There are simple steps one can take to improve online security. This document outlines some important basic steps anyone can take.
Some Terms...

There are many potential threats with the terms ‘hacked’ and ‘virus’ appearing most often. In fact they are specific. The most common threats are not necessarily from ‘hacked’ software and indeed viral infections are relatively rare thanks to anti-virus software.
Even today (2019) there are many who refute the negative use of the term ‘hacker’ since anyone who writes computer code, for good or bad purposes is essentially a ‘hacker’.

Within the coding communities a common term for a malicious coder is a ‘Black Hat’ hacker/coder.
Virus, Trojan?

Computer ‘virus’ is executable code written to automatically spread across networks and media. Each virus has its own functions and by definition self proliferates. A ‘trojan’ is similar but remains dormant until activated.

There are thousands of variants. It is best practice to keep anti-virus applications up to date.
Spyware

Today (2019) Spyware is one of the most common security issues. It is not necessarily a virus. In fact spyware may only be active within web browsers (or email clients) and often only active while a particular browser session runs.

Because it uses a web browser it’s not platform specific, Mac, Windows, Phone, Tablets using web browsers can be infected.
security practices, steps

Auto Locking

Most modern devices can be set to request a PIN or password before use. In ‘idle’ mode they can automatically switch to a screen-saver and one must enter a PIN or password to continue.

Always set your time-out to lock-screens as short a period as possible. A few minutes if you can. The shorter the time to ‘lock-screen’ the better you are protected.
User Accounts

Always require a login

Very many devices allow us to set more than one log-in, a rule of thumb is: if you switch your device on (especially computer) and you see a desktop without logging-in, you are vulnerable. Create a ‘Working’ account where you spend most of your time but if you sometimes have to log into a secure account such as your bank, PayPal or E-Commerce website create a second account (Financial) just for this purpose. Each account should have a different password.

Protection through discipline

With two accounts, be careful not to confuse and mix activities between them. For example, you may be within your ‘Working’ account but find you must pay for something online, log into PayPal? Then switch to your ‘Financial’ account to do this, logging out when finished. This means should one of your accounts get hacked, damage may be restricted to just that one, not to others on your device.

Only visit known, safe and trusted websites within your ‘Financial’ account.
A good password

Loss of a password is one of the main causes for security breach. It’s not always because of spyware, sometimes the password itself simply is not robust enough to defeat scammers and ‘black hat’ hackers.

• Change your password periodically (twice a year)
• Use at least eight characters
• Use at least one numeral
• Use a mixture of upper and lower case characters
• Use at least one non alpha-numeric symbol (e.g. > @ _ !)
• Never share your password with another person
• Do not use sequential numbering (e.g. 1234)
• Do not use common phrases (e.g. Let-me-in)
• Do not use one login (name and password) for all your accounts
Email is shockingly easy to fake!

A fake email is known as a ‘spoof’ and can appear to be from anyone. You can receive a mail appearing to be from a person you trust, even reply to the message and get an answer yet it’s from a ‘scammer’. If there is sensitive information especially when there is a financial transaction requested take care to verify with alternative methods that the request is genuine.

Phishing emails appear to be from authentic companies. Following a link one may see what appears to be their website where you log in to find scammers record your key-strokes and can log into the real website at will, as you!

Always treat embedded links within emails with suspicion. Do not follow email links unless you are absolutely sure the message is genuine.