LESSON 5: SETTINGS, SECURITY AND ACCESSIBILITY

In this section, you will learn about:

- **Home page settings** and how to customize your browser's starting page.
- **Blocking pop-ups** to enhance your browsing experience and reduce distractions.
- **Clearing cookies and cache** to improve website performance and privacy.
- **Data and website security** best practices, including strong passwords, secure connections, and avoiding phishing scams.
- **Malware** threats and how to protect your computer from viruses, spyware, and other malicious software.
- **Staying safe online** and protecting your personal information, including responsible social media use and online shopping practices.
- **Data protection** regulations and your rights as a user, such as GDPR and CCPA.
- **Web accessibility** principles and how to create inclusive websites that can be used by people with disabilities.

5.1. Home page settings

The home page is the website that appears every time you open your web browser. You can set the home page to any website you wish. Steps To change the home page are:

1. Press Alt and F together and then G to open the Settings tab.
2. Activate the search burton and in the search box, type “start-up”, and press Enter.
3. Use the down arrow keys to navigate or press letter H to navigate to theon startup level two heading.
4. Down arrow to the three radio buttons. Press the Spacebar on the Radio button of your choice. If you select either the New tab page or Continue where you left off radio button, you are done, and can press Control W or Control F4 to close the Settings tab.
5. Otherwise, continue Down arrowing to the use a specific page or set of pages radio button. Press the tab key to skip to the link to add a new page. If you press the down arrow key once, you land on the link to use current pages.

Adding a new page

- Activate the link to add a new page using the enter key.
- Navigate to the edit box for site URL and either type or paste your URL
- Navigate out of the edit box and activate the add or cancel burtons

Using current pages

While it is possible to select and unselect among open pages, this is more complicated and you may need sighted assistance.

Exit Chrome and reopen it to verify that your new Start page choice has registered.

If you choose the New tab option, when you open Chrome, you can immediately type in either a web address or a search term. Pressing Enter will then either open the page or generate a search results page with your default search engine. Because I like to be able to quickly access the Google search engine, I prefer the New Tab start page option. I prefer not to use the second Continue where you left off option because different Start pages open from session to session. I find this confusing. Choose the third Use current pages option if you want to always have the same Start page or pages. Some workplaces may prefer that your browser always opens on the organization's website. Or you may have several pages that you open when you begin working on your computer every day, and it is quicker to have them all appear on startup, rather than manually reload them every time. Whichever option you choose, it is easy to change later.

5.2. Blocking pop-ups

Pop-ups are windows that open automatically when you visit some websites. Such pop-ups may relate to gaming or explicit content, and are generally unnecessary. Some pop-ups may be dangerous to your computer; others are not harmful at all.

For screen reader users, they can be disorienting because the screen content site visitors were trying to access suddenly seems to disappear. Pressing the Escape key or a Close button may or may not remove the popup. In such cases, you may need to close the window for that web page by pressing Control F4, or exit the browser entirely by pressing Alt F4. Some websites require that pop-ups be allowed for that site to behave properly.

To block or allow pop ups for a specific website:

1. Navigate to that site, press Alt D to go to the Address bar and press Control C to copy the URL for that page.
2. Press Alt and F together and then G to get into the Settings Tab.
3. Activate the search burton and in the search box, type in "privacy", press the enter key to activate and then Tab to the main region
4. Press H several times to go to the Privacy and security heading, Down arrow to Site settings, and press Enter.
5. Under the Permissions heading, Down arrow to Pop-ups and redirects and press Enter.
6. Use the arrow keys and the space bar to change the default behavior. Choose between either sites can use pop-ups and use redirects or don't allow sites to use pop-ups and redirects.
7. You can also customize the behavior of specific sites. You can either add a site on the list of sites not allowed to use pop-ups and redirects or on the list of sites allowed to use pop-ups and redirects.
8. Navigate under each category and activate the add burton under your choice. Type the website or paste the URL. Don't forget to save if you are sure or cancel if you don't want the changes to take effect.

5.3. COOKIES AND CACHE

Cookies

Cookies are small pieces of data that are sent by websites to your browser when you are browsing. They have different functions, including recording of browsing activity, keeping you logged into websites, allow websites to greet you when you log in and more. Their use raises privacy concerns, but they can also make navigating the Web easier.

