PRIVACY, SECURITY & ETHICS

PRESENTED BY:

AMIRUL SYAFIQ BIN AMIRULLAH (A20EC0013)

NATASYA NADHIRA BT AHMAD NAZRAIN (A20EC0103)

HAFIZ SURYA NUGRAHA (A20EC0304)

LECTURER: DR. SARINA BT SULAIMAN

UTM UNIVERSITI TEKNOLOGI MALAYSIA

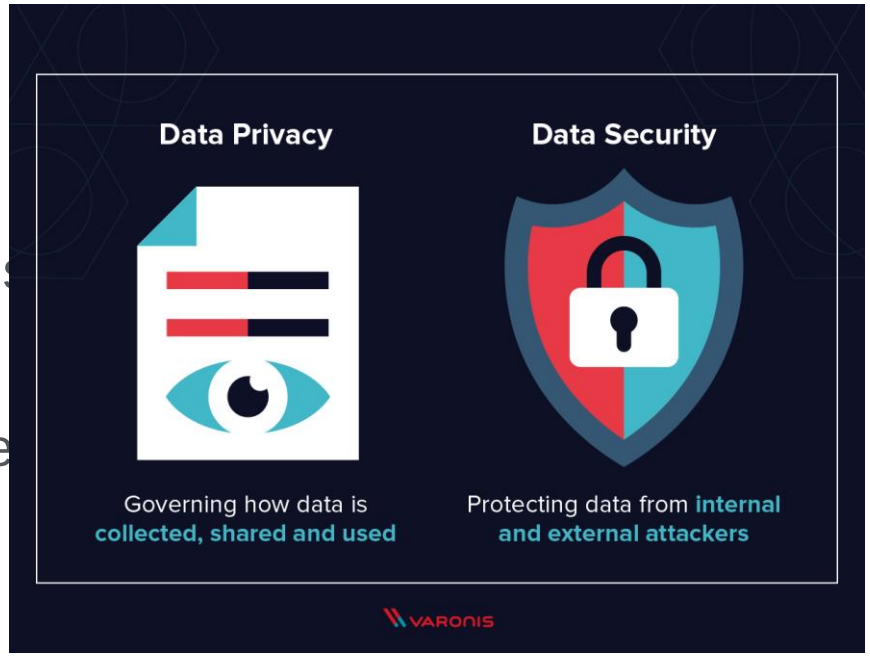
SCHOOL OF COMPUTING
Faculty of Engineering

Brief Introduction

As the rise of Technology and Information, a lot of issues regarding privacy, security and ethics.

Some of the concerns might be:

- Privacy – What type of information should you protect?
- Security – Is it safe to download programs from suspicious website?
- Ethics – What is the copyright issue when using someone else work without crediting?



It is important for us to stay safe while browsing and being ethical when on the web

What is Privacy?

- Concerns the collection and use of data about individuals
- Not a good practice to publicly state private info on the web
- Example: IC Number, Passport

Privacy Issues

1. Accuracy
   - Accuracy represents the legitimacy, precision and authenticity with which information is rendered.
   - When there is inaccuracy of information happen, it will be the responsibility of the data collector
2. Property

- The person or company that owns the right of the software
- Legal action taken if there is copyright issue

3. Access

- To the World Wide Web
- The privilege to obtain data or information from another source.

