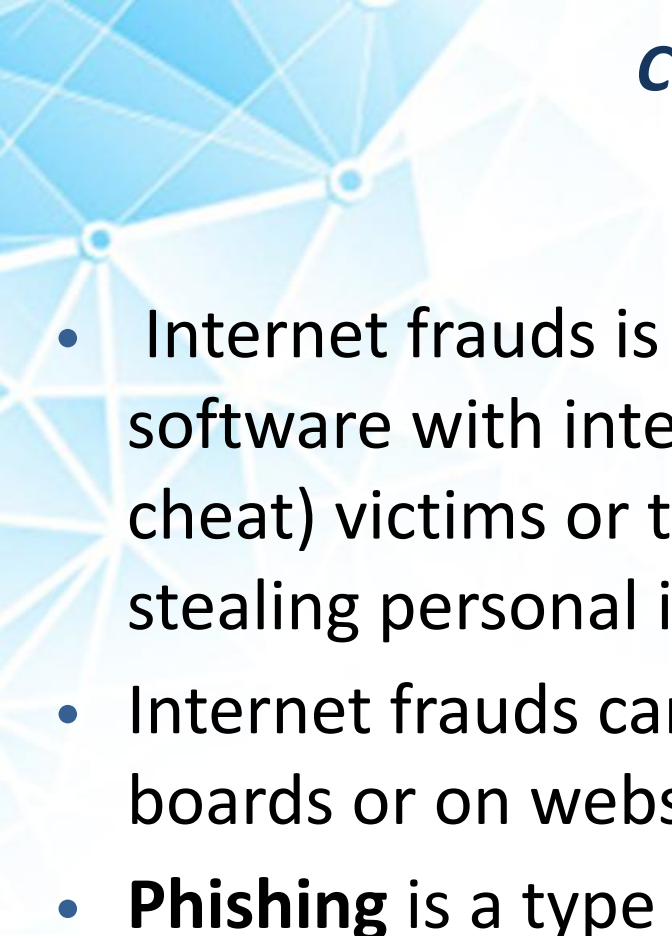
Malicious Email Content Distribution

COMPUTER SECURITY

Hoax

- **Hoaxes** are reports of non-existent viruses or incorrect confusing information.
- Usually they are emails which do some or all of the following:
 - Warn you that there is an undetectable, highly destructive new virus.
 - Ask you to avoid reading emails with a particular subject line , e.g. Join the Crew or Budweiser Frogs
 - Claim that the warnings was issued by a major software company, internet provider or government agency, e.g. IBM, Microsoft, AOL or the FCC.
 - Claim that a new virus can do something improbable, e.g. The ***moment of silence*** hoax says that “no program needs to be exchanged for a new computer to be infected. ”





COMPUTER SECURITY

Internet Frauds

- Internet frauds is the use of internet services or software with internet access to defraud (swindle or cheat) victims or to take advantage of them such as stealing personal information.
- Internet frauds can occur in chat rooms, e-mail, message boards or on websites.
- **Phishing** is a type of internet fraud.

COMPUTER SECURITY

Phishing

- **Phishing** is a form of Internet fraud that aims to steal valuable information such as credit cards, user IDs and passwords.

- **Citibank**

E-mail claims your [Citibank](#) ATM/Debit card PIN must be updated due to "a large number of identity theft attempts."

- **eBay**

E-mail claims auction site [eBay](#) is sending out suspension notices via e-mail and asking customers to verify their account information.

E-mail claims auction site [eBay](#) is sending out notices requesting that users update their account information.

- **FDIC**

E-mail claims the [FDIC](#) insurance on your bank account has been cancelled by the Department of Homeland Security for violations of the Patriot Act.

- **IRS**

E-mail pretends to be the [IRS](#) sending out e-mails directing taxpayers to a web form to use to obtain tax refunds.

