Module 12

Professional Practice Program

Cyber Security

DISCLAIMER AND COPYRIGHT NOTICE

This written material accompanies a spoken presentation and must be considered in conjunction with that presentation. It is prepared at February 2018 and describes the general tenor of legislation and other rules known at the time and is not intended to be relied upon as a substitute for professional advice in relation to actual facts and circumstances. The material may become out of date due to subsequent industry and/or legislative changes. No responsibility can be accepted by the Institute of Public Accountants or the presenters for loss occasioned to any person doing anything or refraining from doing anything as a result of anything contained in this presentation material.

Course completion

The IPA Professional Practice Program has been designed for IPA members in professional practice and for non-practitioners as a refresher Program.

With recognition comes responsibility. The IPA is recognised in legislation as one of the three professional accounting bodies within Australia. This means compliance with the ASIC Act and with regulations and standards set by ATO, TPB, ASIC, APESB, FRC, AASB, AUASB and IFAC.

The regulators, standard setters, government and the public all rely on the professional expertise, competence and ethics of IPA members. Therefore, the IPA has mandated that members moving into professional practice must demonstrate competence in these key areas.

It is compulsory to complete the IPA Professional Practice Program within 6 months of receiving an IPA PPC unless you have completed a Professional Practice Program with Chartered Accountants Australia + New Zealand or CPA Australia within the last 5 years.

The Program consists of self-paced study and a 2 day face-to-face workshop. You should complete the self-paced study before attending the workshop. This will take up to 80 hours, depending on your experience. To successfully complete the Program, you must:

- Attend all sessions of the Program,
- Successfully complete the assessment held at the end of the Program.

The assessment comprises of 30 multiple-choice questions and you are permitted 1 hour to complete the assessment. You may refer to your course materials, but you are not to consult any other person in or outside of the room. There is 1 mark per question and you need to obtain at least 50% to successfully complete the assessment.

If you do not successfully complete the assessment, you will be offered an opportunity to re-sit the assessment. If you are still unsuccessful, you will be required to repeat the 2 day face-to-face workshop and successfully pass the assessment. The IPA reserves the right to cancel a member’s PPC in the event a member does not pass the assessment.

Module 12

Cyber Security

Topic list: **Page**

12.1: Introduction – Cyber Security

You and your computer are on the frontline of the cyber battel ground. Together, you both represent the most significant entry point for attackers obtaining a toe hold into your business.

Nearly every day we read stories about companies that have suffered serious breaches as a result of not taking cyber security seriously.

Some Examples:

1. *Equifax last week disclosed a historic breach involving Social Security numbers and other sensitive data on as many as 143 million Americans (September 2017)*
2. *As many as 14 million records of Verizon subscribers exposed (July 2017)*
3. *Association of British Travel Agents exposed details of 43,000 individuals (January 2017)*
4. *Australians were amongst the 1 billion victims of Yahoo's data breach (December 2016)*
5. *Australian red Cross Blood Services exposes 1.74Gb file containing 1.28 million donors (October 2016)*
6. *Target suffered a massive loss of confidential data when more than 140 million of its customers were leaked included personal identifiable information.*

Despite widespread awareness around cyber security, there's a reason why cyber-attacks are still so effective. They are always several steps in front of us. These miscreants continue to increase their level of sophistication and there are now dozens of different ways that they can attempt to get their hands on your valuable and personal information.

Phishing (pronounced fishing) and ransomware represented the top two most significant threats to hit organisations in the past year.

Their motivation is money, your money.

2017 has been a very productive year for cybercriminals. And it's only going to get worse for us! Criminal data breaches will cost an estimated $8 trillion over the next 5 years. Think about it. The US deficit is $20 trillion right now, but just under half of that figure is what businesses will have to pay for cyber crime and data breaches over the next 5 years (ITWire – April 2017)

So, what Is Cyber Security?

The core function of almost all cyber security measures is to guard hardware, software and data against everything from unauthorised access to malicious attacks and even accidental damage.

As such, majority of cyber security measures needs to be implemented long before an attack occurs.

Everyone should know how important it is to stay safe online. If you fall for a phishing scam or similar, you are liable to end up having your identity stolen, which can have some pretty serious consequences.

Implementing an effective company-wide cyber security plan sounds and looks quite difficult and expensive. But, it's not! By following the described security hygiene measures in this training guide, you will mitigate around 80% of the security incidents.

What Are Your Cyber Security Responsibilities?

