Web - Living in IT ERA

National Service Training Program (Xavier University - Ateneo de Cagayan)

MODULE 3: THE WEB AND THE INTERNET

Overview

Internet is defined as an information superhighway, to access information over the web. However, it can be defined in many ways, internet is a world-wide global system of interconnected computer networks.

Objectives

At the end of this lesson, the student should be able to:

- Explore the current breakthrough technologies and disruptive innovations that have emerged over the past few years.
- Identify and analyze various emerging technologies.
- Explore the evolution of the internet.
- Identify and understand the different uses of internet in today's generation.
- Discuss the fundamental terms and definitions used in the internet.

Lesson 1: The Web

The Web (World Wide Web) consists of information organized into Web pages containing text and graphic images. The world wide web is larger collection of interconnected documents or content. It contains hypertext links, or highlighted keywords and images that lead to related information. A collection of linked Web pages that has a common theme or focus is called a Web site. The main page that all of the pages on a particular Web site are organized around and link back to is called the site's home page. **Sir Timothy John Berners-Lee OM KBE FRS FREng FRSA FBCS, also known as TimBL, is an English engineer and computer scientist best known as the inventor of the World Wide Web.** He is a Professorial Fellow of Computer Science at the University of Oxford and a professor at the Massachusetts Institute of Technology.

A. Web 1.0 (Read Only Static Web)

It is an old internet that only allows people to read from the internet. First stage worldwide linking web pages and hyperlink. Web is use as "information portal". It uses table to positions and align elements on page.

- Most read only web. If focused on company's home pages.
- Dividing the world wide web into usable directories
- It means web is use as "Information Portal"
- It started with the simple idea "put content together"

Example of Web 1.0

- Mp3.com

- Home Page
- Directories
- Page Views
- HTML/Portals.

Disadvantages

- Read only web
- Limited user interaction
- Lack of standards

B. Web 2.0 (Read-write interactive web)

A term used to describe a new generation of Web services and applications with an increasing emphasis on human collaboration.

- It is a platform that gives users the possibility (liberty) to control their data.
- This is about user-generated content and the read-write web.
- People are consuming as well as contributing information through blogs or sites.
- Allows the user to interact with the page known as DYNAMIC PAGE; instead of just reading a page, the user may be able to comment or create a user account. Dynamic page refers to the web pages that are affected by user input or preference.
- Is focused on the ability for people to collaborate and share information online via social media, blogging and *Web*-based communities.

Example of Web 2.0 are the following:

A. Social Networking - is the use of Internet-based social media sites to stay connected with friends, family, colleagues, customers, or clients. Social networking can have a social purpose, a business purpose, or both, through sites such as:

Example

Facebook Twitter LinkedIn Google+ Pinterest Tumblr Instagram Page

B. Blogs - is a discussion or informational website published on the world wide web consisting of discrete, often informal diary-style text entries (posts). Posts are typically displayed in reverse chronological order, so that the most recent post appears first, at the top of the web page.

Example

Wordpress Blogger Tumbler

C. Wikis - is a hypertext publication collaboratively edited and managed by its own audience directly using a web browser. A typical wiki contains multiple pages for the subjects or scope of the project and may be either open to the public or limited to use within an organization for maintaining its internal knowledge base.

Example:

- Wikipedia
- Wikibooks
- Wikiversity
- Commons
- Wiktionary
- Wikiquote
- Wikivoyage
- Wikidata
- Wikinews
- Wikispecies
- MediaWiki

D. Video Sharing Sites - a website that lets people upload and share their video clips with the public at large or to invited guests.

Example:

- Youtube
- Facebook
- LinkedIn
- Flickr
- Photobucket LinkedIn
- Flickr
- Photobucket Twitter
- Veoh
- Dailymotion
- VimeoPRO
- Myspace.com Metacafe

Key Features of Web 2.0:

- **Folksonomy** – allows users to categorize and classify/arrange information using freely chosen keywords (e.g. tagging).
- **Rich User Interface** – content is dynamic and is responsive to user's input. An example would be a website that shows local content.
- **User Participation** – the owner of website is not the only one who is able to put content. Others are able to place a content on their own by means of comments, reviews, and evaluation.
- **Long Tail –** services are offered on demand rather than on a one-time purchase. This is synonymous to subscribing to a data plan that charges you for the amount of time you spent on Internet or a data plan that charges you for the amount of bandwidth you used.