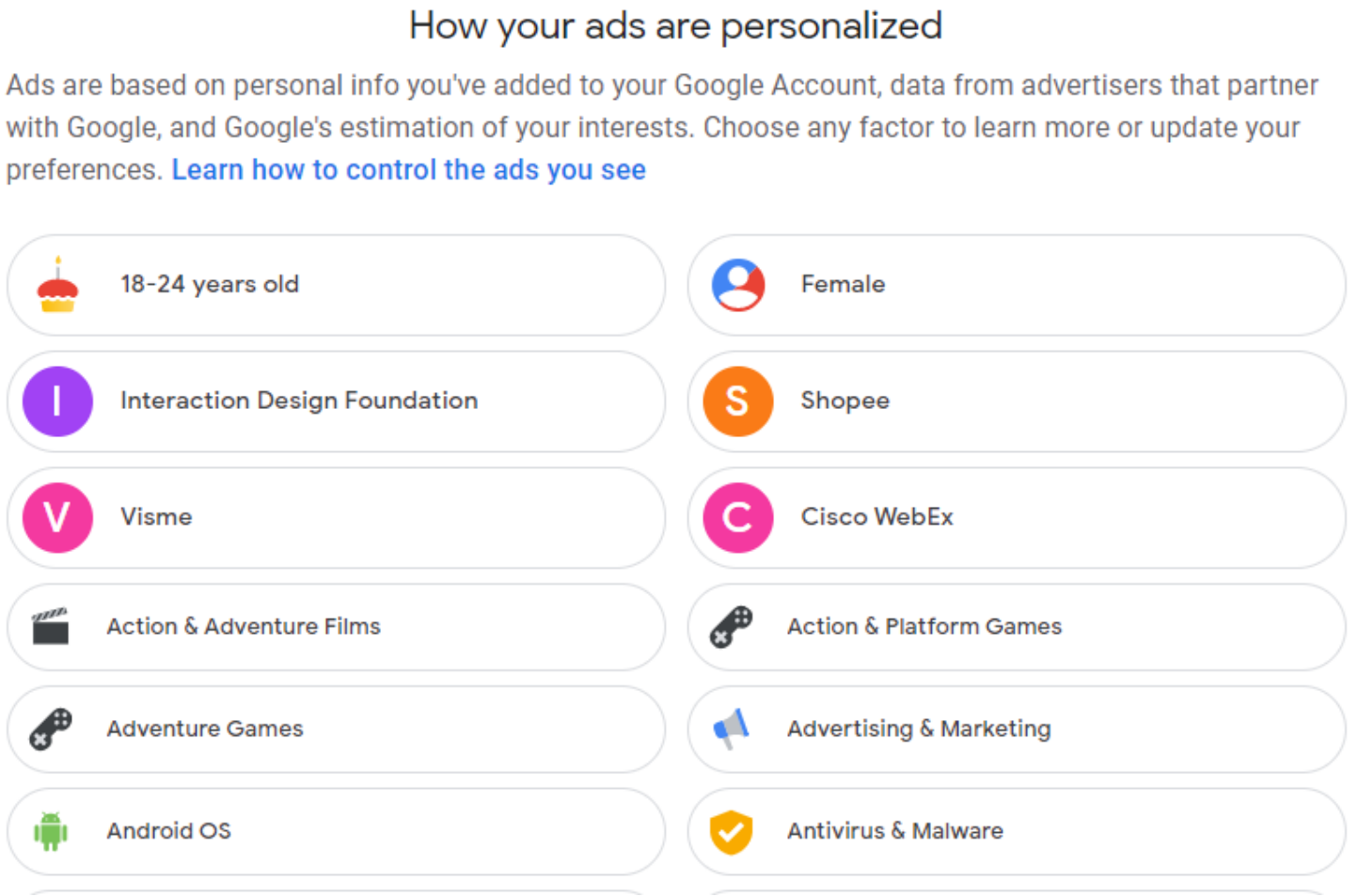
Large Database

- Compilation of our daily data information
- Large Databases are usually created and maintained by the firms that need to deal with a huge number of records that are about resources and people.
- Using large databases allow information brokers to collect large volume of detailed information about an individual's personal attributes, activities and behaviour through the electronic profiles.
- Data collectors include:
  1. Telephone companies (Reverse directory lists of calls we make)
  2. Supermarket scanners (What item we buy and the time of purchase)
  3. Search engines (What is the most visited sites)

- Information brokers or Information resellers use collected data to sell it to various customers such as marketing companies. They create e-profiles from the database and the marketing companies can market their product based on the bulk information provided.

- Impact on privacy:

  - This is still less danger to the privacy, some ill uses of this has been reported as well, the owners of the data many times spread that data without personal consent.
  - Some of the problems that were triggered after large databases involved are identity theft and spyware.

