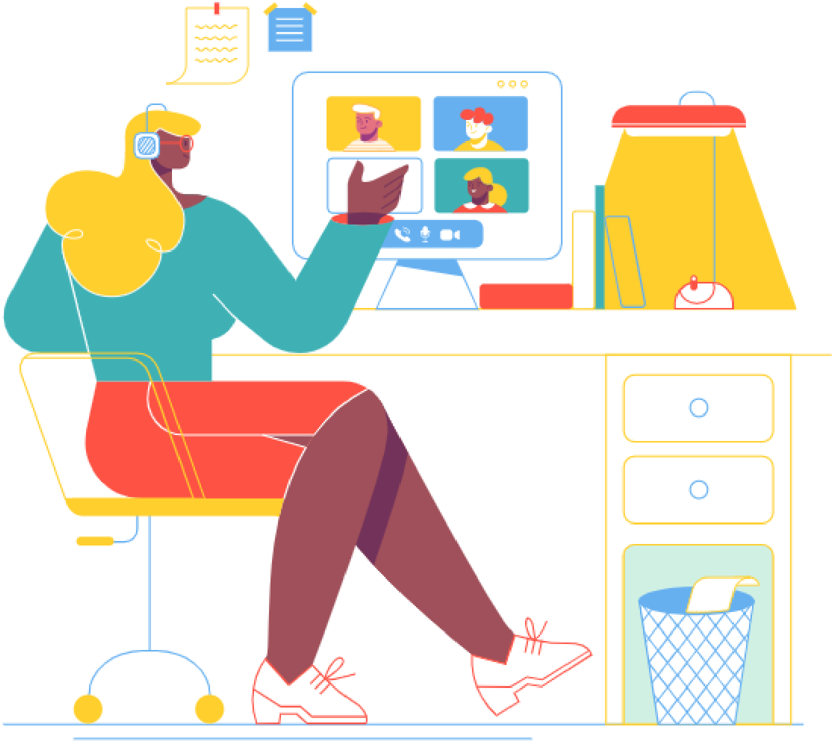


Introduction

to

COMPUTER SECURITY

Computer Security

The protection of computer systems and information from harm, theft, and unauthorized use.

It is the process of preventing and detecting unauthorized use of your computer system.

Types of Computer Security

Information Security is securing information from unauthorized access, modification & deletion

Application Security is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.

Computer Security means securing a standalone machine by keeping it updated and patched

Network Security is by securing both the software and hardware technologies

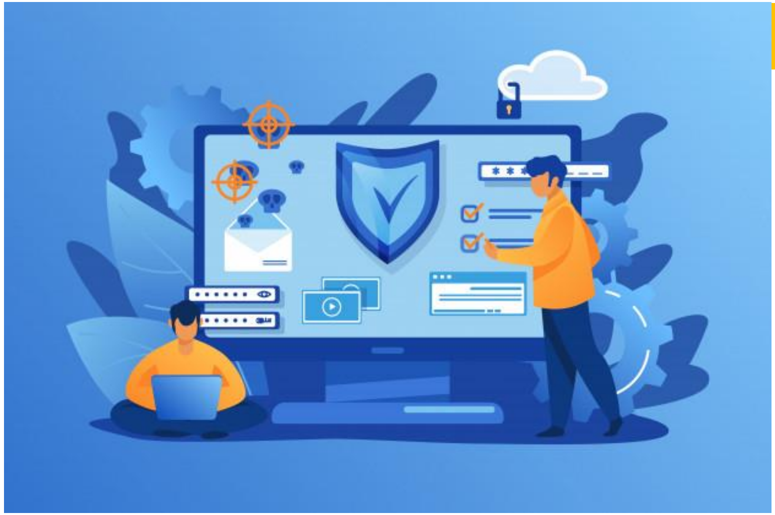
Cybersecurity is defined as protecting computer systems, which communicate over the computer networks

Components of computer system

Hardware, the physical part of the computer, like the system memory and disk drive

Firmware, permanent software that is etched into a hardware device’s nonvolatile memory and is mostly invisible to the user

Software, the programming that offers services, like operating system, word processor, internet browser to the user