C. Web 3.0: (Read-write intelligent web)

- Suggested name by John Markoff of the New York Times for the third generation of the web.
- In this generation, all the application on web or mobile will be upgraded with more features. It applies same principles as Web 2.0: two-way interaction.
- Web 3.0 will be more connected, open, and intelligent, with semantic web technologies, distributed databases, natural language processing, machine learning, machine reasoning and autonomous agents.
- Semantic Web - provides a framework that allows data to be shared and reuse to deliver web content specifically targeting the user.
- It is a web of data.
- Changing the web into a language that can be read and categorized by the system rather than humans.

Types of websites:

- **eCommerce Website**

is a website people can directly buy products from you've probably used a number of eCommerce websites before, most big brands and plenty of smaller ones

have one. Any website that includes a shopping cart and a way for you to provide credit card information to make a purchase falls into this category.

- **Business Website**
  is any website that's devoted to representing a specific business. It should be branded like the business (the same logo and positioning) and communicate the types of products and/or services the business offers.

- **Entertainment Website**
  If you think about your internet browsing habits, you can probably think of a few websites that you visit purely for entertainment purposes.

- **Portfolio Website**
  are sites devoted to showing examples of past work. Service providers who want to show potential clients the quality of the work they provide can use a portfolio website to collect some of the best samples of past work they've done. This type of website is simpler to build than a business website and more focused on a particular task: collecting work samples.

- **Media Website**
  collect news stories or other reporting. There's some overlap here with entertainment websites, but media websites are more likely to include reported pieces in addition to or instead of content meant purely for entertainment.

- **Brochure Website**
  are a simplified form of business websites. For businesses that know they need an online presence, but don't want to invest a lot into it (maybe you're confident you'll continue to get most of your business from other sources), a simple brochure site that includes just a few pages that lay out the basics of what you do and provide contact information may be enough for you.

- **Nonprofit Website**
  In the same way that businesses need websites to be their online presence, nonprofits do as well. A nonprofit website is the easiest way for many potential donors to make donations and will be the first place many people look to learn more about a nonprofit and determine if they want to support it.

- **Educational Website**
  The websites of educational institutions and those offering online courses fall into the category of educational websites. These websites have the primary goal of either providing educational materials to visitors or providing information on an educational institution to them.

- **Infopreneur Website**
  websites overlap a bit with business and eCommerce websites, but they represent a unique type of online business. Infopreneurs create and sell information products. That could be in the form of courses, tutorials, videos or eBooks.

- **Personal Website**

  Not all websites exist to make money in some way or another. Many people find value in creating personal websites to put their own thoughts out into the world. This category includes personal blogs, vlogs, and photo diaries people share with the world.

- **Web Portal**

  are often websites designed for internal purposes at a business, organization, or institution. They collect information in different formats from different sources into one place to make all relevant information accessible to the people who need to see it. They often involve a login and personalized views for different users that ensure the information that's accessible is most useful to their particular needs.

- **Wiki or Community Forum Website**

  Most people are familiar with wikis through the most famous example of one out there: Wikipedia. But wikis can be created on pretty much any subject you can imagine. A wiki is any website where various users are able to collaborate on content and all make their own tweaks and changes as they see fit. There are wikis for fan communities, for business resources, and for collecting valuable information sources.

Lesson 2: The Internet

The Internet or “net” (network of network) is the largest computer network in the world that connects billions of computer user. The word internet comes from combination between “interconnection” and “network”. Network is a collection of computers and devices connected via communication channels and transmission media allow to share resources (hardware, software, data, information). Generally, nobody owns the internet.

A. Brief History of Internet

ARPA – Advanced Research Project Agency January 2, 1969 – started an experimental computer network. Concept – No server, but equal importance/participation to every computer in the network. Even if, one or two node destroyed that will now affect the network. In 1982 the word internet started. 1986 – First “ free net” created in Case Western Reserve University 1991: US government allowed business agencies to connect to internet. Now all people can connect to the internet and improve their life and work quality. The internet support various aspects in our life. Vinton Gray Cerf ForMemRS is an American Internet pioneer and is recognized as one of "the fathers of the Internet", sharing this title with TCP/IP co-developer Bob Kahn.

B. Major Components of the Internet

1. **Servers** – is a computer program that provides service to another computer program and it’s user.