COMPUTER SECURITY

Protection from Internet Frauds

- You can guard yourself while you are buying something from Internet by paying attention to general Internet fraud tips
 - Use a secure browser
 - Shop with companies you know
 - Keep your password(s) private
 - Do not use a password that you use for other areas in your life, such as your school login.
 - Pay by credit or charge card
 - Keep a record of purchase order and confirmation number of your purchases
 - Keep personal information private
 - Look for an online privacy policy

COMPUTER SECURITY

Firewalls

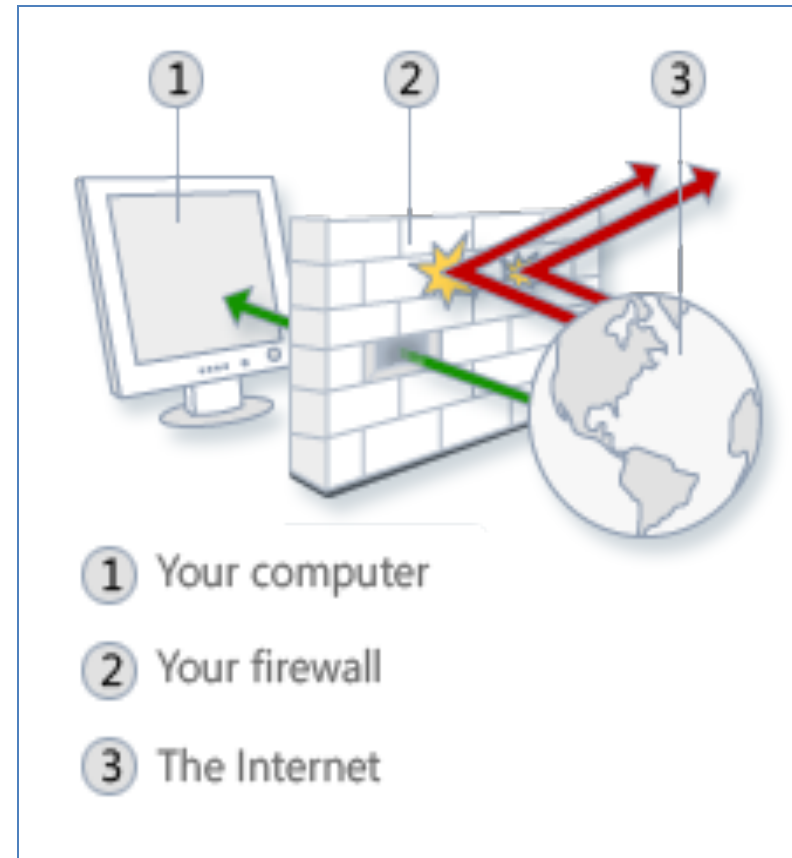
- A firewall is a software or hardware that checks information coming from the Internet or a network and then either turns it away or allows it to pass through to your computer, depending on your firewall settings.
- In this way, a firewall helps to prevent hackers and malicious software from gaining access to your computer.
- Windows Firewall is built into Windows and is turned on automatically.



COMPUTER SECURITY

Firewalls

- If you run a program such as an instant messaging program or a multiplayer network game that needs to receive information from the Internet or a network,
 - The firewall asks if you want to block or unblock (allow) the connection.
 - If you choose to unblock the connection, Windows Firewall creates an exception
 - The firewall won't bother you when that program needs to receive information in the future.