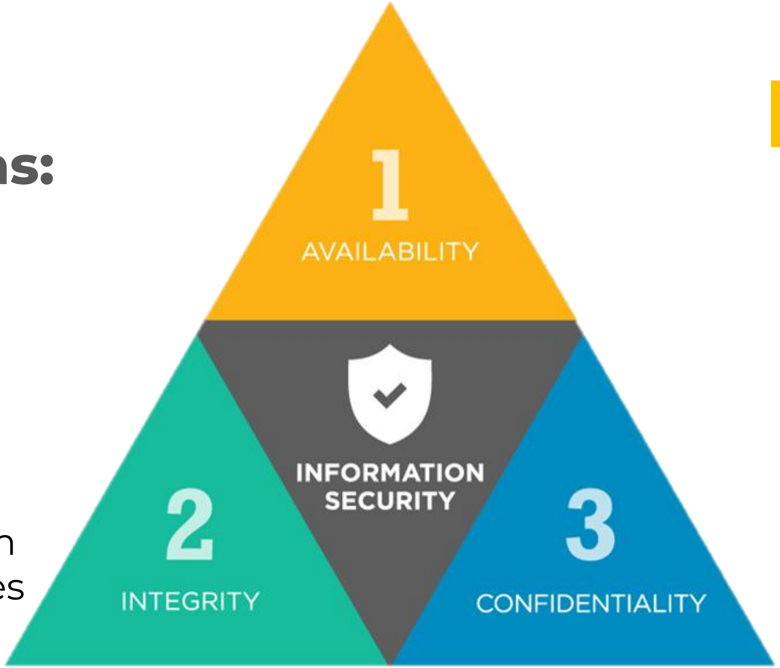
The CIA Triad

Computer security is mainly concerned with three main areas:

Confidentiality *is* ensuring that information is available only to the intended audience

Integrity *is* the consistency, accuracy, and trustworthiness of data over its entire life cycle.

Availability *is* protecting information from being modified by unauthorized parties



Computer Security Threats

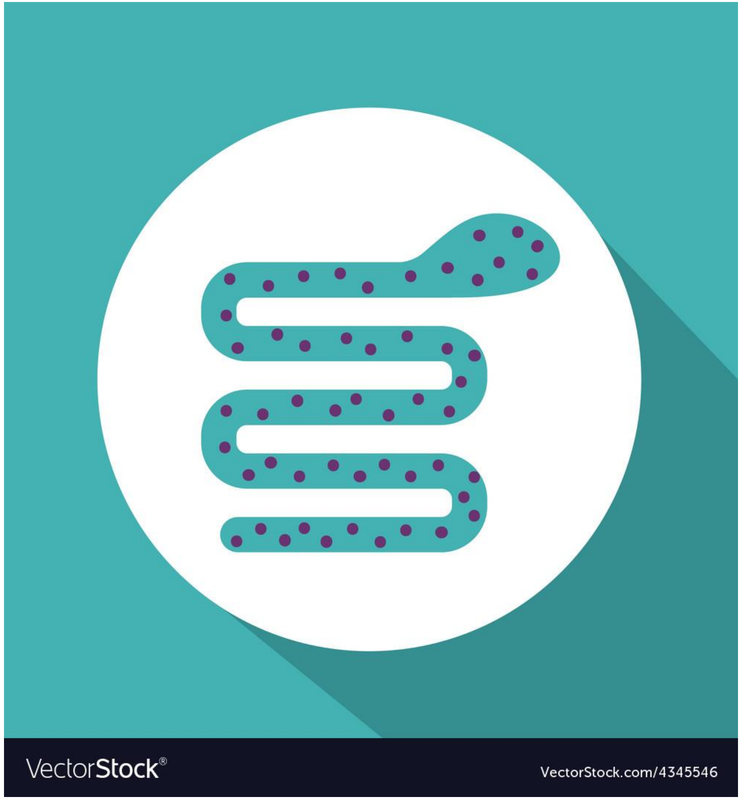
Computer security threats are possible dangers that can possibly hamper the normal functioning of your computer. In the present age, cyber threats are constantly increasing as the world is going digital. The most harmful types of computer security are:

Viruses

A computer virus is a malicious program which is loaded into the user's computer without user's knowledge. It replicates itself and infects the files and programs on the user's PC. The ultimate goal of a virus is to ensure that the victim's computer will never be able to operate properly or even at all.

