Chapter Three
Computer Security

Module Name: ICT Tools and Digital Media
Lecturer: Mrs Shameera Lauthan

Learning Objectives

Generated by Google's Gemini AI

Digital Protection Strategies

Apply strategies to protect personal and professional digital environments.

Cyber Threat Detection & Prevention

Detect and prevent common cyber threats.

Safe & Informed Web Navigation

Navigate safely in online environments, including understanding the risks and tools associated with the dark web.

Proactive Digital Security Mindset

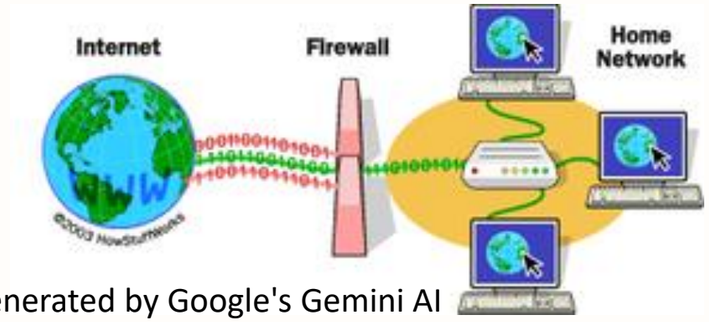
Adopt a proactive attitude toward digital security and privacy management.

Keeping Your Computer Secure at Home

Protecting your computer is crucial in our interconnected world. Here are fundamental steps to ensure your digital safety:

Implement a Firewall

A firewall acts as a barrier, preventing unauthorised access to your computer.



Generated by Google's Gemini AI

Maintain Software Updates

Regularly update all software to patch vulnerabilities and enhance security.

Strong Passwords & Safe Browsing

Use robust, unique passwords and exercise caution with suspicious links and pirated content.

Utilise Antivirus Software

Install and keep antivirus software current to detect and remove malicious threats.

Generated by Google's Gemini AI

Protecting Your Machine from Spyware (Adware)

Spyware is insidious software installed without your knowledge, designed to monitor your activities and transmit data to a third party. Often, it's bundled with freeware or shareware, hidden within lengthy licensing agreements.

These programs track your web browsing habits and duration, primarily for advertising purposes (known as adware). They can significantly impact your system's performance.

Generated by Google's Gemini AI

Consequences of Spyware Infestation

Spyware, though often unseen, can have a detrimental impact on your computer's performance and your internet experience.

System Resource Drain

Spyware operates in the background, consuming valuable CPU and memory. This can lead to sluggish performance, frequent crashes, and system lock-ups, severely disrupting your workflow.

Internet Connection Slowdown

Since spyware transmits your activity data over the internet, it monopolises bandwidth. This results in significantly slower internet speeds, affecting browsing, streaming, and online work.

Malware, Viruses, and Worms: Understanding the Threats

Malware is an umbrella term for any software intentionally designed to cause damage or gain unauthorised access to a computer system. It often disguises itself as legitimate software.

Viruses

Small programs that cause unexpected events and spread through emails, file shares, and infected programs.

Worms

Self-replicating viruses that reside in memory, aiming to spread to as many machines as possible without altering files.

Common Malware Examples

Beyond general malware, specific types pose unique threats, designed for particular malicious activities.

Backdoor

A type of malware that grants a remote attacker complete control over your computer, allowing them to modify or delete files, install programmes, and create user accounts.

Keylogger

This malicious tool records every keystroke you make, capturing sensitive information like credit card details, passwords, and private messages, posing a severe threat to your privacy.

These examples highlight the sophisticated nature of modern malware and the importance of robust cybersecurity practices.

Essential Computer Hygiene for Digital Safety

Good computer hygiene is your first line of defence against cyber threats. Adopting these habits can significantly reduce your risk:

Think Before You Click

Be extremely cautious with email attachments, suspicious websites, and prompts to download unknown software.

Strong Passwords

Use complex, unique passwords for all accounts and change them regularly.

Secure File Sharing

Avoid creating non-password protected file shares to prevent unauthorised access.

Regular Data Backups

Frequent backups ensure your data is recoverable in case of system compromise or failure.

Minimal Applications

Install only necessary applications and services, reducing potential vulnerability points.

Understanding the Deep Web and Dark Web

The internet has layers beyond what search engines index. Understanding these layers is key to comprehensive digital literacy.

The Deep Web

- Content not indexed by standard search engines.
- Includes paywalled content, membership sites, and private corporate pages.
- Estimates suggest it comprises 96-99% of the internet.
- Not inherently malicious; it's simply private or restricted content.

The Dark Web

- A subset of the deep web, intentionally hidden.
- Requires specific software, like Tor Browser, for access.
- Estimated to be around 5% of the total internet.
- While it has illicit uses, it also hosts legitimate anonymous services.

Navigating the Dark Web with Tor Browser

Tor Browser is essential for accessing the dark web, offering significant privacy and security features for users seeking anonymity online. It's built on the principle of multi-layered encryption, routing your traffic through a network of volunteer-run servers to obscure your digital footprint.

Blocks Trackers

Isolates each website visit, clearing cookies and browsing history to prevent third-party tracking.

Defends Against Surveillance

Hides your browsing activity from observers, showing only that you're using Tor.

Resists Fingerprinting

Makes all users appear the same, preventing identification based on browser or device information.

Browse Freely

Bypasses network blocks, allowing access to restricted sites.

Key Takeaways & Next Steps

Proactive computer security is far easier than reacting to an intrusion. By implementing the strategies discussed today, you can significantly enhance your digital safety and privacy.

1

Use Strong Passwords

Combine complexity with regular changes for maximum security.

2

Install & Update Security Software

Antivirus, anti-spyware, and firewalls are your essential digital guards.

3

Practice Good Internet Hygiene

Be cautious with links, downloads, and online purchases. Think before you click!

4

Understand Your System

Know what's running on your computer and disable unnecessary processes.

For a comprehensive checklist by a computer security expert, visit: http://securityfocus.com/columnists/220

[Link to Assignment on Network Fundamentals]