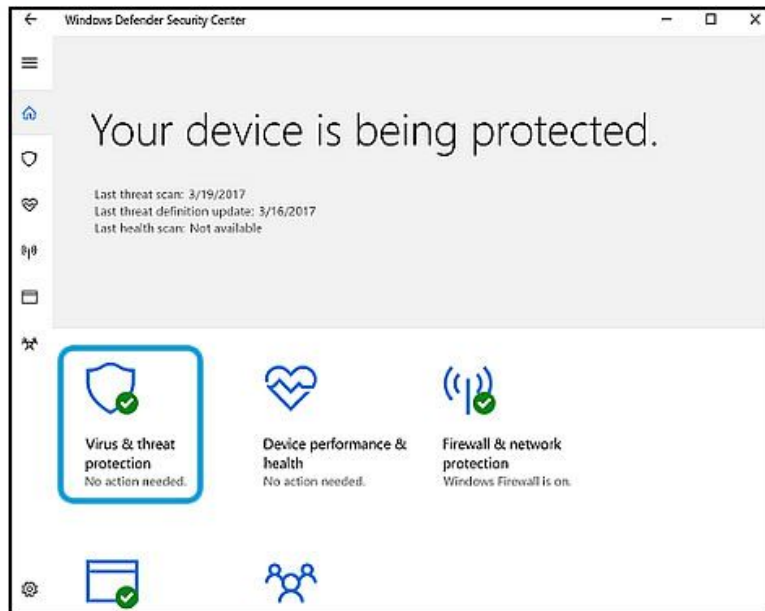
Functioning of the Firewalls

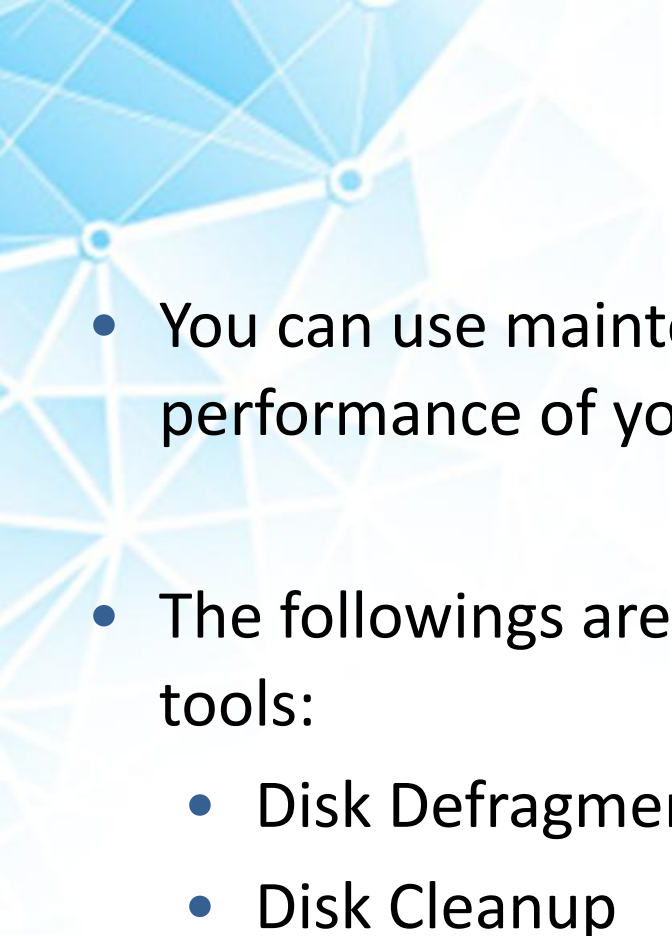
COMPUTER SECURITY

Firewalls

How to activate firewall on Windows

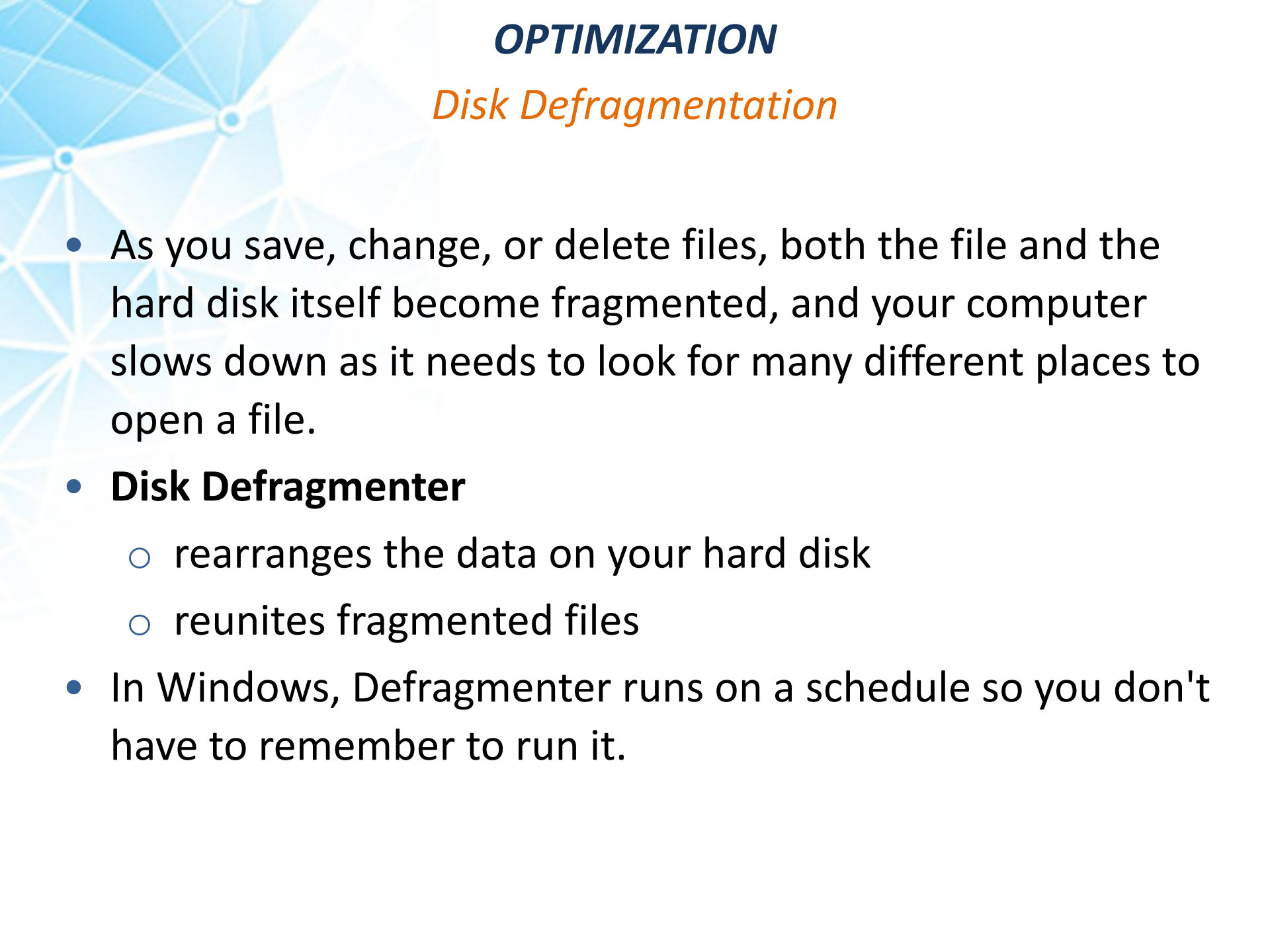
1. Go to Start and open Control Panel.
2. Open System and Security > Windows Defender Firewall.
3. Choose Customize Settings > Turn Windows Firewall on or off for domain, private, and public networks.