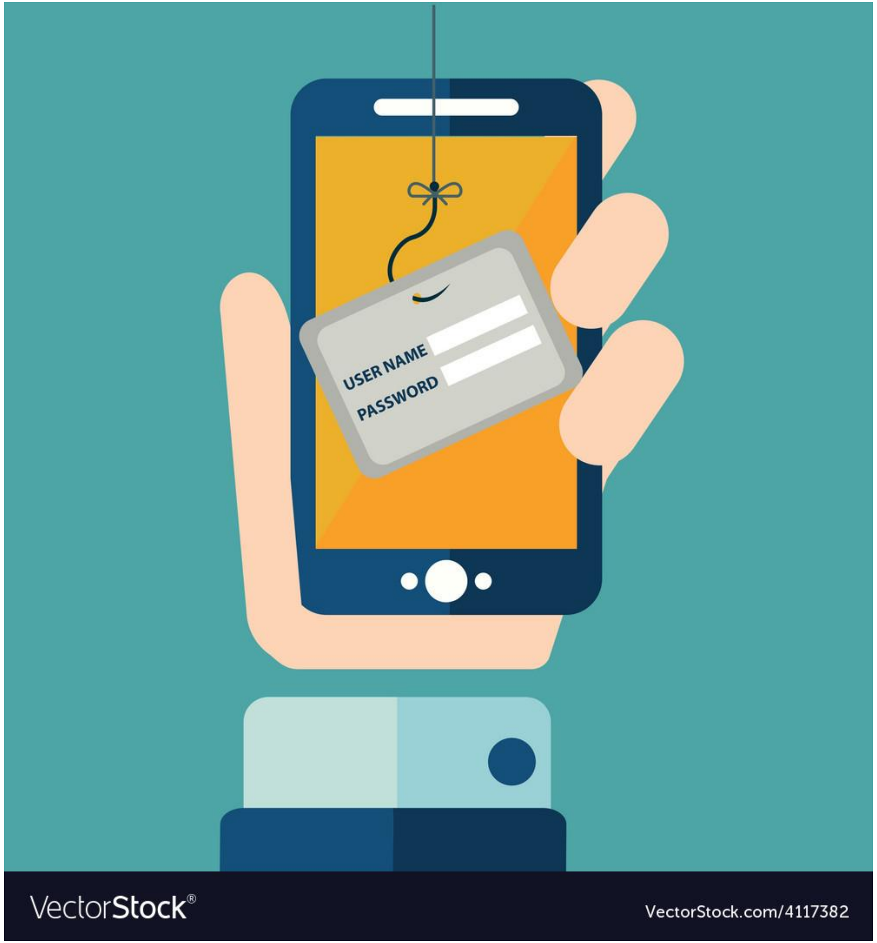
Computer Worm

A computer worm is a software program that can copy itself from one computer to another, without human interaction. The potential risk here is that it will use up your computer hard disk space because a worm can replicate in great volume and with great speed.



Phishing

Disguising as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Phishing in unfortunately very easy to execute. You are deluded into thinking it’s the legitimate mail and you may enter your personal information.



Rootkit

A rootkit is a computer program designed to provide continued privileged access to a computer while actively hiding its presence. Once a rootkit has been installed, the controller of the rootkit will be able to remotely execute files and change system configurations on the host machine.

Keylogger

Also known as a keystroke logger, keyloggers can track the real-time activity of a user on his computer.
It keeps a record of all the keystrokes made by user keyboard. Keylogger is also a very powerful threat to steal people’s login credential such as username and password.

Computer Security

Computer security threats are becoming relentlessly inventive these days. There is much need for one to arm oneself with information and resources to safeguard against these complex and growing computer security threats and stay safe online. Some preventive steps you can take include:

Computer Security Practices

- ✓ Secure your computer physically by:
  - ▪ **Installing reliable, reputable security and anti-virus software**
  - ▪ **Activating your firewall, because a firewall acts as a security guard between the internet and your local area network**
- ✓ Stay up-to-date on the latest software and news surrounding your devices and perform software updates as soon as they become available
- ✓ Avoid clicking on email attachments unless you know the source
- ✓ Change passwords regularly, using a unique combination of numbers, letters and case types
- ✓ Use the internet with caution and ignore pop-ups, drive-by downloads while surfing
- ✓ Taking the time to research the basic aspects of computer security and educate yourself on evolving cyber-threats
- ✓ Perform daily full system scans and create a periodic system backup schedule to ensure your data is retrievable should something happen to your computer.

Computer Ethics

Set of moral standards that govern the use of computers. It is society's views about the use of computers, both hardware and software. Privacy concerns, intellectual property rights and effects on the society are some of the common issues of computer ethics.