Types of Servers

Application Server – a program in computer that provides the business logic for an application program.
Web Server – a computer program that serves requested HTML pages or files.
Proxy Server – is a software that acts as an intermediary between an endpoint device, such as computer and another server from which a user is requesting.
Mail Server – is an application that receives incoming e-mail from local users and remote senders and forward outgoing e-mail for delivery
File Server – is a computer responsible for central storage and management of data files so that other computer on the same network can access them.
Policy Server – is a security component of a policy – based network that provides authorization services and facilities tracking and control of files.

2. **IP Address (Internet Protocol**) – is a numerical label assigned to each device. This provides identity to a network device.
3. **Browser** – is an application program that provides a way to look information on

the web.

Example of browsers: Google chrome, safari, internet explorer, opera, Mozilla

4. **Domain Name System (DNS)** – is the phonebook of internet. We access information online through domain names.

Example of DNS: www.facebook.com, www.pup.edu.ph,www.academia.edu

Name	Entity
.com	commercial
.org	organization
.net	network
.edu	education
.gov	National and State Government Agencies
.ph	Philippines
.au	Australia

5. **Internet Service Provide (ISP)** – is an organization that provides services for accessing, using or participating in the internet.

Two types of ISP:

National ISP – provided internet access to a specific geographic area.
Regional ISP – business that provides internet access in cities and towns nationwide.

Example of ISP: Sky Broadband, PLDT, Converge

C. Uses of Internet

- Look for information
- School works, jobs, and home purposes
- Send and receive electronic mail
- Video teleconferencing (video call, video chat)
- Buy and sell product
- Social networking
- Watch & post videos
- Games
- Take college courses
- Monitor home while away
- Financial transactions
- Download music and movies

D. Internet Terms and Definition

- **Internet -** A global network of thousands of computer networks linked by data lines and wireless systems.
- **Web** – a collection of billions of webpages that you can view with a web browser
- **Email** – the most common method of sending and receiving messages online
- **Social media** – websites and apps that allow people to share comments, photos, and videos
- **Online gaming** – games that allow people to play with and against each other over the Internet
- **Software updates** – operating system and application updates can typically downloaded from the Internet
- **HTML** - Hypertext Markup Language is a coding language used to tell a browser how to place pictures, text, multimedia and links to create a web page. When a user clicks on a link within a web page, that link, which is coded with HTML, links the user to a specific linked web page.
- **URL -** Uniform Resource Locator is a web address used to connect to a remote resource on the world wide web.(ex. https://www.microsoft.com/)
- **Bit -** is a single digit in the binary numbering system (base 2). For example: 1 is a bit or 0 is a bit.
- **Byte -** generally consists of eight bits.
- **Upload -** To upload is to transfer data from your computer to another computer.
- **Download -** To download is to transfer data from another computer to your computer.
- **HTTP -** is the acronym for Hypertext Transfer Protocol, the data communication standard of web pages. When a web page has this prefix, the links, text, and pictures should work correctly in a web browser.
- **HTTPS -** is the acronym for Hypertext Transfer Protocol Secure. This indicates that the web page has a special layer of encryption added to hide your personal information and passwords from others.
- **Router or router-modem** combination is the hardware device that acts as the traffic cop for network signals arriving at your home or business from your ISP. A router can be wired or wireless or both.
- **Encryption -** is the mathematical scrambling of data so that it is hidden from eavesdroppers. Encryption uses complex math formulas to turn private data into meaningless gobbledygook that only trusted readers can unscramble.
- **Web Bot** - A term that applies to programs/applets (macros and intelligent agents) used on the Internet. Such bots perform a repetitive function, such as posting messages to multiple newsgroups or doing searches for information.
- **Search Engine -** specialized software, such as Google and Yahoo, that lets www browser users search for information on the web by using keywords, phrases.

MODULE 4: THE NETIQUETTE AND THE COMPUTER ETHICS

Overview

The Netiquette and The Computer ethics discusses about the ethical issues in the field of computer. May it be in online or practicing in professional.

Objectives

At the end of this module, you should be able to:

- Discuss the importance of being a responsible netizen by following the rules of common courtesy online and the informal “rules of the road” of cyberspace.
- Discuss the difference between privacy and security.
- Explain various risks to internet privacy.

Lesson 1: Netiquette

What is Netiquette?