Cache

The Cache is a place on your PC where you can store data, so that the data does not need to be downloaded repeatedly. Most websites have many of the same elements on multiple pages. A company logo is one example. Because it is quicker to load an element from your hard disk than from the web, the Cache exists on your hard disk to store data that repeatedly appear on a site. This can speed up the responsiveness of your browser when opening previously visited web pages.

The first time you visit any page on a site, the browser downloads logos and various other items into the Cache. It then displays them as part of the page you are viewing. For each additional page you visit, if the same elements are displayed, they do not need to be downloaded again, thus saving time.

For various technical reasons unknown to most people, myself included, the Cache sometimes gets “confused.” There is probably a fancier term for this, but this conveys the message. A confused Cache can result in quirky behavior when downloading pages. Examples include partially loaded or badly formatted webpages, pages that update incorrectly or not at all, and incomplete pictures, among other things.

When your browser seems to be performing oddly, clearing the Cache is one of the first things to try.

Steps for clearing the cookies and Cache are similar among the browsers. Start by pressing the universal keystroke combination of Control Shift Delete. This opens a browsing history dialog box. Its title differs slightly between the browsers. There are several check boxes here for deleting other things beyond just the cookies and cache. These include browsing history etc.

After tabbing to the checkbox for clearing the Cache in Chrome and Edge, you will first hear “Cached images and files.” The amount of space that will be freed up is announced too. You are also told that “Some sites may load more slowly on your next visit.” Firefox only says “Cache.”

After checking the check box for clearing the Cache and any other history elements you want to clear, Tab to the OK, Clear data or Clear now Button and press Enter.

Please note that chrome gives you an option to delete your cache, cookies and browsing history for a specific time range. This combo box is usually at the top after activating the shortcut control, shift plus delete key.

5.4. SECURITY AND SAFETY Concepts

Maintaining data security is a vital for individuals, small businesses and large

corporations. Ensuring that data is kept secure is essential in avoiding disaster,

both personally and professionally, but unfortunately it can be a difficult task due

to malicious or unintentional behavior.

The following are some of the common terms related to data threats:

1. Data

A collection of facts, figures and statistics related to an object. Data can be processed to create useful information. Data is raw and unorganized facts and figures.

- Information

Information is data that is organized and processed to give it more meaning and context. While data is like pieces of a puzzle, information is like a completed puzzle that shows a final picture to the user.

- Cybercrime

An offence that involves using the Internet or a computer to carry out illegal activities, often for financial or personal gain. Examples include identity theft and social engineering.

- Hacking

Hacking involves using computer expertise to gain access to a computer system without authorization. The hacker may wish to tamper with programs and data on the computer, use the computer's resources, or just prove they can access the computer.

Key threats to data security:

a. System crashes and hard disk crashes a system or hard disk crash may cause physical damage to the storage media.

- Computer viruses which may delete or corrupt files.
    - Faulty disks and disk drives.
    - Physical damage to disks such as bad sectors.
    - Data lost by accidentally deleting or overwriting files.
    - Deletion by unauthorized users or hackers.
    - Destroyed by natural disasters, such as floods, fire or earthquakes.
    - Acts of terrorism, or war.
    - Accidental or malicious deletion by employees.

5.5. VALUE OF INFORMATION

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Reasons for Protecting Personal Information

Nowadays, more and more people are using the Internet and mobile devices for online shopping, banking, business, communication and other activities. Some companies rely on various cloud services and other web based services to run their day to day business.

Making information easier to access through the Internet also exposes businesses to some security issues. Hackers are able to take advantage of vulnerabilities in the transmission of data online to gain unauthorized access to systems and networks. There have been many reports of data breaches and identity theft in the past few years.

Cybercriminals often steal personal information such as banking records, credit card details, usernames and passwords for financial gain.

Personal Information is most often used by companies to identify and authorize users who transact business on their websites. For example, an online shopping site may have a record of a user's name, address, credit card details, etc.

Hackers may steal this information in order to impersonate a user and then conduct fraudulent and unauthorized transactions and other fraudulent activities. Without adequate security and protection of personal information, users are exposed to Internet based crimes such as identity theft and fraud and loss of privacy.