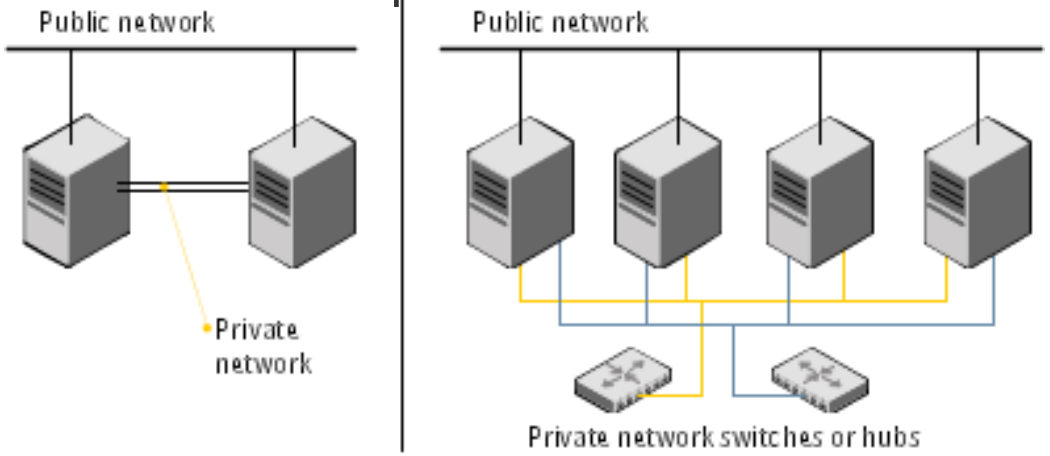


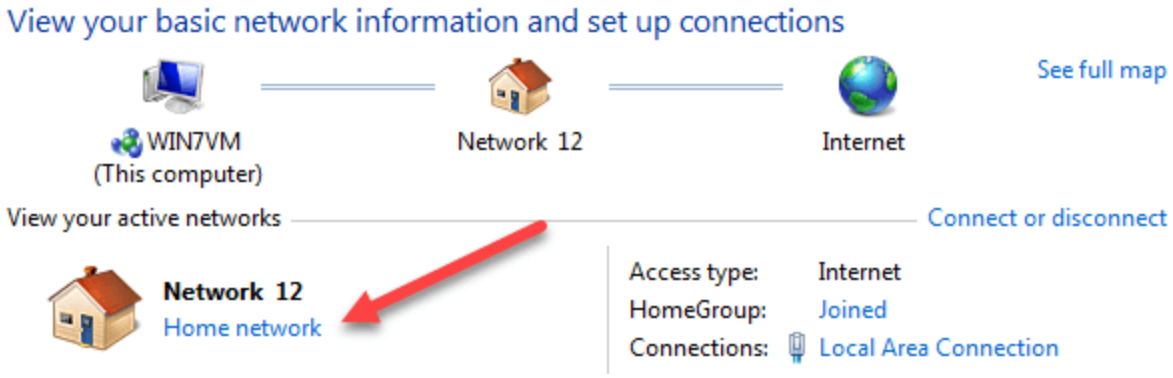
Example of Google Data Collection

Google makes an electronic profile for ads personalized purposes

Private Network

- Any connection within a specified network wherein restrictions are established to promote a secured environment. This type of network can be configured in such a way that devices outside the network cannot access it. Only a selected set of devices can access this type of network depending on the settings encoded in the network routers and access points.





❖ Impact on privacy:

- Employers can monitor e-mail legally
  - Because there is the same connection to the work (private) network
  - A proposed law could prohibit this type of electronic monitoring or at least require the employer to notify the employee first