What is Netiquette? Simple stated, it’s **network etiquette** – that is the etiquette of cyberspace and “etiquette” means the forms of required by good breeding or prescribed by authority to be required in social or official life. In other words, **netiquette is a set of rules for behaving properly online**.

Netiquette, or network etiquette, is concerned with the "proper" way to communicate in an online environment. Consider the following "rules," adapted from Virginia Shea's the Core Rules of Netiquette, whenever you communicate in the virtual world.

When you use e-mail, instant messenger, video calls, or discussion boards to communicate with others online, please be sure to follow the rules of professional online communications known as netiquette. These rules will help you communicate with instructors, classmates, and potential employers more effectively and will help prevent misunderstandings.

REMEMBER THE GOLDEN RULE – Even though you may be interacting with a computer screen, you are communicating with a real person who will react to your message. Make a good impression - treat others with the same respect that you would like to receive and avoid confrontational or offensive language.

To help convey meaning when creating messages, it is sometimes acceptable to include appropriate emoticon symbols, such as a smiley face :) However, for professional communications these would be inappropriate.

AVOID SLANG, ACRONYMS, AND TEXT TALK – Communicating effectively in college and business environments requires the use of correct terminology, spelling, and grammar that can easily be understood. For example, use "your" instead of "ur".

AVOID "SCREAMING" IN TYPED MESSAGES – Typing an entire message using all capital letters is known as "screaming". It is distracting and generally frowned upon in professional environments. It is better to draw emphasis to selected words or phrases by: using italic or bold text; using a different color for text or background color; or denoting emphasis using special characters (Example: **Important**).

PROOFREAD YOUR MESSAGES BEFORE SENDING THEM – Proofreading your messages before you send them is a best practice for effective and efficient communication. Strive to make your communications concise and free of any:

- Spelling and grammar errors
- Confusing terms or phrases that could be misunderstood
- Errors of omission, such as missing content or recipients
- Errors in accuracy of information

EXERCISE GOOD JUDGMENT WHEN SHARING INFORMATION WITH OTHERS ONLINE – E-mail and chat messages that you send or receive are considered private and should not be forwarded or copied to others without gaining the consent of all involved participants. In general, messages posted to discussion boards and social media sites can be read by the public. You may never know who might read or share what you post. It is a good practice to always ask a post's author for permission before sharing a post with other parties.

- To protect your privacy and safety, do not share online any sensitive personal information such as:
    - Your home address or phone number
    - Personal conversations
    - Social plans, such as vacations
    - Financial information
    - Usernames, passwords, or hints
    - Anything personal that you would not want shared by others over the Internet

- If the material you share with others online came from another source, make every effort to gain permission from the original author or copyright holder. Copying someone else's work and passing it off as your own is plagiarism. It damages your reputation and could subject you to serious academic and legal consequences.

RESPECT DIVERSITY IN VIEWPOINTS - Be constructive and respectful when sharing opinions, beliefs, and criticisms, or responding to those of others in the conversation.

- When sharing a viewpoint that differs from someone else's, it is a best practice to first acknowledge the other person by briefly restating what he or she said, but in your own words. This lets the person know that you are listening and trying to understand them.
- When presenting an opinion or criticism, it is helpful to use phrases that

identify to whose point of view you are referring. If the opinion is yours, you can begin with the phrase “In my experience” or “In my opinion”. If it is a viewpoint of someone else, make sure you identify that in your message (Example: “According to Eric Ericson,” or “The president believes”).

Ten Commandments of Computer Ethics

a) Rule 1: Remember the Human When communicating electronically, whether through email, instant message, discussion post, text, or some other method, practice the Golden Rule: Do unto others as you would have others do unto you. Remember, your written words are read by real people, all deserving of respectful communication. Before you press "send" or "submit," ask yourself, "Would I be okay with this if someone else had written it?"

b) Rule 2: Adhere to the same standards of behavior online that you follow in real life While it can be argued that standards of behavior may be different in the virtual world, they certainly should not be lower. You should do your best to act within the laws and ethical manners of society whenever you inhabit "cyberspace." Would you behave rudely to someone face-to- face? On most occasions, no. Neither should you behave this way in the virtual world.

c) Rule 3: Know where you are in cyberspace "Netiquette varies from domain to domain." (Shea, 1994) Depending on where you are in the virtual world, the same written communication can be acceptable in one area, where it might be considered inappropriate in another. What you text to a friend may not be appropriate in an email to a classmate or colleague. Can you think of another example?