Companies which do not protect their user's personal information may lose customers' trust - and their business.

Reasons for Protecting Commercially Sensitive Information

Commercially sensitive information is any information owned by a company that could cause harm if it is lost, misused, stolen or altered in any way.

The following are examples of information that may be classified as being commercially sensitive:

1. Financial statements such as balance sheets, cash flow, income statements or equity statements.
2. Information such as lists of current and past clients.
3. Trade secrets such as designs, formulas, production processes etc.
4. Information about new products, marketing strategies or patent information.

Commercially sensitive information must be protected to prevent:

- Theft of private and confidential company information – company information could be stolen by corporate spies, social engineering or hacking. The data may be passed on to the company's competitors to the disadvantage of the owner of the information.
- Accidental loss of data – users may mistakenly delete or alter sensitive data. Storage media or mobile devices containing sensitive information could be misplaced.
- Fraudulent use of company data – such as client information and credit details.
- Corporate sabotage – some competitors may use information to sabotage your business.

5.6. Protecting yourself online

There are a range of measures that you can take to protect yourself when you are online.

1. Purchase from Secure Reputable Websites.
   When shopping online, take steps to check the security and reputation of a web site. For example, is the web site linked to an established business that has a physical presence? Are there independent reviews of the web site? If you cannot answer yes to these questions, maybe you should reconsider using the web site. You should also check that the Internet connection is secure before you make a payment. Avoid unnecessary disclosure of personal and financial information.
2. Do not give any personal or financial information over the Internet if the website is not secure.
   Even if the connection is secure, you should only provide personal and financial information if it is necessary to make a purchase. In addition, you should be very cautious about providing personal and financial information in other contexts, for example when communication via e-mail or instant messaging. If you are chatting on a discussion board or via instant messaging with someone you do not know personally, use a nickname instead of your real name. Be wary of strangers who may be interested in getting you to reveal personal information that they might seek to misuse.
3. Log off from websites. It's important that you remember to log out from any website that you have logged in to when you have finished browsing, especially if you are on a computer or device to which other people have access. If you do not log out, other people may gain access to your personal or financial information, or may impersonate you.

5.7. PERSONAL SECURITY

Social Engineering

Social engineering is a way to manipulate or influence people with the goal to illegally obtain sensitive data (for example, passwords or credit card information).

Social engineers research and learn about the personal environment of their target and fake their identity to obtain confidential information from the victim. In most cases, they infiltrate third-party computer systems to spy on sensitive data.

Methods of Social Engineering

- Phone calls

One of the most common methods social engineers use in their attacks is conducted via the phone. The attacker may impersonate a person of authority, a person representing a person of authority or a service provider to extract information from an unsuspecting user. For example, a person claiming to be the CEO of the company calls someone on the help desk, requesting for his password, which he claims to have forgotten.

- Phishing

A type of social engineering attack wherein the perpetrator sends an e-mail that appears to come from a legitimate source for example, a bank.

The e-mail usually requests for verification of information, sometimes warning of dire consequences if the recipient fails to comply. A phishing e-mail usually includes links to fraudulent web pages which are made to look very similar to legitimate web pages, including logos and content.

- Shoulder Surfing

This includes direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, ATM pins and security codes.

- Identity theft

This is a situation when someone deliberately impersonates and uses another person's identity. This is usually done for financial gain or to obtain credit and/or other benefits using someone else's name: for example, when someone uses another person's identity to obtain a driver's license. This type of fraud could have a devastating effect on the person whose identity has been assumed.

An initial implication of identity theft is the amount of time and money needed to re-establish your identity and credit history and to clear your name.

Methods of Identity Theft

- Information Diving

Also known as Dumpster Diving, it is a method of obtaining personal or private information by digging through a dumpster or trash bin for discarded documents or material such as utility bills or credit card statements.

- Skimming

Identity thieves use skimming as a method of capturing a victim's personal data by using a small electronic device. A skimmer is a device that is usually attached to an ATM machine's card slot. A victim may unwittingly slide his card into the skimmer, which then reads and stores all the information from the card's magnetic strip.