Privacy Concerns

Hacking – is unlawful intrusion into a computer or a network. A hacker can intrude through the security levels of a computer system or network and can acquire unauthorised access to other computers.

Malware – means malicious software which is created to impair a computer system. Common malware are viruses, spyware, worms and trojan horses. A virus can delete files from a hard drive while a spyware can collect data from a computer.

Privacy Concerns

Data Protection – also known as information privacy or data privacy is the process of safeguarding data which intends to influence a balance between individual privacy rights while still authorising data to be used for business purposes.

Anonymity – is a way of keeping a user's identity masked through various applications.

Intellectual Property Rights

Copyright – is a form of intellectual property that gives proprietary publication, distribution and usage rights for the author. This means that whatever idea the author created cannot be employed or disseminated by anyone else without the permission of the author.

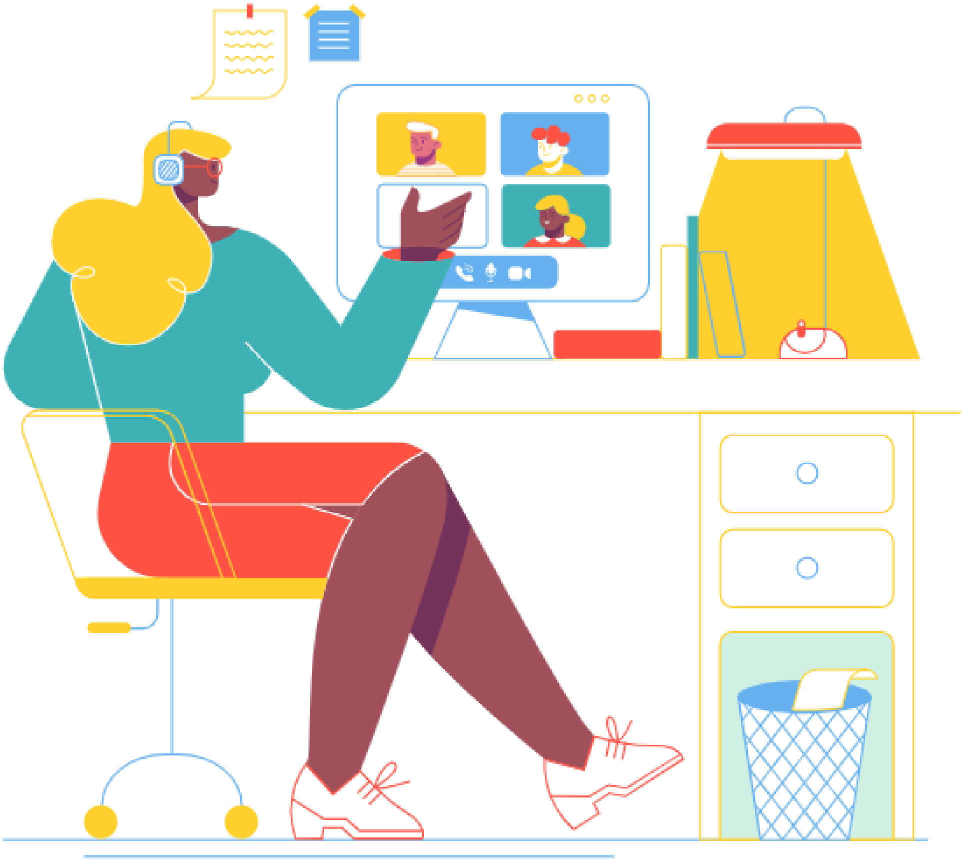
Plagiarism – is an act of copying and publishing another person's work without proper citation. It's like stealing someone else's work and releasing it as your own work.

Intellectual Property Rights

Cracking – is a way of breaking into a system by getting past the security features of the system. It’s a way of skipping the registration and authentication steps when installing a software.

Software License – allows the use of digital material by following the license agreement. Ownership remains with the original copyright owner, users are just granted licenses to use the material based on the agreement.

Effects of Computer on Society



Jobs – Some jobs have been abolished while some jobs have become simpler as computers have taken over companies and businesses. Things can now be done in just one click whereas before it takes multiple steps to perform a task. This change may be considered unethical as it limits the skills of the employees.

- **There are also ethical concerns on health and safety of employees getting sick from constant sitting, staring at computer screens and typing on the keyboard or clicking on the mouse.**

Environmental Impact – Environment has been affected by computers and the internet since so much time spent using computers increases energy usage which in turn increases the emission of greenhouse gases.