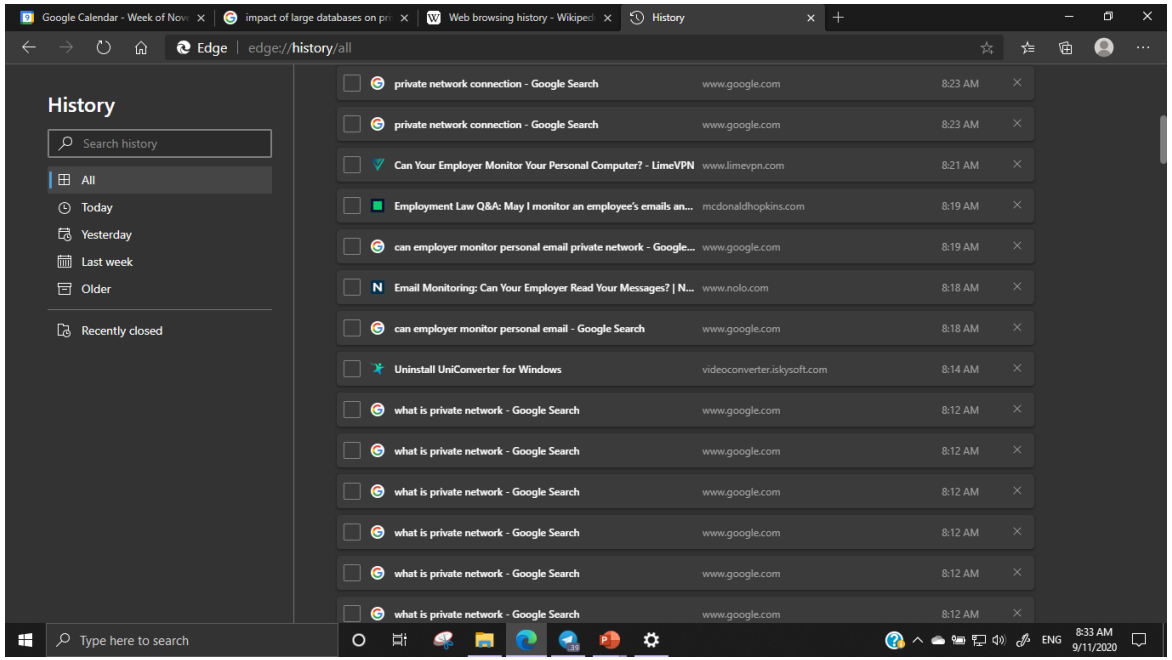
The Internet and the web

- Surfing online doesn't mean complete anonymity. People usually have self aware of how much information has been stored from the web.
- Critical Information is stored in these locations:

1. History files
2. Temporary Internet Files – also known as cache
3. Cookies
4. Privacy Mode

History files

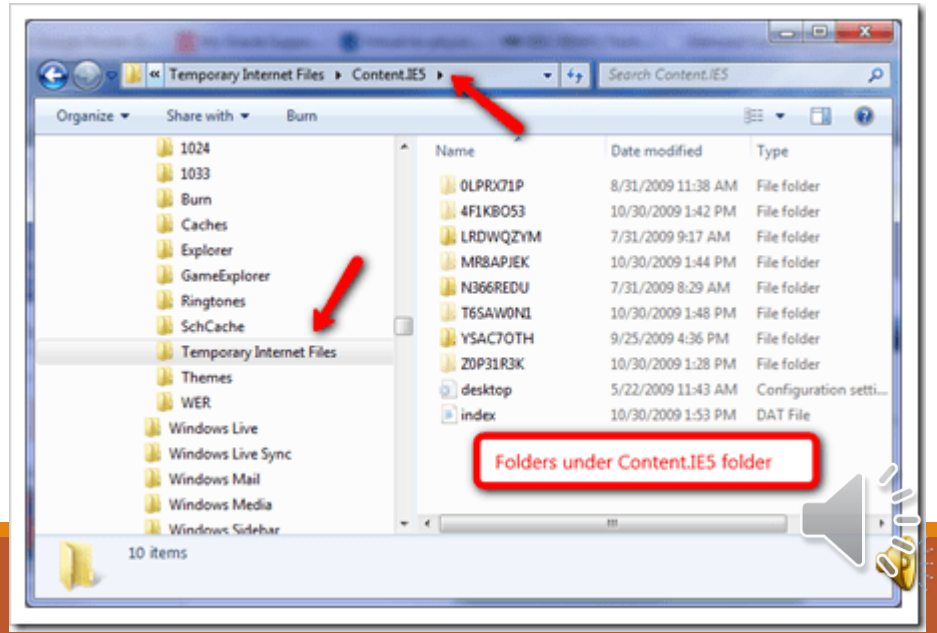
- Web browsing history is the list of web pages a user has visited, as well as associated data such as page title and time of visit. Web browsing history is usually collected by web browsers, and sometimes by third party organizations.
- Impact on privacy:
  - A shared computer can easily let other people snoop on the website that is recently or most visited



