

KEEPING YOUR COMPUTER SAFE

THREATS AND WHAT
YOU CAN DO TO
PROTECT YOURSELF
AND YOUR COMPUTER



WHAT ARE THE THREATS?

You can be the victim of a Phishing Scam.

Your accounts can be hacked into, most often your email account.

Malware or computer software with malicious intent.

Your computer files can be corrupted.

Your computer can be held for ransom.



malicious
soft**ware**

NAMES OF DIFFERENT MALWARE

Spyware software that transmits data covertly from their hard drive.

Virus software that replicates itself by modifying other computer programs and inserting its own code.

Adware software that automatically displays or downloads advertising material.

Rootkit software that enable an unauthorized user to gain control of a computer system without being detected.

Ransomware malware that perpetually block access to computer data unless a ransom is paid.

Trojan horse malware that is often disguised as legitimate software.

RAT Remote Access Trojan malware program that gives an intruder administrative control over a target computer

Types of malware



Worm malware that self-replicates and infects networks.

Keylogger malware used to record user keystrokes to steal passwords and other sensitive information.

WHAT ARE THE RISKS IF YOUR COMPUTER IS INFECTED?

The Risks not much.

Many security breaches are harmless.

Your email can become a spamming tool, sending out messages on behalf of someone else.

Files on your computer can be corrupted including system files.

Your computer can become a zombie in denial of service attacks (you may be prevented from accessing email, websites etc.)

Credit card information can be stolen leading to credit card fraud.



HOW TO PROTECT YOURSELF



USE COMMON SENSE when using email, downloading or using attachments.

DO NOT BE LEAD ASTRAY emails often use fraudulent hyperlinks, beware of unfamiliar websites.

BEWARE OF EMAILS WITH ATTACHMENTS only open attachments from known senders.

AVOID FILLING OUT FORMS CONTAINED WITHIN EMAIL often they are phishing for personal information.

ALWAYS LOG DIRECTLY TO THE OFFICAL WEBSITE FOR THE BUSINESS IDENTIFIED IN THE EMAIL instead of using a provided link which may be fake.

BEWARE IF YOU ARE ASKED TO ACT QUICKLY OR AS AN EMERGENCY IT MAY BE A SCAM fraudsters try to create a sense of urgency to try to make you act.

CREATE STRONG PASSWORDS best passwords use numbers and letters avoiding real words.

HOW TO PROTECT YOUR COMPUTER



USE A CLOUD TOOL Dropbox, OneDrive, Google Drive will store files for free.

INSTALL ANTI-VIRUS SOFTWARE Windows Security on Windows 10, Norton, MacAfee, Avast, Kaspersky, Malwarebytes anything is fine.

UPDATE YOUR OPERATING SYSTEM use update and security from Windows 10 settings screen.

UPDATE ANTI-VIRUS DEFINITIONS AND RUN SCANS definitions should be updating automatically but do this once in a while anyway.

USE A CLEANER AND ANTI-VIRUS TOOL this will help keep your computer running fast, ccleaner and malwarebytes are good.