d) Rule 4: Respect other people's time and bandwidth Electronic communication takes time: time to read and time in which to respond. Most people today lead busy lives, just like you do, and don't have time to read or respond to frivolous emails or discussion posts. As a virtual world communicator, it is your responsibility to make sure that the time spent reading your words isn't wasted. Make your written communication meaningful and to the point, without extraneous text or superfluous graphics or attachments that may take forever to download.

e) Rule 5: Make yourself look good online. One of the best things about the virtual world is the lack of judgment associated with your physical appearance, sound of your voice, or the clothes you wear (unless you post a video of yourself singing Karaoke in a clown outfit.) You will, however, be judged by the quality of your writing, so keep the following tips in mind: Always check for spelling and grammar errors Know what you're talking about and state it clearly Be pleasant and polite

f) Rule 6: Share expert knowledge The Internet offers its users many benefits; one is the ease in which information can be shared or accessed and in fact, this "information sharing" capability is one of the reasons the Internet was founded. So, in the spirit of the Internet's "founding fathers," share what you know! When you post a question and receive intelligent answers, share the results with others. Are you an expert at something? Post resources and references about your subject matter. Recently expanded your knowledge about a subject that might be of interest to others? Share that as well.

g) Rule 7: Help keep flame wars under control What is meant by "flaming" and

"flame wars?" "Flaming is what people do when they express a strongly held opinion without holding back any emotion." (Shea, 1994). As an example, think of the kinds of passionate comments you might read on a sports blog. While "flaming" is not necessarily forbidden in virtual communication, "flame wars," when two or three people exchange angry posts between one another, must be controlled or the camaraderie of the group could be compromised. Don't feed the flames; extinguish them by guiding the discussion back to a more productive direction.

h) Rule 8: Respect other people's privacy Depending on what you are reading in the virtual world, be it an online class discussion forum, Facebook page, or an email, you may be exposed to some private or personal information that needs to be handled with care. Perhaps someone is sharing some medical news about a loved one or discussing a situation at work. What do you think would happen if this information "got into the wrong hands?" Embarrassment? Hurt feelings? Loss of a job? Just as you expect others to respect your privacy, so should you respect the privacy of others. Be sure to err on the side of caution when deciding to discuss or not to discuss virtual communication.

i) Rule 9: Don't abuse your power Just like in face-to-face situations, there are people in cyberspace who have more "power" than others. They have more expertise in technology or they have years of experience in a particular skill or subject matter. Maybe it's you who possesses all of this knowledge and power! Just remember: knowing more than others do or having more power than others may have does not give you the right to take advantage of anyone. Think of Rule 1: Remember the human.

j) Rule 10: Be forgiving of other people's mistakes Not everyone has the same amount of experience working in the virtual world. And not everyone knows the rules of netiquette. At some point, you will see a stupid question, read an unnecessarily long response, or encounter misspelled words; when this happens, practice kindness and forgiveness as you would hope someone would do if you had committed the same offense. If it's a minor "offense," you might want to let it slide. If you feel compelled to respond to a mistake, do so in a private email rather than a public forum.

Lesson 2: Cybercrimes

What is Cyber?

It is the Characteristics of the culture of computers, information, technology and virtual reality.

> **Cybercrime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming and child pornography) is used as a tool to commit an offense.
>
> **Cybercriminals** may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes.

Republic Act No. 10175 Cybercrime Prevention Act of 2012 is a law in the Philippines approved on September 12,2012 which aims to address legal issues concerning online interactions and internet.

Republic Act No. 10173 Data Privacy Act of 2012 is an act protecting individual personal information.

COMMON FORMS OF CYBERCRIMES:

a. Copyright

The exclusive legal right, given to an originator or an assignee to print, publish, perform, film, or record literary, artistic, or musical material, and to authorize others to do the same.

> **Copyright infringement** is the violation, piracy or theft of a copyright holder's exclusive rights through the unauthorized use of a copyrighted material or work.

b. Plagiarism

An act or instance of using or closely imitating the language and thoughts of another author without authorization.