Temporary Internet Files

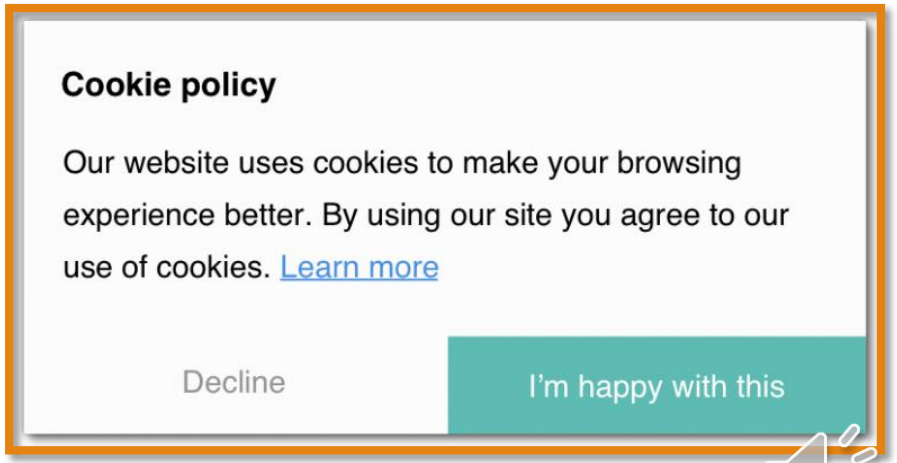
- In a user's computer, a collection of the most recent Web pages and files downloaded from the Web. The files are stored in a folder that acts as a cache so that subsequent requests are retrieved from the local hard disk. When the user requests the same page again, a request is sent to the website for the date of the file. If the date is newer than the one stored locally, the page is downloaded. If it is the same, the page is read locally.
- This mean that cache save files from visited website and it will reload after the next time the web is visited again.
- Impact on privacy:

• If the website that you visited using insecure temporary files can leave application and system data vulnerable to attacks.



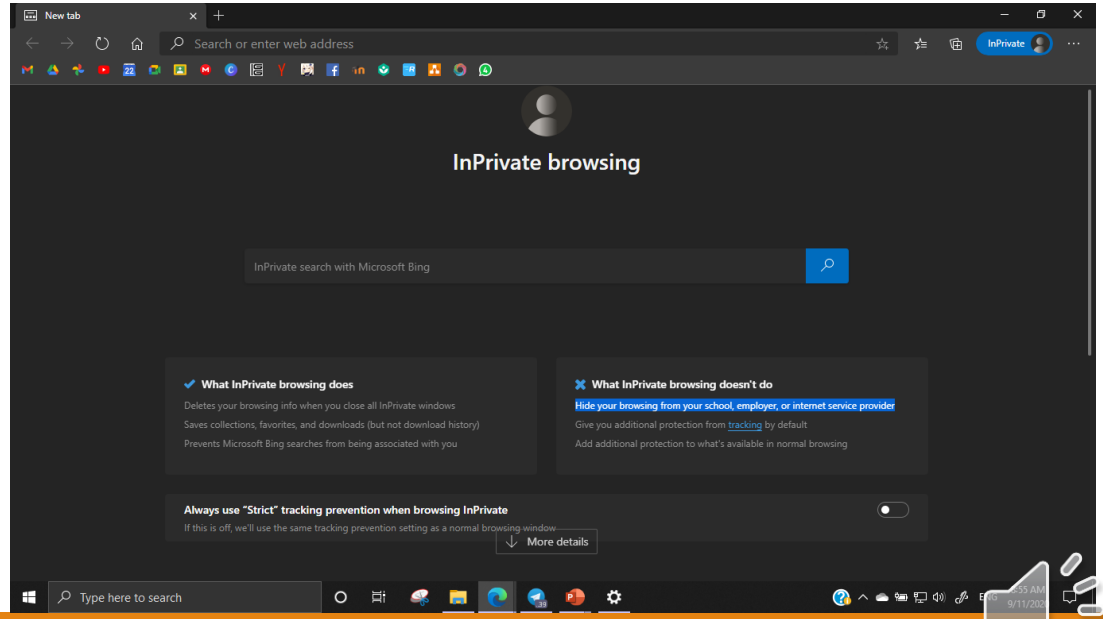
Cookies

- are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience.
- HTTP cookies are essential to the modern Internet but a vulnerability to your privacy. As a necessary part of web browsing, HTTP cookies help web developers give you more personal, convenient website visits.
- Impact on privacy:
  - Cookies let websites remember you, your website logins, shopping carts and more. But they can also be a treasure trove of private info for criminals to spy on.