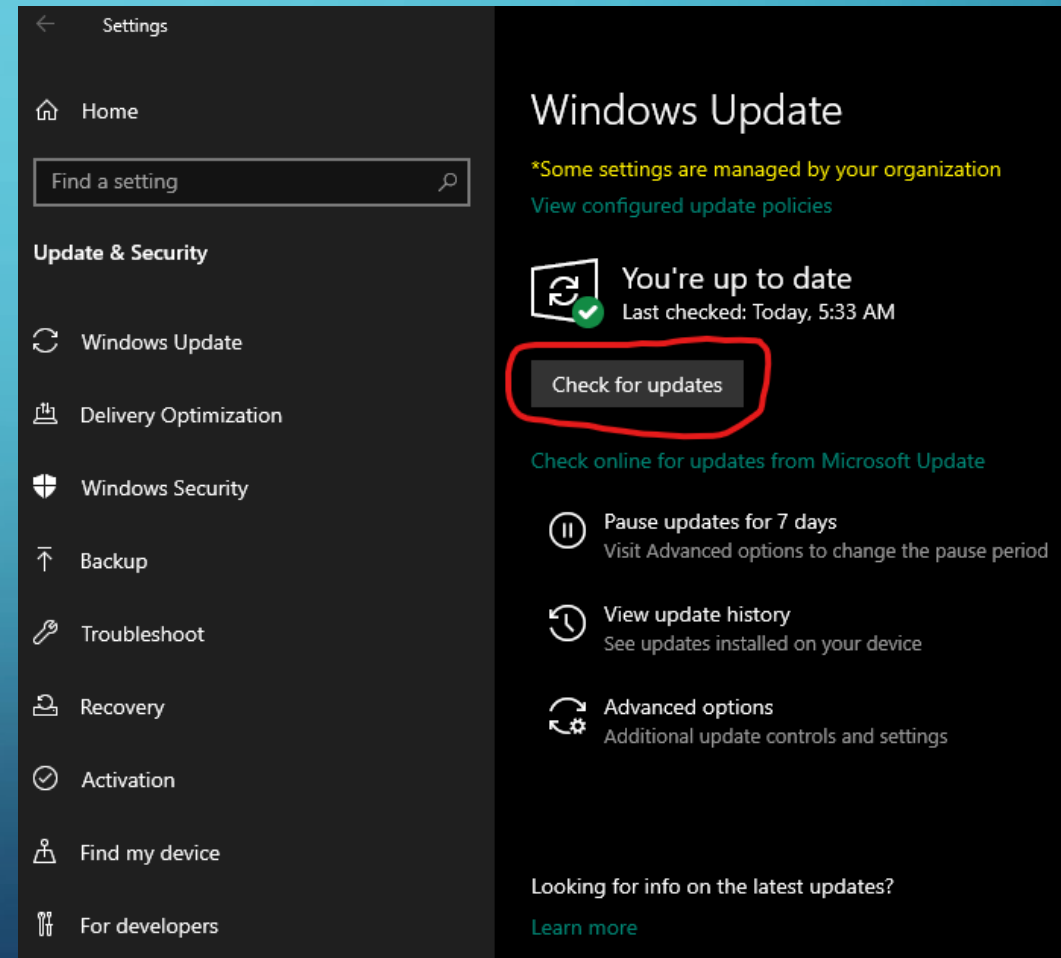
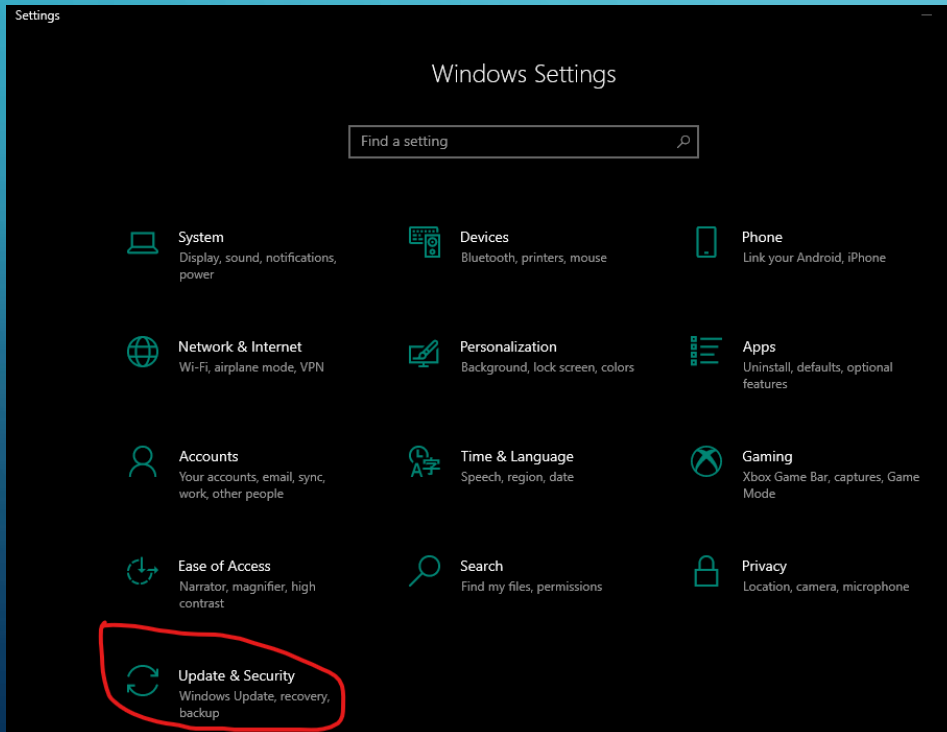
HOW DO I UPDATE WINDOWS 10?