- **There are ways where we can save energy like limiting computer time and turning off the computer or putting on sleep mode when not in use. Buying energy efficient computers with Energy Star label can also help save the environment.**

Social Impact – Computers and the internet help people stay in touch with family and friends. Social media has been very popular nowadays.

- Computer gaming influenced society both positively and negatively. Positive effects are improved hand-eye coordination, stress relief and improved strategic thinking. Negative effects are addiction of gamers, isolation from the real world and exposure to violence.
- Computer technology helps the government in improving services to its citizens. Advanced database can hold huge data being collected and analysed by the government.
- Computer technology aids businesses by automating processes, reports and analysis.

The 10 Commandments of Computer Ethics

Ethics deals with placing a “**value**” on acts according to whether they are “**good**” or “**bad**”. Every society has its rules about whether certain acts are ethical or not. These rules have been established as a result of consensus in society and are often written into laws.

Rule #1: Thou shalt not use a computer to harm other people.

You should not program a computer to do dangerous things to people. For example, to program a robot to kill people, make viruses, or weapons of mass destruction. The programmer is responsible for the actions of his programs.

Rule #2: Thou shalt not interfere with other people's computer work.

Computer **viruses** are small programs that disrupt other people's computer work by destroying their files, taking huge amounts of computer time or memory, or by simply displaying annoying messages. Generating and consciously spreading computer viruses is unethical.

Rule #3: Thou shalt not snoop around in other people's computer files:

Reading other people’s e-mail messages is as bad as opening and reading their letters: This is invading their privacy. Obtaining other people’s non-public files should be judged the same way as breaking into their rooms and stealing their documents.

Rule #4) Thou shalt not use a computer to steal.

Using a computer to break into the accounts of a company or a bank and transferring money should be judged the same way as robbery. It is illegal and there are strict laws against it.

Rule #5: Thou shalt not use a computer to bear false witness.

The Internet can spread untruth as fast as it can spread truth. Putting out false "information" to the world is bad. For instance, spreading false rumors about a person or false propaganda about historical events is wrong.

Rule #6: Thou shalt not copy or use proprietary software for which you have not paid.

Software is an intellectual product. In that way, it is like a book: Obtaining illegal copies of copyrighted software is as bad as photocopying a copyrighted book. There are laws against both.

Rule #7: Thou shalt not use other people's computer resources. without authorization or proper compensation.

Multiuser systems use **user id’s** and **passwords** to enforce their memory and time allocations, and to safeguard information. You should not try to bypass this authorization system. **Hacking** a system to break and bypass the authorization is unethical.

Rule #8: Thou shalt not appropriate other people's intellectual output.

If you copy text or images from a website and post them on your own website it is a crime in most countries, and definitely not ethical. Why? You are causing irreparable damage to the creator of the content

Rule #9: Thou shalt think about the social consequences of the program you are writing or the system you are designing.

Do you write software that helps people to steal, kill, spy, gamble, or spread pornography? Please ask yourself why. Is there a way you can use your IT talents for good purposes?

Rule # 10: Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

References:

1. Archana Choudary. 2020. What is Computer Security? Introduction to Computer Security (July 2020). Retrieved August 31, 2020 from https://www.edureka.co/blog/what-is-computer-security/
2. Teach Computer Science. 2020. Computer Ethics. Retrieved from https://teachcomputerscience.com/computer-ethics/

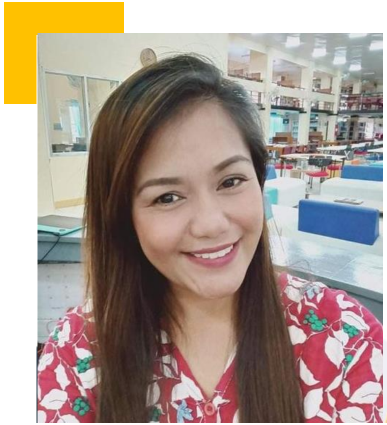
TUROTEAM

Kezia Velasco

INSTRUCTOR 1

Kenno Fortz

INSTUCTOR 1



Josefina Llagas

INSTRUCTOR 1

https://www.rasmussen.edu/degrees/technology/blog/it-vs-computer-science-degree-infographic/
https://thebestschools.org/careers/best-information-technology-jobs/