CRIMINAL ACTIVITIES

a. Hacking

- Unauthorized access of or interference with computer systems, servers, or other information and communication systems
- Unauthorized access to corrupt, alter, steal, or destroy electronic data using computers or other information and communication systems without the computer or system owner's knowledge and consent
- The introduction of computer viruses resulting in the corruption, alteration, theft, or loss of such data
- Illegal Access
- Illegal Interception
- Data Interference
- System Interference
- Misuse of Devices
- Infection of IT Systems with Malware – if the act is committed against critical infrastructure of the Philippines the, penalty is between 12-20 years ***reclusion temporal***
- Six years up to twelve years of imprisonment **also known as *prison mayor.***

b. Computer-related forgery, fraud and/or identity theft

- An attempt to obtain sensitive information such as usernames, passwords, and credit card details and (indirectly money), often for malicious reasons.
- Phishing
- Pharming
- Spam
- Maximum of Php 200,000 fine or *prison mayor (6-12yrs)*

c. Electronic theft

- Illegal Downloading
- Obtaining files that you do not have the right to use from the internet.
- Digital Piracy
- Practice of illegally copying and selling digital music, video, computer software, etc.
- Copyright Infringement
- Penalty of Php 50,000 – 500, 000 and or *prison mayor*

d. Cyberbullying

- The use of electronic communication to bully a person, typically by sending a message of an intimidating or threatening nature.
- The Anti-Bullying Act of 2013 (RA 10627)

e. Cybersex

- Willful engagement, maintenance, control, or operation, directly or indirectly of any lascivious exhibition of sexual organs or sexual activity with the aid of a computer system for favor or consideration.
- There is a discussion on this matter if it involves "couples" or "people in relationship" who engage in cybersex.
- Penalty at least Php 200,000 and or prison mayor

f. Child Pornography

- Is a form of child sexual exploitation.

- Unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti- Child Pornography Act of 2009, committed through a computer system.
- Penalty of 12-20 years of imprisonment or reclusion temporal

g. Cyber Defamation

- Is an unprivileged false statement of fact which tends to harm the reputation of a person or company.
- Penalty of 6-12 years of imprisonment or prison mayor.

Lesson 3: Internet Threats

Hacking
Hacking is a term used to describe actions taken by someone to gain unauthorized access to a computer. The availability of information online on the tools, techniques, and malware makes it easier for even non-technical people to undertake malicious activities.
The process by which cyber criminals gain access to your computer.

What it can do:

- Find weaknesses (or pre-existing bugs) in your security settings and exploit them in order to access your information.
- Install a Trojan horse, providing a back door for hackers to enter and search for your information.

Malware
Malware is one of the more common ways to infiltrate or damage your computer. Malicious software that infects your computer, such as computer viruses, worms, Trojan horses, spyware, and adware.

What it can do:

- Intimidate you with scareware, which is usually a pop-up message that tells you your computer has a security problem or other false information.
- Reformat the hard drive of your computer causing you to lose all your information.
- Alter or delete files.
- Steal sensitive information.
- Send emails on your behalf.
- Take control of your computer and all the software running on it.

Pharming
Pharming is a common type of online fraud.
It means to **point you to a malicious and illegitimate website by redirecting the legitimate URL.** Even if the URL is entered correctly, it can still be redirected to a fake website.

What it can do:

- Convince you that the site is real and legitimate by spoofing or looking almost identical to the actual site down to the smallest details. You may enter your personal information and unknowingly give it to someone with malicious intent.

Phishing

Phishing is used most often by cyber criminals because it's easy to execute and can produce the results they're looking for with very little effort.

Fake emails, text messages and websites created to look like they're from authentic companies. They're sent by criminals to steal personal and financial information from you. **This is also known as "spoofing".**

What it does:

- Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action.
- Provides cyber criminals with your username and passwords so that they can access your accounts (your online bank account, shopping accounts, etc.) and steal your credit card numbers.

Ransomware

Ransomware is a type of malware that restricts access to your computer or your files and displays a message that demands payment in order for the restriction to be removed. The two most common means of infection appear to be phishing emails that contain malicious attachments and website pop-up advertisements.

What it can do:

- There are two common types of ransomware:
- Lockscreen ransomware: displays an image that prevents you from accessing your computer
- Encryption ransomware: encrypts files on your system's hard drive and sometimes on shared network drives, USB drives, external hard drives, and even some cloud storage drives, preventing you from opening them
- Ransomware will display a notification stating that your computer or data have been locked and demanding a payment be made for you to regain access. Sometimes the notification states that authorities have detected illegal activity on your computer, and that the payment is a fine to avoid prosecution.