Select Windows Start Button  + I

Select Gear/Settings

Select Updates & Security

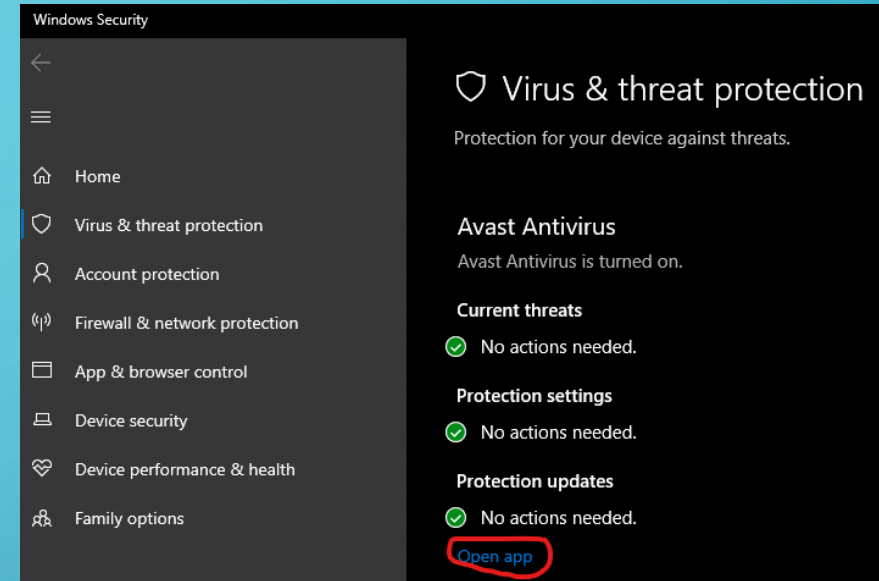
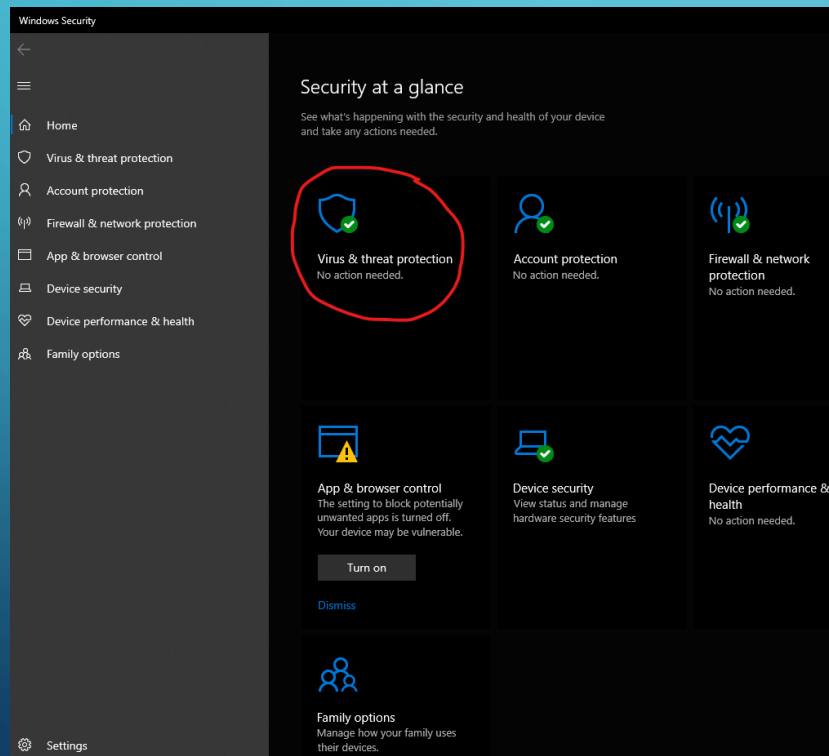
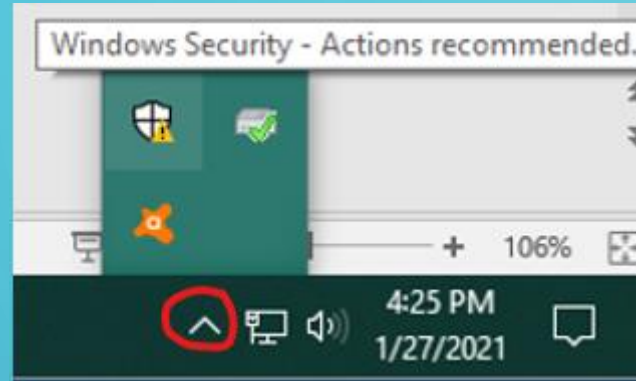
Select Check for Updates



HOW DO I UPDATE VIRUS PROTECTION

Select  on toolbar
Select Virus & threat protection

Select update virus definitions OR
run scan (select quick scan or targeted scan)






Virus Scans

Here you'll find a variety of scan types, from our popular Smart Scan (to detect malware and other issues) to more specialized scans below.

RUN SMART SCAN

Other scans

 SCAN NOW Full Virus Scan Scan your entire PC from top to bottom	 SCAN NOW Targeted Scan Scan specific folders or external drives	 OPEN NOW Boot-Time Scan Scan for threats before Windows starts up
---	---	---