Privacy Mode

- A mode that is offered from web browser to not record your browsing activity
- Example:
  - Incognito mode by Google
  - InPrivate mode by Microsoft edge
- Impact on privacy:
  - Private browsing is doesn't hide your browsing from your school, employer, or internet service provider



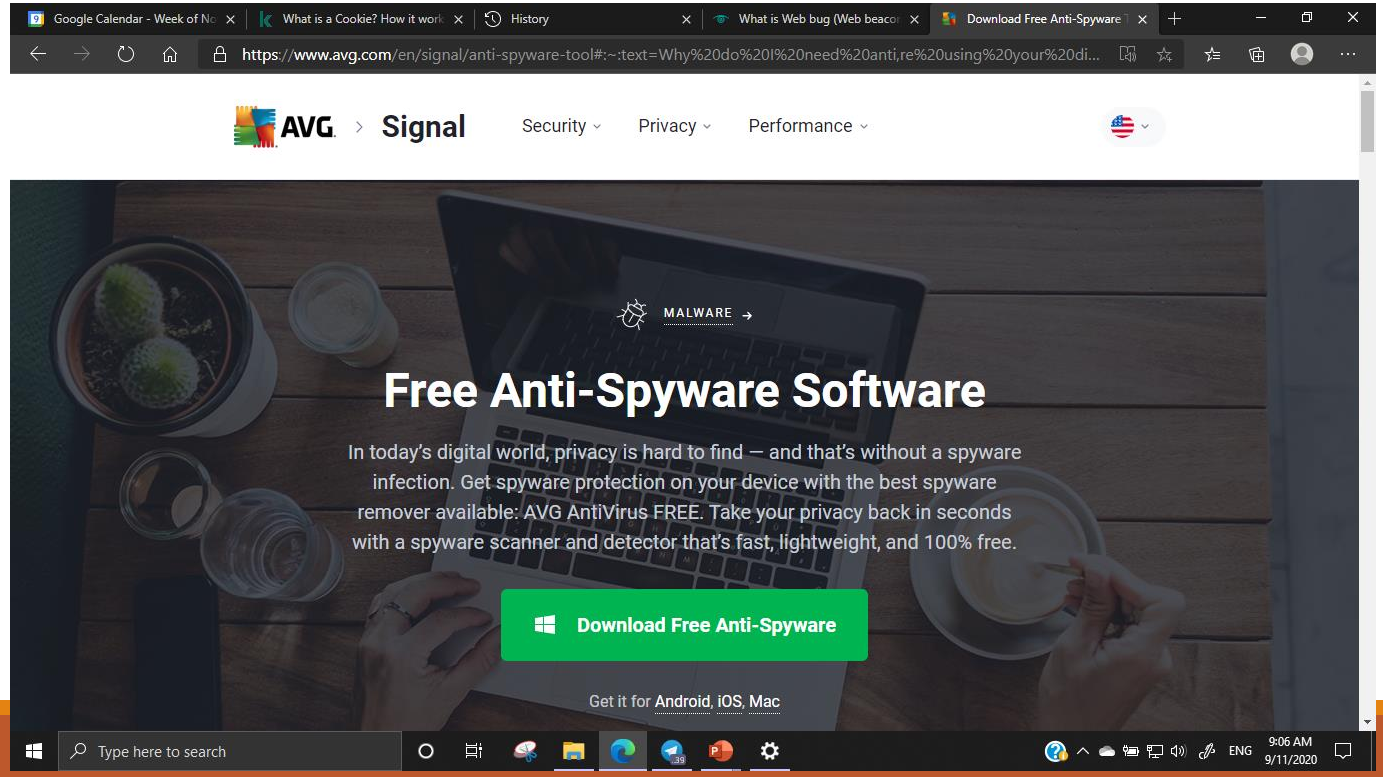
Privacy Threat

- Web bugs
  - Invisible images or HTML code hidden within an e-mail message or web page
  - When a user opens the message information is sent back to the source of the bug
  - Web bug can gather the following statistics: The IP address of the computer that fetched the Web bug, The type of browser that fetched the Web bug, a previously set cookie value.
- Spyware
  - software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive
- Computer Monitoring Software
  - Recording a user's activity on the computer. Computer monitoring programs are used to determine how much time an employee spends on various tasks as well as possible illicit activities. Programs can record keystrokes, chat and instant messaging conversations, links to websites and even take screen dumps and Webcam pictures, all of which can be stored locally or transmitted elsewhere.