OPTIMIZATION

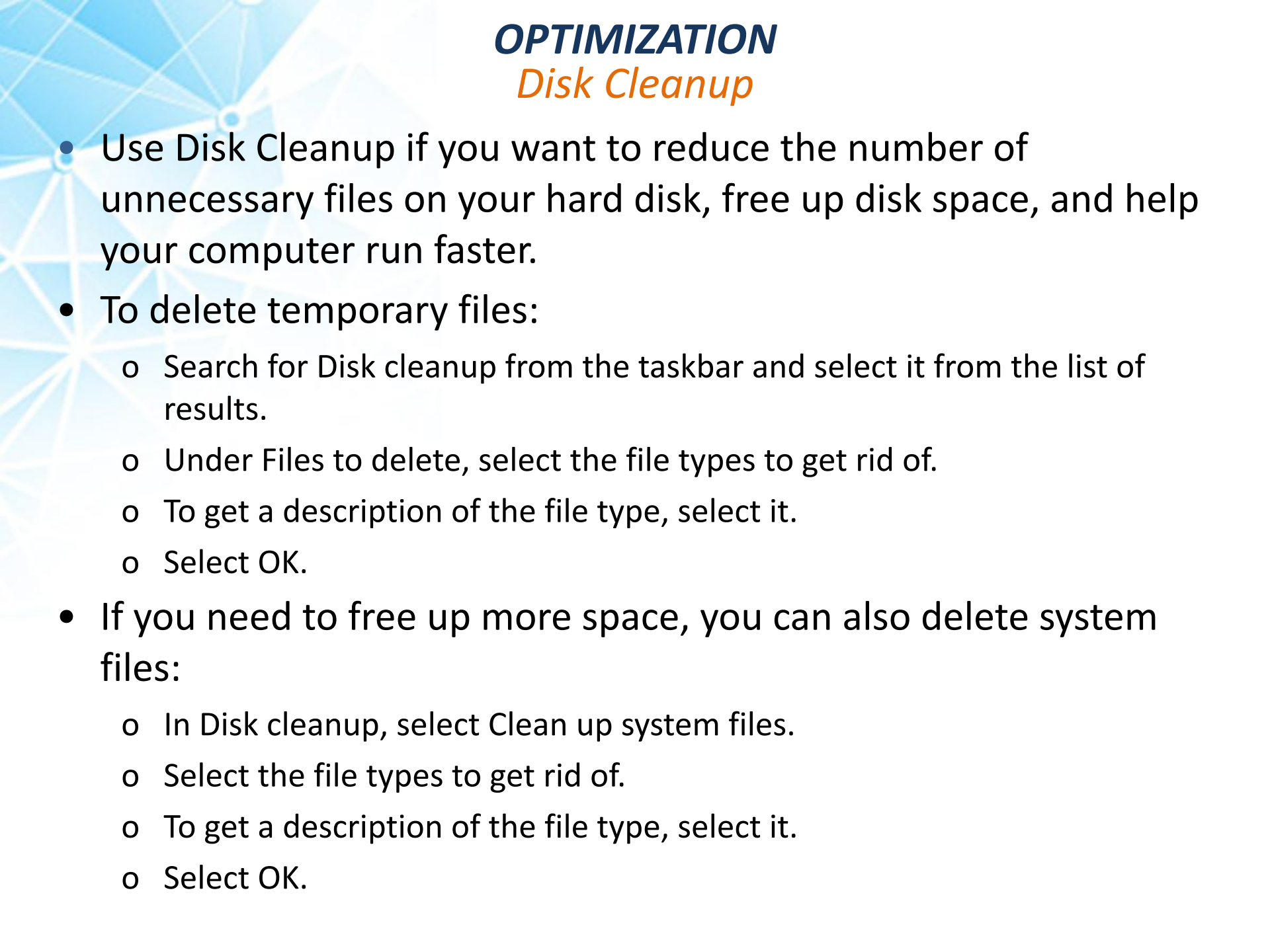
- You can use maintenance tools to optimize the performance of your computer.
- The followings are some example of disk management tools:
 - Disk Defragmentation
 - Disk Cleanup



OPTIMIZATION

Disk Defragmentation

- As you save, change, or delete files, both the file and the hard disk itself become fragmented, and your computer slows down as it needs to look for many different places to open a file.
- **Disk Defragmenter**
 - rearranges the data on your hard disk
 - reunites fragmented files
- In Windows, Defragmenter runs on a schedule so you don't have to remember to run it.



OPTIMIZATION

Disk Cleanup

- Use Disk Cleanup if you want to reduce the number of unnecessary files on your hard disk, free up disk space, and help your computer run faster.
- To delete temporary files:
 - o Search for Disk cleanup from the taskbar and select it from the list of results.
 - o Under Files to delete, select the file types to get rid of.
 - o To get a description of the file type, select it.
 - o Select OK.
- If you need to free up more space, you can also delete system files:
 - o In Disk cleanup, select Clean up system files.
 - o Select the file types to get rid of.
 - o To get a description of the file type, select it.
 - o Select OK.