- Pretexting

This involves creating and using an invented scenario (the pretext) to engage a targeted victim. The pretext increases the chance the victim will revel information or perform actions that would be unlikely in ordinary circumstances – for example, someone pretending to be from MTN or Airtel money might persuade you to share your password with them.

5.8. MALWARE

Malware is malicious software that is designed to install itself on a computer or device without the owner’s consent. It is used as an umbrella term to describe the

following types of malicious software.

1. Viruses Malware that can replicate when triggered by a human action and cause damage to a computer.

- Worms Self-replicating malware that uses a computer network to send copies of itself to other computers.
- Trojan horses A non-self-replicating malware that pretends to be a harmless application.
- Rootkits Malware that enables continued access to computers or devices while hiding their presence.
- Backdoor A backdoor is a method of bypassing normal authentication in an attempt to remain undetected. This is usually done in an attempt to secure remote access to the computer.

Below are a few examples of the way data theft and extortion can happen using

malware:

1. Adware A type of software that automatically downloads and displays unwanted ads. It is used by authors to generate revenue and collect data without the victim’s knowledge or consent. Some adware may trick users into downloading malware or visiting malicious websites.

- Spyware Hackers use spyware to monitor all your activities.

Spyware can capture your keystrokes, take screenshots, view your webcam, monitor sites that you visit, and view programs and files that you run on your computer. Spyware could be unintentionally installed when a user clicks on adware or installs seemingly harmless files.

- Botnet The term bot is short for robot. Criminals distribute malware that can turn your computer into a bot.

When this occurs, your computer can perform automated tasks over the Internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a botnet.

- Keylogger A Keylogger is a hardware or software based tool used to keep track of, or record the keys struck on a keyboard. This is usually done secretly, so as not to alert the user that their keystrokes are being recorded. This allows a hacker to secretly gather confidential data such as passwords and credit card information without the victim’s knowledge.
- Dialer A dialer is a program that tries to establish a phone connection with a premium-rate number. It infects computers that uses a modem to connect to the Internet, as it modifies the phone and modem configuration, changing the number

provided by the ISP (Internet Service provider), which is normally charged at local rates, for an expensive premium-rate telephone numbers, often located in small countries far from the host computer. Alternatively, it can dial a hacker's machine to transmit stolen data.

Anti-virus software

Anti-virus software identifies and eliminates various malware by scanning files in your computer system. It is important to have anti-virus software installed on your computer to reduce the threat of malicious and damaging threats to your information and work.

Typically, anti-virus software uses two different techniques to accomplish this:

1. By scanning and examining files on the computer system and comparing them to known malware based on certain virus signatures.

- By checking programs for various types of bad behaviour which may indicate a new type of virus. This technique is known as "heuristic checking."

Most well-known anti-virus software in the market use both techniques when performing a scan.

Anti-virus software needs an updated list of the newest viruses and other malware

in order to be effective in protecting your system. Without this, the software may be unable to detect some viruses. The capabilities of different anti-virus software varies depending on how updated the software is. It is also essential to keep web browsers, plug-ins, applications and operating systems up-to-date as most updates contain bug fixes and measures that will help keep developed viruses and malware from your computer.

Please note:

Go to the following web page to learn how to download, install and run the free Microsoft Safety Scanner tool to scan and remove malicious programs from your computer's security profile:

https://learn.microsoft.com/en-us/defender-endpoint/safety-scanner-download

5.9. Good Password Policies

In order to protect computer systems from unauthorized usage and data theft, a good password policy must be put in place and continuously practiced by all users. A good password policy should include the following guidelines

- Always use complex passwords of at least 8-12 character length, which include upper and lowercase, numbers, and special characters.
- Avoid words found in the dictionary.
- Change passwords on a relatively regular basis.
- Avoid using passwords that include your personal information, such as your name, birthdate, or spouse name.

- Never keep default user names and passwords such as “admin”, “root” or “password.”
- Consider using a password manager software instead of, for example, writing down passwords on sticky notes.
- Do not use the same password for different services.
- Do not divulge or share your password with anyone.

Password Management Software

A password manager helps you store login information to various sites and helps you login to those sites automatically. Some password managers may also allow you to generate complex passwords.

