Securing a System?

Whether you use your computer for work tasks or personal use or both, it's likely you want to keep it safe and secure. When it comes to computer security, a broad range of threats should be considered, including malicious attacks by hackers, people physically stealing your computer and the information it houses.

Software security updates

While software and security updates seem a bit annoying, they are really important. Aside from adding extra features, they often cover security holes. This means the provider of the operating system (OS) or software has found vulnerabilities which could compromise the program or even your computer.

Apart from the OS, all software(s) that you run on your computer could potentially have flaws. So, whenever it is possible, update them.

Even though they are usually good, you should be wary of updates. Sometimes software companies offer pre-release versions to try. These may be unstable and should be used at your own risk. Even with stable release versions, you may want to wait a day or two in case there are any obvious bugs.

Another thing to watch out for is a fake update which is used by hackers to persuade you to click a link or enter credentials. So always do a little research into the latest updates from the software company.

2. Have your wits about you

Inarguably, being suspicious is one of the best things you can do to keep your computer secure. With hacking techniques becoming increasingly sophisticated, it can be difficult to tell when you're under attack. All it takes is one email/link click and your computer could be compromised.

Make sure to think twice about opening or clicking on anything that doesn't look legit. Don't rely on spam filters to always catch sketchy emails as criminals are constantly trying to outsmart these settings.

3. Enable a firewall

A firewall acts as a barrier between your computer/network and the internet. It effectively closes the computer ports that prevent communication with your device. This protects your computer from incoming threats and could prevent data leak.

While it's possible to close ports manually, a firewall acts as a simple defence to close all ports, opening them only to trusted applications and external devices as required.

If your operating system comes with a firewall, you can simply enable the built-in firewall. In Windows, this can be found by navigating to **Control Panel>System** and **Security**. You might choose to install an additional firewall as an extra layer of defence or if your OS doesn't already have one. A couple of free options are Comodo and TinyWall.

Apart from these software firewalls, there are hardware firewalls too. While these can be purchased separately, they often come built into home routers.

4. Adjust your browser settings

On most browsers, you can adjust the level of privacy and security which could lower the risk of malware infections and hackers attacking your device. Some browsers even enable you to tell websites not to track your movements by blocking cookies.

However, many of these options are disabled by default. But you can easily go into your browser settings and make the necessary adjustments. Chrome, Firefox, Safari, and Edge all provide detailed instructions to help. You can add an additional layer of protection by installing an anti-tracking browser extension like Disconnect or uBlock Origin.

If you want more privacy, you can consider some privacy-focused alternatives like Epic Privacy Browser, Comodo Dragon, or Tor Browser.

5. Install antivirus and anti-spyware software

An antivirus software isn't a completely fool proof option to protect your software, but it can help. There are free options out there, but they're limited, and besides, the paid programs aren't that good. Bitdefender is a popular option that I recommend.

Spyware is a specific type of malware that is designed to secretly infect a computer. It enters the system, gathers information and sends it to a third party. It typically consists information of sensitive nature, such as credentials or banking details, which could ultimately lead to identity theft.

In the spyware category, you have adware (often causing popups), Trojans (posing as a harmless software), and system monitors (such as keyloggers), all of which are risky. Other forms of spyware like tracking cookies are typically harmless, but annoying. Thankfully, many antivirus programs have anti spyware built in.

If spyware has entered your computer, then you can remove it using a ton of options for spyware removal, including many free offerings and some paid tools.

6. Password protect your software and lock your device

Most web-connected software requires login credentials. Always remember not to use the same password across all applications. This makes it easier for someone to hack into all your accounts and possibly steal your identity.

If you're having trouble remembering passwords, then you could try a password manager. This will keep all your passwords safe. A master password can be combined with an email or SMS as part of a two-step verification (2SV) method. 2SV requires you to verify your identity with a PIN code.

While it is rare, but someone could get their hands on your actual computer. So have a strong computer password to at least make it more difficult for them to enter.

Other forms of verification include biometric methods like a fingerprint or retina scan. Alternative methods might involve key cards and fobs, such as those offered by Yubico. Any of these can be combined with each other and/or a password as part of a two-step authentication (2FA) process.

Another option is a physical lock which is good for laptops but can also be used on home/work computers. Kensington locks and similar brands provide small locks that insert into a special hole in the device. Some require a physical key while others work using a code.

7. Encrypt your data

Encrypting your data secures it as it requires resources to decrypt, which alone might be enough to deter a hacker from pursuing action.

There is a plethora of tools out there to help you encrypt things like online traffic and accounts, communication, and files stored on your computer. For full disk encryption, some popular tools are VeraCrypt and BitLocker. You can also find separate tools to help you encrypt your mobile device.

8. Use a VPN

A Virtual Private Network (VPN) is an excellent way to increase your security. It encrypts all your internet traffic and tunnels it through an intermediary server in a separate location. This masks your IP, replacing it with a different one, so that your ISP can no longer track you.

You can typically choose the server location for getting the fastest speeds or unblocking geo-locked content. A VPN can help you browse securely while using open Wi-Fi networks and censored material (e.g. Facebook in China).

There are some free offerings out there which are limited in features but can be good for a start. Some paid options have free trial periods for the full service and most offer generous money-back guarantee periods.

No matter what you store on your computer, it’s important to protect its content. Although nothing is ever completely secure, following the steps above will provide most people with ample privacy and security.