Avoid Privacy Threat

Anti-Spyware programs

- Detect and remove privacy threats
- Ensures that no one will be able to eavesdrop on you while you're using your digital devices.



Online identity

- Internet identity, also online identity or internet persona, is a social identity that an Internet user establishes in online communities and websites. It can also be considered as an actively constructed presentation of oneself
- Social media has a big impact on online identity. People are posting more of their personal data information, such as their current location and activities, by themselves.
- Any data that has been shared public on the web will make it hard to hide it back into private as the web have searching and archive features.

Major Laws on privacy

1. Gramm-Leach-Bliley Act (GLB Act)
   - It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information.
   - Compliance with the GLBA protects consumer and customer records and will therefore help to build and strengthen consumer reliability and trust.

2. Health Insurance Portability and Accountability Act (HIPAA)
   - The HIPAA Privacy regulations require health care providers and organizations, as well as their business associates, to develop and follow procedures that ensure the confidentiality and security of protected health information when it is transferred, received, handled, or shared.

3. Family Educational Rights and Privacy Act (FERPA)
   - Itis a United States federal law that governs the access to educational information and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments

Technology and Information System

Security

What is Computer Security?

- **Computer security by definition is how much protection of a computer will be needed to guard itself from any unwanted threats such as :**

  - virus attack
  - computer theft
  - malware attack
  - preventing usage from unauthorized users

Hackers

- As technology advances in our modern times, hackers nowadays has also have become more clever and always come up with new ideas on how to exploit weakness in one's computer or server. With their expertise of computing and high social engineering skills, they can easily access one's content illegally with malicious intents such as

  - deletes, adding and altering any important files without permission
  - stealing one's sensitive personal data such as passwords and credit card numbers
  - damage the security of victim's computer

Hackers

- However, not all hackers are bad, unauthorized people. There are ethical hackers which is often called “White hat hackers”. These hackers uses their ability for the good of people.
- These authorized hackers are getting paid to work as security specialists with an attempt to find the security weaknesses.
- They penetrate testing and expose any security holes but only with the intention to improve the security later on
- Their method of hacking is the same as normal hackers but they do it only with the owner’s consent.

Computer Crime

- Computer crime, also known as cybercrime is a criminal offense from a computer and a network to further the illegal ends such as child pornography, human trafficking, committing any fraud intentions, stealing identities, stealing data and also to exploit privacy.

- Computer crimes can be done on malicious programs, Denial of Service or DoS, rogue wifi hotspots, data manipulation, identity theft, Online internet scams and cyberbullying.

Computer Crime

- **Malicious programs** – Programs that are filled with worms, viruses, and Trojan horses
- **Denial of Service (DoS)** – Causing computer or network to be lagged and forced to shut down or stop because of excessive requests of information.
- **Rogue wifi hotspots** – imitates real wifi networks, purposely set by hackers to gain an unauthorized access to one's personal information
- **Data manipulation** – fraudulent activity of modifying any digital documents and leaving prank messages
- **Identity theft** – uses another persons personal information to commit fraud activities
- **Online Internet scams** – Scams by the Internet to lure users into clicking their fraudulent website, usually by phishing method
- **Cyberbullying** – uses Internet to send contents with intentions to humiliate the person

Internet Scams

Types of Internet scams	Descriptions
Chain letter	Chain letter is an old-fashioned way of texting in which the recipient will have to send the text to a certain number of people. Then, the other people who received the text will have to share the text to another amount of people. Sometimes, the text threatens that bad things will happen if people do not share the texts.
Fraudulent auctions	There were payments about a merchandise but the merchandise has never been sent.

