PROTECTING YOUR COMPUTER

January 2023

https://righttoconnect.org

Your personal and official data, including bank information, emails, files, images, videos, and other digital communications, are all stored on your computers and other electronic devices, and you must protect them. In order to protect them and safeguard your sensitive data stored in them, please follow these instructions:

ACTIVATE THE FIREWALL

Activate the firewall while you are online. A firewall acts as a wall between a network and the outside world, providing basic security. Sometimes a firewall is a standalone server, other times, it is a router; and still, other times, it is computer software.

A firewall controls network traffic. With a firewall, a proxy server is often used to mask the IP address of the internal network and reveal a single IP address to strangers.

Install an antivirus

Install an antivirus on your PC. Computer viruses and malware are commonplace. Viruses may be the primary cause of your computer's sluggish performance or the deletion of crucial files, or they may be less evident.

Every action is monitored by antivirus software, which is always active. This applies to each time you access a file from the internet, run the software, or open a document. All new files are scanned by the application, and any ones it finds suspicious are quarantined. Always make sure updates are being applied to your antivirus. Do not install more than one antivirus on your PC at a time.

Here are the top 5 antiviruses for 2023

1. Bitdefender – the very finest antivirus program
https://www.bitdefender.com
2. Norton – feature-rich antiviral program https://ca.norton.com
3. TotalAV – antivirus software with basic security features
https://www.totalav.com
4. Surfshark – fantastic antivirus and VPN bundle
https://surfshark.com
5. NordVPN – cutting-edge real-time security
https://nordvpn.com

Antispyware

Install an antispyware package. Spyware is a particular type of software that secretly monitors and collects information from people or organizations. For example, some spyware keeps track of every keystroke, allowing users to acquire passwords and other private financial information. Spyware programs can track every computer activity, and third parties have multiple ways to acquire this information. Additionally, malware may begin to download in the background while you are just visiting a specific website. Fortunately, Antispyware is now either included as standard in most antivirus systems or is available as an add-on option.

Upgrade the operating system and apps

Upgrade your operating system and Apps. Both your operating system and your antivirus program will automatically update. However, you should update your web browsers, Java, Adobe Reader, and a number of other programs that are not updated automatically. Some upgrades eliminate the bugs that allow malicious malware to attack these programs. Updates to the operating system should be applied immediately. The majority of updates include security patches that prevent hackers from accessing your data and utilizing it for their own ends.

Use a secure password

Make sure your PC password is secure. In terms of digital security, it is a crucial step. By breaking passwords, hackers and attackers try to access your information systems. Have a solid Windows password but rely on something other than Windows passwords to protect your data. They are swiftly obliterated. It is recommended to write down your passwords and store them securely rather than using a short, obvious password. Use a different password every time and ensure it's secure and has nothing to do with your hobbies or way of life. Frequently change your passwords.

Password managers

1. NordPass – leading password manager https://nordpass.com
2. Keeper – ideal for Apple devices https://www.keepersecurity.com
3. RoboForm – intent for browsers https://www.roboform.com
4. Dashlane – perfect for sharing passwords
https://www.dashlane.com
5. 1Password – ideal for family use https://1password.com
6. LastPass – the most feature-rich choice
https://www.lastpass.com
7. Passwarden – ideal for personal use
https://www.keepsolid.com/passwarden

SPAM

Be aware of spams. It is an unwanted email that is sent to many recipients in an uninvited manner. A common way for a virus or worm to spread is through spam. Spam is also used to send emails to entice recipients to visit phishing websites to steal their identities. In summary, spam is an annoyance at best and a means of spreading malware like spyware, viruses, worms, and phishing scams at worst. Be cautious when opening attachments or clicking links in emails from unknown senders. The most blatant spam is being caught by spam email filters more and more often.

Shut Down your computer

Turn your computer off at night or for extended periods of time while you're not using it. Because leaving your computer on makes it more visible and a target for hackers, shutting it down eliminates any connection a hacker may have formed with your network and prevents any potential harm from occurring.

Two - factor authentication

Utilize two-factor authentication. Using a password as your main line of defense against computer hackers is secure, but adding another layer makes security better. When you log in to a website, you may often choose to use two-factor authentication, which ups security by asking you to enter a code in addition to your password. Your phone number or email address will receive this code.

Resources

https://nordpass.com
https://www.keepersecurity.com
https://www.roboform.com
https://www.dashlane.com
https://1password.com
https://www.lastpass.com
https://www.keepsolid.com/passwarden
https://www.bitdefender.com
https://ca.norton.com
https://www.totalav.com
https://surfshark.com
https://nordvpn.com