What you can do:

- Do not pay the ransom. These threats are meant to scare and intimidate you, and they do not come from a law enforcement agency. Even if you submit payment, there is no guarantee that you will regain access to your system.
- If your computer has been infected (i.e. you are unable to access your computer or your files have been encrypted), contact a reputable computer technician or specialist to find out whether your computer can be repaired and your data retrieved.
- In order to lessen the impact of a ransomware infection, be sure to regularly back-up your data with a removable external storage drive. It's possible that your files might be irretrievable; having an up-to-date backup could be invaluable.

Spam

Spam is one of the more common methods of both sending information out and collecting it from unsuspecting people.

The mass distribution of unsolicited messages, advertising or pornography to addresses which can be easily found on the Internet through things like social networking sites, company websites and personal blogs.

What it can do:

- Annoy you with unwanted junk mail.
- Create a burden for communications service providers and businesses to filter electronic messages.
- Phish for your information by tricking you into following links or entering details with too-good- to-be-true offers and promotions.
- Provide a vehicle for malware, scams, fraud and threats to your privacy.

Spyware (Spyware & Adware)

Spyware and adware are often used by third parties to infiltrate your computer.

What it is:

Software that collects personal information about you without you knowing. They often come in the form of a 'free' download and are installed automatically with or without your consent. These are difficult to remove and can infect your computer with viruses.

What it can do:

- Collect information about you without you knowing about it and give it to third parties.
- Send your usernames, passwords, surfing habits, list of applications you've downloaded, settings, and even the version of your operating system to third parties.
- Change the way your computer runs without your knowledge.
- Take you to unwanted sites or inundate you with uncontrollable pop-up ads.

Trojan Horses

A Trojan horse may not be a term you're familiar with, but there's a good chance you or someone you know has been affected by one.

A malicious program that is disguised as, or embedded within, legitimate software. It is an executable file that will install itself and run automatically once it's downloaded.

What it can do:

- Delete your files.
- Use your computer to hack other computers.
- Watch you through your web cam.
- Log your keystrokes (such as a credit card number you entered in an online purchase).
- Record usernames, passwords and other personal information.

Viruses

Most people have heard of computer viruses, but not many know exactly what they are or what they do.

Malicious computer programs that are often sent as an email attachment or a download with the intent of infecting your computer, as well as the computers of everyone in your contact list. Just visiting a site can start an automatic download of a virus.

What they can do:

- Send spam.
- Provide criminals with access to your computer and contact lists.
- Scan and find personal information like passwords on your computer.
- Hijack your web browser.
- Disable your security settings.
- Display unwanted ads.
- When a program is running, the virus attached to it could infiltrate your hard drive and also spread to USB keys and external hard drives. Any attachment you create using this program and send to someone else could also infect them with the virus.

How will you know if your computer is infected?

Here are a few things to check for:

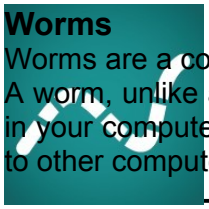
- It takes longer than usual for your computer to start up, it restarts on its own or doesn't start up at all.
- It takes a long time to launch a program.
- Files and data have disappeared.
- Your system and programs crash constantly.
- The homepage you set on your web browser is different (note that this could be caused by Adware that has been installed on your computer).
- Web pages are slow to load.
- Your computer screen looks distorted.
- Programs are running without your control.
- If you suspect a problem, make sure your security software is up to date and run it to check for infection. If nothing is found, or if you are unsure of what to do, seek technical help.

Wi-Fi Eavesdropping

WiFi eavesdropping is another method used by cyber criminals to capture personal information.
Virtual “listening in” on information that's shared over an unsecure (not encrypted) WiFi network.

What it can do:

- Potentially access your computer with the right equipment.
- Steal your personal information including logins and passwords.



Worms

Worms are a common threat to computers and the Internet as a whole.
A worm, unlike a virus, goes to work on its own without attaching itself to files or programs. It lives in your computer memory, doesn't damage or alter the hard drive and propagates by sending itself to other computers in a network – whether within

a company or the Internet itself.

What they can do:

- Spread to everyone in your contact list.
- Cause a tremendous amount of damage by shutting down parts of the Internet, wreaking havoc on an internal network and costing companies' enormous amounts of lost revenue.