Internet Scams

Types of Internet scams	Descriptions
Vacation prizes	Scammers will usually prompt these “free vacation” trip on the Internet, claiming that “everyone is a winner”. The victim who tried this will then be asked to pay some money in order to claim the prize, some are even asking about their credit card number to claim the rewards of “free stay” which is not free at all.
Advanced fee loans	If a loan is approved, the scam lenders usually asked the victim to pay for a fee to an individual or wire the money before getting the cash loan.

Safety Regulations to Protect Computer Security

- Restricting Access

  Restricting and limiting access from unrecognized users by

  - **Two factor authentication verifications**

    Users will be given a verification link whenever users try to log in

  - **Password expiration and reuse**

    Users will have to reset their password according to the rule set by the admin every time they log in

  - **Time range access restriction**

    User who try to log in outside the time range specified will be prompted by a restriction notice

Safety Regulations to Protect Computer Security

- Security Automation

  Security automation is the machine-instructed program that is executed to programmatically detect and investigate cybercriminals and cyberthreats without human intervention

- It can detect any suspicious activities within its range

- Useful in handling repetitive tasks such as monitoring and managing security and act as an observant to avoid hackers penetrating the security

Encryption

- Encryption is also a way to improve computer security. It encrypts the encoding information, making it unreadable for regular users, except those who have the encryption key. It converts the plain text into other alternative, unreadable text known as "ciphertext". Typically, only authorized parties are allowed to decrypt the ciphertext back into plain text.

- Various encryption is available to use when the user likes to convey private information towards another user and remain anonymous.

  - **Email/file/website encryption**
  - **Virtual Private Network (VPN)**
  - **Wireless network encryption**

COMPUTER ETHICS

Ethics?

- Ethic Refers To The Standards And Rules
- That “Should” Be Followed And It Helps Us To Regulate Our Conduct In A Group Or With A Set Of Individuals.Since The Term Ethics Is A Relative Term, It Is Branched Under Philosophy, Which States How Users Of World Wide Web Should Make Decisions Regarding Their Conduct

Why Do We Need Ethics In Computing?

1.Respecting Ownership
-Not Stealing Other People Work

2.Respecting Privacy
-Reading Others Mails Or Files Without Permission

3.Respecting Property
-Act Of Tampering And Changing Electronic Information Is Considered As Vandalism And Disrespect For Other People Property

The Differences Between Ethics And Law

ETHICS

- Free To Follow
- No Punishment
- Universals
- Produce Ethical
- Computer User
- Immoral

LAW

- Must Follow
- Penalties,punishMent
- Depends On Coutry
- Prevent Misusing Of Computer
- Crime

Examples Of Ethics Computer Code Of Conducts Include:

- Sending Warning About Viruses To Other Computer About Computer Users
- Asking Permission Before Sending Any Business Advertisements To Others
- Using Information With Authorization

Copyright

Copyright Is A Legal Concept,enacted By Most Governments, Giving The Creator Of An Original Work Exclusive Rights To It,usually For A Limited Time.

HISTORY OF COPYRIGHT

Copyright Come About With The Invertion Of The Printing Press And With Winder Public Literacy.As A Legal Concept,its Origins In Britain Were From A Reaction To Printers Monopolies. Charles II Of England Was Concerned By The Unregulated Copying Of Books And Passed The Licensing Of The Press Act 1662 By Act Of Parliament.

Computer Ethical Hacking

- An ethical hacker is usually employed by an organization who trusts him or her attempt to penetrate networks and computer system,using the same methods as a hecker.for the purpose of finding and fixing computer security vulnerabilities.

Unauthorized Hacking

Unauthorized Hacking that Is Gaining Access To Computer Sytems Without Prior Authorization From The Owner is A Crime In Most Countries,but Peneration Testing Done By Request Of The Owner Of The Victim System Or Network Is Not A Certifield Ethical Hacker Has Obtained A Certification In How Look For The Weaknesses And Vulnerabilities In Target Systems And Uses The Same Knowledge And Tools As A Hacker

Conclusion

- As Technology Advances,computers Continue To Have A Greater Impact On Society,computer Ethics Promotes The Discussion Of How Much Influence Computers Should Have In Areas Such As Artifical Intelligence And Human Communication As The World Of Computer Evolves,computer Ethics Continues To Create Ethical Standars That Address New Issues Raised By New Technology.