What is GDPR? The General Data Protection Regulation is a strict privacy law regulating how personal data is collected and processed globally.

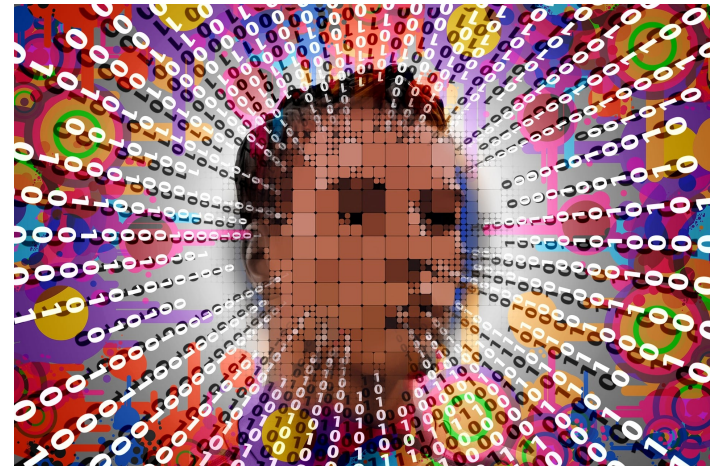


Explicit Consent: You cannot collect user data secretly. Users must clearly agree (opt-in) and know exactly how their data will be used.

Data Minimization: Only collect data that is absolutely necessary for your application to function. Do not hoard user information.

Right to be Forgotten: Users have the legal right to request a complete and permanent deletion of their personal data from your systems.

Why it matters for you: As future professionals, you must adopt "Privacy by Design," ensuring data protection is built



BASIC STEPS FOR TROUBLESHOOTING

Problem: PC Freeze

- If your PC freezes up and you want it to continue working, here are some steps to follow:
 - Press the **Ctrl, Alt** and **Delete** keys on your keyboard at the same time and choose the **Task Manager** button, this will bring up the Windows Task Manager.
 - On the **Applications Tab** look for the **Status** of the programs, if it says 'Not Responding', highlight that application and choose **End Task**. Choose **End Task** again when prompted.
 - Or you can try to **Switch To** a different task.
 - If this doesn't help, try restarting your computer by choosing the **Ctrl, Alt, Delete** keys again and choose the **Shutdown** button then choose **Restart**.

BASIC STEPS FOR TROUBLESHOOTING

Problem: Equipment Failure

- There are certain basic steps you can try when your hardware isn't working:
 - Is the power for the unit on?
 - Is the power surge strip powered on?
 - Are all cables tightly plugged in?
 - Try to power off and reboot all components (computer, router, printer, etc...)
 - Try to swap in an identical part (i.e. if the keyboard doesn't work try connecting a different keyboard to see if it works.)

SECURITY BEST PRACTICES

- Do not use public WiFi connections on airports, hotels, cafes, and restaurants for critical tasks such as online banking and online shopping.
- Instead use your own mobile connection.
- Always use secure connections (🔒 HTTPS) over non-secure connections (HTTP). Check address bar for the lock icon.
- Always update your operating system and applications to the latest versions.
- Do not leave your mobile phones and laptops unattended or unlocked.
- If you are using METU lab computers, do not forget to log off.
- **Always be careful, there is no absolute security!**





**METU
ODTÜ**



TEST YOURSELF

COMPUTER MAINTENANCE, SECURITY AND PROBLEM SOLVING

References

1. **How to password protect my documents with 7-ZIP?** <https://www.eduhk.hk/ocio/content/faq-how-password-protect-my-documents-7-zip> Last Visit: May, 2026
2. **Where is Control Panel?** <https://support.microsoft.com/en-gb/help/13764/windows-where-is-control-panel> Last Visit: May, 2026
3. **15 Outrageous Email Spam Statistics that Still Ring True in 2018** <https://www.propellercrm.com/blog/email-spam-statistics> Last Visit: May, 2026
4. **Disk cleanup in Windows 10** <https://support.microsoft.com/en-us/help/4026616/windows-10-disk-cleanup> Last Visit: May, 2026