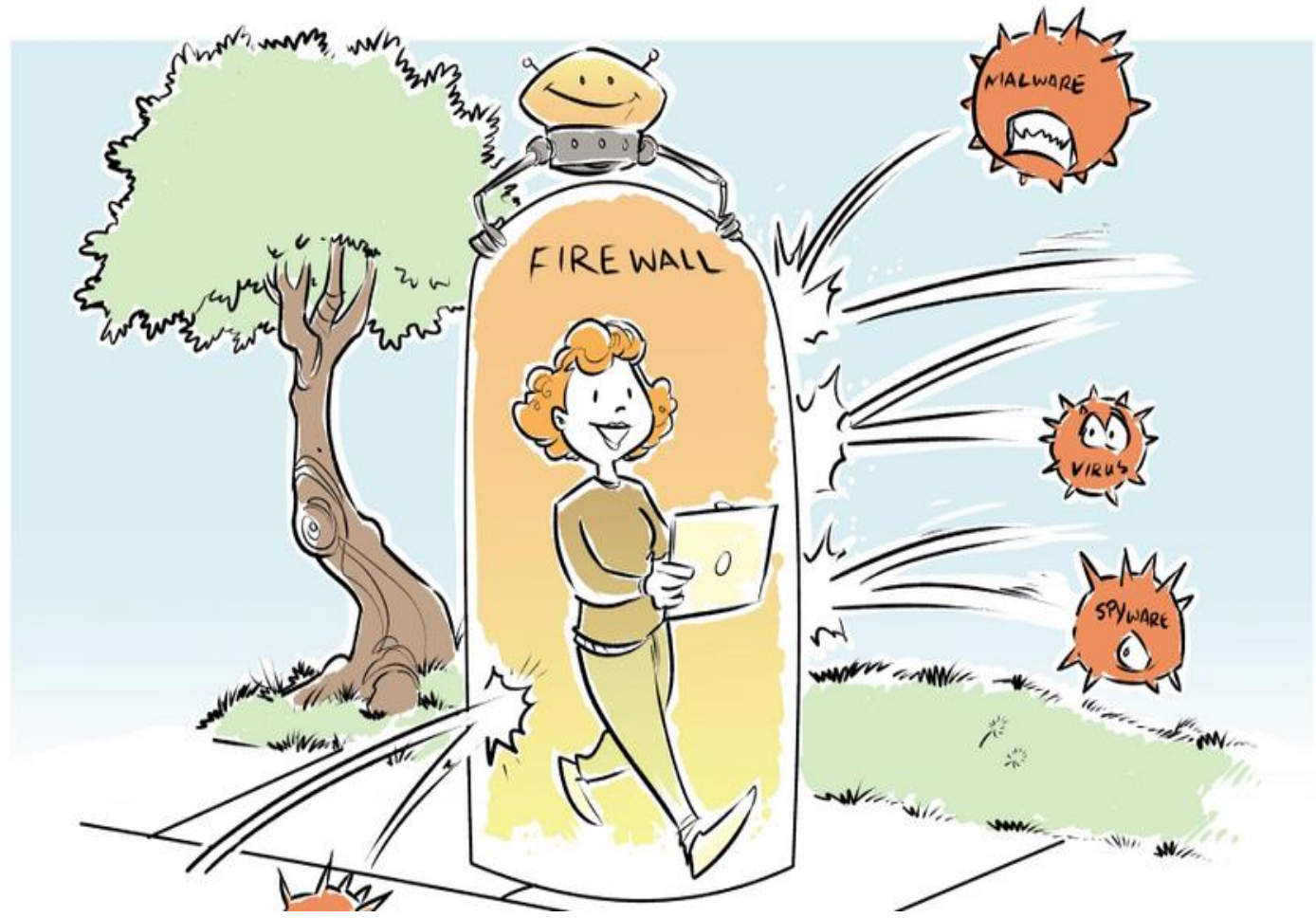
How can I protect myself against malware?

A few simple precautions can help prevent your devices from getting malware in the first place.



Firewalls - A firewall is a software-based network security device that both monitors and manages incoming and outgoing network traffic. As you browse the web, send emails, or stream movies, you request data from specific web servers.

Your firewall stands between your local network and the internet, sifting through your network's traffic, accepting the data you requested and blocking unwanted or unrecognised connections, like malware and cyber-attacks, from accessing and compromising your device. Like castle walls, firewalls are essentially your network's first line of defence. A firewall's purpose is to establish a barrier between your internal network and an external network, like the internet. Most security software and operating systems come with firewalls installed. Be sure yours are turned on and configure your security settings so that updates run automatically.

Remember! - Firewalls shouldn't be your only line of defence against malware. Consider them as a layer of security, that forms part of a comprehensive online security regimen.

Additionally, you should incorporate the following measures:

Anti-virus software - Antivirus software, on the other hand, helps protect your devices, not your network, from malware and other threats. Download and install an app that actively scans and blocks malware threats, both on your computer and your mobile device.

Antivirus software is a program(s) that is created to search, detect, prevent and remove software viruses that can harm your system. Other harmful software such as worms, adware, and other threats can also be detected and removed using an antivirus. This software is designed to be used as a proactive approach to cyber security, preventing threats from entering your computer and causing issues. Most antivirus software operates in the background once installed, providing real-time protection against virus attacks.

The **antivirus software** is available in **2 types**:

(i) **Free**: Free anti-virus software provides basic virus protection.

(ii)**Paid**: commercial anti-virus software provides more extensive protection against the many existing forms of malware.

Remember! - Smartphones and tablets *(including both Android and IOS*) may also require strong antivirus software and there are various anti-virus applications that are available for you to download to ensure you remain fully protected, irrespective of the type of device you are using.

Keep everything up to date. Be sure that all your internet-enabled devices - including your mobile devices, are up to date with the latest operating system, web browsers, and security software. Outdated software creates security vulnerabilities that are routinely patched with software updates. **The latest version is the safest version!**

Never download and/or run software from a provider you don't trust. All of the protections provided by a firewall and other security software are easily rendered useless by the simple act of downloading and running some malicious software from the internet.

Secure your wireless router - Your router is the device that receives and sends data between the internet and the internet-enabled devices in your home. Replace the default manufacturer password it came with, review your security settings, and set up a guest network for visitors when possible.

Back up your data regularly - backing up your files to an external drive, a cloud, or both will not stop malware from getting onto your device, but it's the best defence against an attacker locking you out of your data, such as with ransomware attacks.

Be careful online – avoid clicking on popups and ads and be aware of suspicious messages, emails and attachments. Don't click on unknown links in emails, texts, or social media messages, especially from a sender you don't recognize. Never open an attachment unless you know what it is.

Be careful where you browse - stick to reputable, trusted sites, and pay attention to domain names - avoid sites without top-level domains, like .com, .net, .org, etc as malware may often reside on websites with poor backend security.

Set strong passwords and use multi-factor authentication - the stronger your passwords, the better protected your system is from attackers and malware. Maintain strong, unique passwords for all accounts on your devices.