Computer Security

Software updates | internet | Passwords | Sensitive Data | Emails & Attachments | Protective Software

Software updates

Chances are you've noticed the pop-ups on your computer notifying you of available updates. Although it's easy to hide the alerts, or even ignore them altogether, it's important to pay attention to them.

Software updates are released to do a myriad of things: provide bug fixes, release new features, remove outdated features, and fix security vulnerabilities. A vulnerability is a security weakness or a security hole; hackers exploit these vulnerabilities to infect computers with viruses, steal sensitive information, and commit other crimes.

Having up to date software for your programs and operating system is key to avoid these situations. Always download and install the latest security updates for all applications.

Tip: Turn on automatic updating for your operating system

Computer Security

When you connect to the internet, your data and private information is vulnerable and at risk; connecting to the web makes you a target to hackers and other criminals with malicious intent.

Decrease the risk by enabling network encryption; this will help prevent other computers in your area from using your Internet connection. Encryption scrambles the information sent over the Internet signal. All routers support some kind of encryption; several well-known encryption methods include WEP, WPA, and WPA2.

If you live in a small space it may be a good idea to decrease the range on your router. Additionally, you may want to consider changing the name of your SSID (Wireless Network Name) on your router. Although this will not necessarily make your network more secure, it is a good best practice that ensures others know which network they are connecting to.

Tip: Enable network encryption to prevent others from using your signal

Computer Security

Having weak or insecure passwords leaves you vulnerable to hackers and thieves. They can log into your accounts, access private information such as financial data, and even gain access your personal photos.

This is why it’s crucial to choose strong passwords that use a combination of letters, numbers, and special characters. It’s best to create a unique password for each account. You don’t have to worry about tracking them because there are applications and tools you can use to help you manage and store your passwords.

It’s important to never share your password with anyone else, not even friends, family, or coworkers. Finally, it seems obvious but it’s worth stating that you should never post your password somewhere obvious or in plain sight.

Tip: Use more than 12 characters in your passwords

Computer Security

It’s very important to protect your sensitive data. The first tip is to keep this kind of information (Social Security Number, credit card information, health information, etc.) off your computer as much as possible.

One basic, yet often overlooked, tip is to regularly back up your data. It’s important to have a duplicate in case it is lost, stolen, or compromised. It’s a good idea to create a backup to the cloud so that data remains accessible even if a device becomes corrupt or unusable.

Make it a best practice to always remove sensitive data and files from your system when you no longer need them. Only use encrypted networks and not access any sensitive or personal information using public internet connections.

If you have a home wireless network you might share files between machines. However, don’t make your files visible to other machines; you should disable file and media sharing completely for safety purposes.

Tip: Do not access financial information over public internet connections

Computer Security

Emails should be a fun and harmless way to communicate but they can in fact be very dangerous. Email attachments and links in particular can be harmful. Any type of file can be attached to an email, including dangerous malware that will take over and infect a computer.

It's critical to never open an unknown email and never click on any links or attachments. Fake emails, called phishing scams, can be extremely sophisticated and made to look like real emails from banks and other financial institutions.

Most email services will automatically scan incoming attachments for malware and inform you of dangerous or risky attachments. If you do not know the sender of an email, or if you see a warning that an attachment is malicious, do not open it. Delete all chain mails and junk mail.

Tip: Never open attachments or click on links in unknown emails

Computer Security

Anti-virus software is used to prevent, detect, and remove malware, like computer viruses, bugs etc. It also prevents and removes adware, spyware, and other forms of malware.

Anti-virus software is one of the best ways you can protect your computer. It's critical that you keep the software up to date to ensure your anti-virus program remains effective.

In addition to using anti-virus software it's important to not open any dangerous attachments, files, or emails. It's important to be very careful about which links and downloads you click on at all times when you are using the Internet.

Tip: Always use up-to-date anti-virus software