Despite their convenience, password managers have been criticized. If the password used to access the password manager is compromised, access will be given to all of a user’s passwords. To many they are a useful tool, but be aware that they are not dependable.

Different Password Managers include:

1. Dashlane
2. LastPass
3. KeePass

Please note

Visit the following website to assess how secure your password is.

https://www.security.org/how-secure-is-my-password/

when you access the website above, the link directly opens in an edit box to enable you type your preferred password for testing. After typing your password, press the enter key and your results will be below your edit box.

5.10. COPYRIGHT AND INTELLECTUAL PROPERTY Concepts

Copyright is a legal right that gives the creator of an original work, such as text or an image, exclusive rights for its use and distribution. Intellectual property refers to the work that has been created and can be protected by laws such as copyright. For example, most software programmes that you buy are copyrighted and you are generally not permitted to copy and share them. Copyright and intellectual property does not just apply to software. You should assume that copyright applies to all information that you find on the Web. For example, if you are researching a topic for a study paper or a blog and you find some interesting material online, you cannot just copy this and present it as your own. You may, however, be able to cite or quote from other sources as long as you give a reference to that source. Some websites have copyright information in their footers or on the home page. These may set out the terms under which you can copy information from the website. If you are in any doubt about whether or not you can reuse specific content, you should always get the permission of the copyright owner. If you are found guilty of copyright infringement or plagiarism, you could face legal punishment.

5.11. Web Accessibility

Web accessibility means that people with disabilities can perceive, understand, navigate, and interact with the Internet, and that they can do so using the assistive technology tools at their disposal. For persons with little or no usable vision, that means using screen reader programs, sometimes in conjunction with refreshable braille displays. For those with varying degrees of usable vision, screen magnification programs like ZoomText, Fusion, and Windows Magnifier are the main tools.

Web Content Accessibility Guidelines

Web Content Accessibility Guidelines (WCAG) are the most widely recognized and accepted standards for web accessibility. These guidelines have been put together by an international group of web experts called the World Wide Web Consortium (W3C). WCAG has evolved over time to keep pace with technological change. WCAG 2.0 and 2.1 were published in 2008 and 2018, respectively. Version 2.2 was released in October 2023, and WCAG 3.0 is already being developed with an expected release date five or six years from now.

A set of detailed criteria are elaborated under four broad principles. As an everyday user of the web, familiarity with the WCAG criteria can help you to better understand what you can reasonably expect from websites in terms of accessibility. When you run into accessibility roadblocks, familiarity with these criteria will aid you to more precisely describe problems to website owners if you want to recommend improvements.

WCAG identifies four general accessibility principles to be used by web developers and policy makers. Within these broad areas, specific criteria are laid out. These principles are:

1. Perceivable. The contents of the page must be detectable to everyone, regardless of disability.
2. Operable. All users must be able to interact with the components of the page.
3. Understandable. All users must be able to understand the meaning of the information on the page, as well as any instructions for interacting with page components.
4. Robust. No matter what a web page looks like or what it contains, it has to remain accessible – able to be used and understood – on a wide variety of devices and using a wide range of assistive technologies.

Use “POUR” as a mnemonic to remember the four WCAG principles.

There are three levels of WCAG Conformance.

- Level A: A minimum level of accessibility that will not meet the needs of all people with disabilities.
- Level AA: provides accessibility for most people and is the level that most web developers aim for. It is the standard for most policy actions or legal proceedings undertaken in the United States related to web accessibility.
- Level AAA: the highest standard of accessibility. It is often aspirational, rather than always achievable, although certain AAA criteria may be important to achieve, depending on one’s target audience.

Usability

Usability is closely related to accessibility. The W3C website states that “**Usability** is about designing products to be effective, efficient, and satisfying.”. In the context of web browsing, a web page is “usable” if it is reasonably straightforward for screen reader users with average skills to interact with it. A website might be technically accessible, but difficult to use. In such cases, information can theoretically be accessed, but with considerable difficulty and frustration. A skilled “power user” might be able to access information on a particular site. At the same time, accessing that same content might be extremely difficult for the majority of users.

Open the link below to understand The W3C website accessibility success criteria with explanations and examples.

https://www.w3.org/WAI/WCAG21/Understanding