Computers I

2. Protecting Information and Hardware

We must take measures when using computers not only to keep our files, and identity safe and secure, but also our equipment. Much like a car, taking the proper measures to protect a computer will ensure it will run as designed and not break down on us.

2.1 Protecting your equipment

If the processor and other components of a system overheat, the system will get unstable and components will begin to fail and become damaged. Damaged computer parts are expensive and it is essential both for private users and corporations to keep their machines cool.

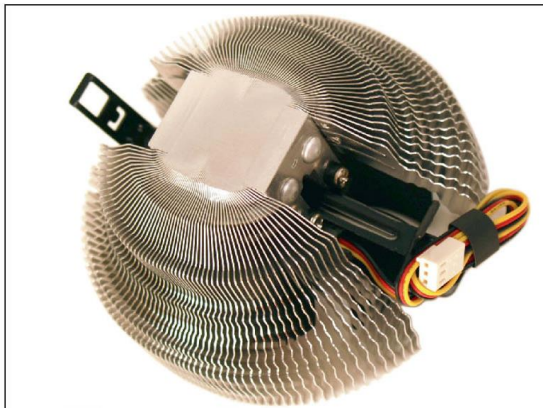
The maximum heat of a computer should be 185 degrees.

A properly cooled system should maintain a temperature of 90 – 110 degrees.

Devices used to cool a system include:

- CPU and case fans – case fans draw hot air out of the case to prevent overheating.

- Coolers – sit on top of processor. Contains fan and heat sink. The heat sink draws heat away from processor and the fan blows away the drawn heat.



- Dust-preventing tools – such as those discussed in lesson 2

The video card draws the most powers and some video cards can be purchased with a connectable fan to cool down the system.

When protecting your computer, the most basic protection begins with combating surges and spikes.

Surge protectors are inexpensive devices that filter electrical power to eliminate surges and spikes before they get to your equipment. Surge protectors are very inexpensive, starting at around $10 for a 4-outlet protector.

When purchasing a surge protector, the lower the let-through voltage, the better your equipment will be protected. It is also wise to purchase a surge protector that has a warranty that not only covers the surge protection device, but the equipment that it is protecting.

2.2 Protecting your files

System failure, virus, file corruption, or some other problems can cause data loss.

Just like we discussed in lesson 2 one of the best methods of protecting your data is by backing them up.

Never trust important data to only one media and that is why we should always have multiple copies and store them on different devices.

After you backup, you should delete a file and attempt to recover it to ensure that the backup process has worked fine.

To protect your files antivirus software is one of the best lines of defense.

Antivirus - is computer software used to prevent, detect and remove malicious computer viruses.

Antivirus software can protect you from

- Virus, Spyware, Malware
- Firewall Protection
- Secure Online Shopping & Banking
- Privacy Protection
- Prevents spying
- Data Theft
- Phishing scams

Antivirus software also allows us to search web sites and be alerted prior to accessing a harmful site by scanning sites in the search results and based on prior information known about a website.

2.3 Protecting your identity

Aside from protecting your files it is crucial that you protect yourself. Your identity is very vulnerable online and you must take steps that your personal information is not stolen.

Ways to protect your identity

- Use anti-virus software, anti-spyware software, and a firewall.
- Create strong passwords.
- Keep your computer's operating system, browser, and security up to date.

Create strong passwords that mix 10 or more letters, numbers and special characters. Don't use the same password for more than one account.

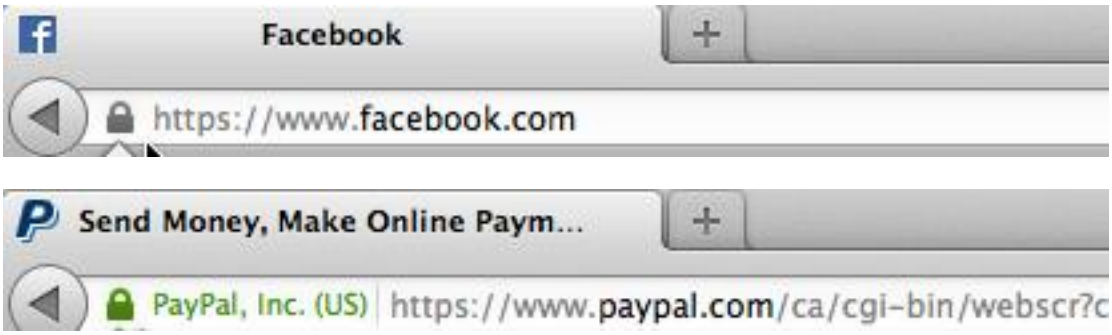
Use anti-virus software, anti-spyware software, and a firewall on your computer. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software.

A tip is to set your computer's operating system, web browser, and security system to update automatically.

When you send sensitive information over the Internet ONLY do so if a "lock" icon on your browser's status bar is present. This means your information will be safe when it's transmitted. If the bar has a lock and is green that means a stronger encryption is being used and the website is even safer than usual.

If a website does not pass sensitive information there will not be any locks but the website is still okay to use. A popular example of such a website is youtube.com

Certain aspects of the website can be secure, for example a YouTube partner looking at his or her ad revenue would be looking at it through an encrypted page as it can contain tax information social security numbers and even bank account numbers.



Don’t always trust free Wi-Fi

Before you use a public Wi-Fi network, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

Identity thieves rely on people making purchases and connecting to bank accounts through these unsecure Wi-Fi networks for them to steal credit card numbers and other important information.

These unsecure networks are a result of being set up by a person that is not as knowledgeable in the security sector. It is up to the consumer to always be aware and knowledgeable.

Many big companies have been attacked via unsecured Wi-Fi over the years and it has resulted in hundreds of thousands of compromised accounts.