Effective cyber security is more than just a benefit to your business, it’s also a responsibility. And depending on the nature of your business, size and complexity, hardening and developing resiliency against cyber threats to your business can be difficult, time consuming, and expensive. That said, there are a variety of easy counter measures that virtually all businesses should adopt. And these are described in the next chapter – Your Security Hygiene

12.2: Cyber Security Hygiene

Every day we do things to safeguard ourselves and our business. For example, when we drive our cars, we buckle up; We brush our teeth daily to maintain our mouth and gums hygiene; We apply sun screen to our skin to protect ourselves from the harmful rays of the sun; We take car insurance in case of an unforeseen accident.

Protecting our information digital business worlds needs to become our normal day-today activity. We must adopt a high level of hygiene practice on a day to day basis or else we endanger our business.

Remember, your BUSINESS is your BUSINESS. Whether you are in business or managing someone else business, you are responsible for its success.

The following 4 sections of the notes are the fundamentals hygiene practices that you need to adopt.

1. Patching Your Operating Systems & All Applications
2. Running Anti Malware Software
3. Ensuring Fully Functional Backup / Restore Processes
4. Adopting Best Practice User Awareness

Please note this module provides tools to manage cyber security for Microsoft operating systems, not for Mac operating systems.

12.3: Patching Microsoft Windows Operating Systems and all Applications

If your system seems to be working correctly, you may be wondering why you need to apply any updates or patches to either to the system or its applications. We have often heard of the saying “if it isn’t broken, don’t fix it!”.

Great quote, but unfortunately, it doesn’t apply for engendering business resiliency from cyber threats.

Malware is continuously adapting. Its dynamic. Which means your cyber resilience effectiveness has a direct correlation with the latest system and application updates.

And if you decide to not apply the updates, you might be leaving the door wide open for malware to take advantage. Malware exploits flaws in your operating system and applications.

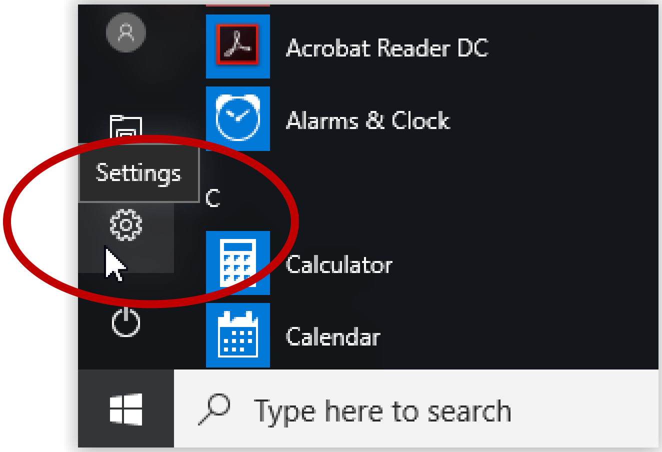
By applying these update, you minimise the attack surface.

12.3.1: Microsoft Windows Operating Systems

Every computer running windows comes with the windows update functionality. This enables Microsoft to provide computers with the latest software patches that fix security problems within the operating system and the (Microsoft) applications.

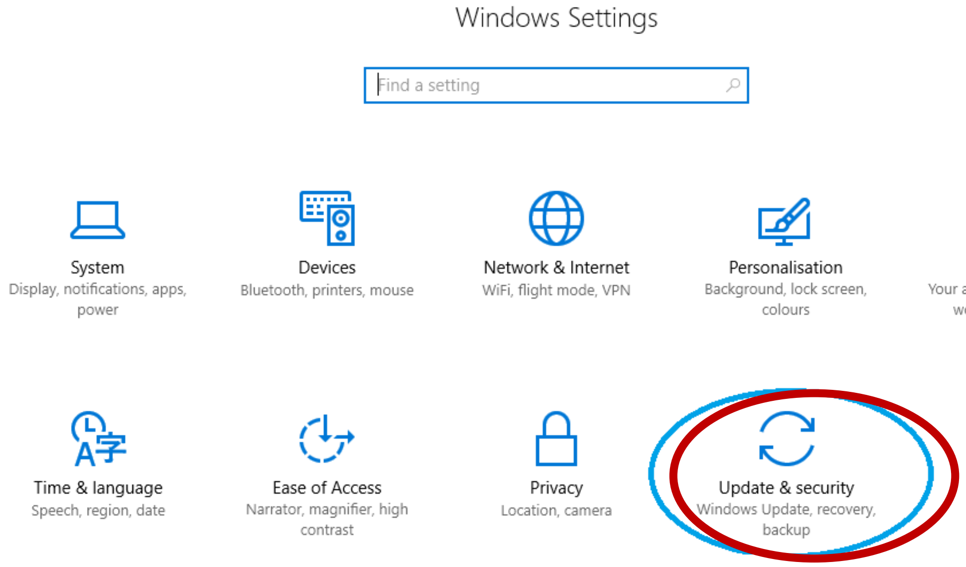
One can check the status of the updates by following these steps:

Click on the “Windows” button followed by a click on “Settings”

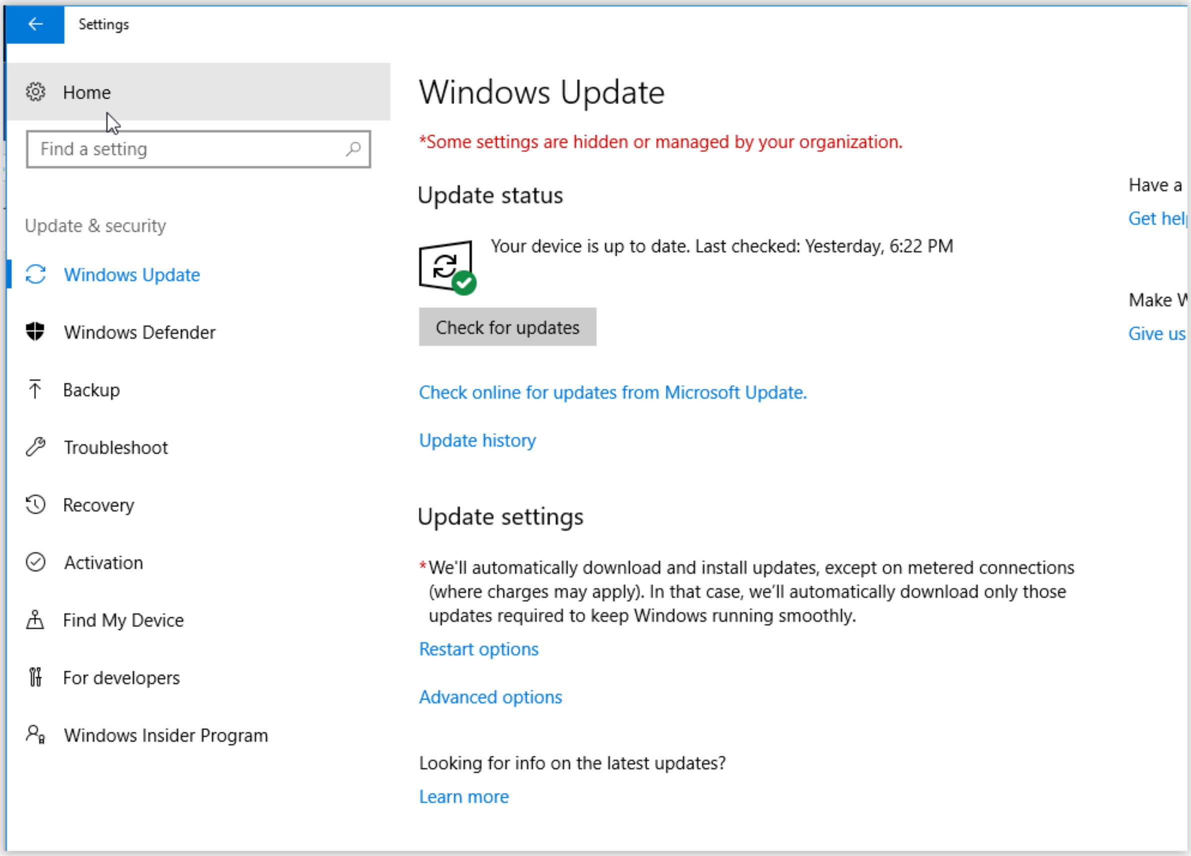


In Windows Settings double click on “Updates & Security”

-


Windows Settings
Find a setting
System
Display, notifications, apps, power
Devices
Bluetooth, printers, mouse
Network & Internet
WiFi, flight mode, VPN
Personalisation
Background, lock screen, colours
Accounts
Your accounts, email, sync, work, other people
Time & language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & security
Windows Update, recovery, backup

This will pop up a window and will show the status of "Update Status"



Windows Update

*Some settings are hidden or managed by your organization.

Update status

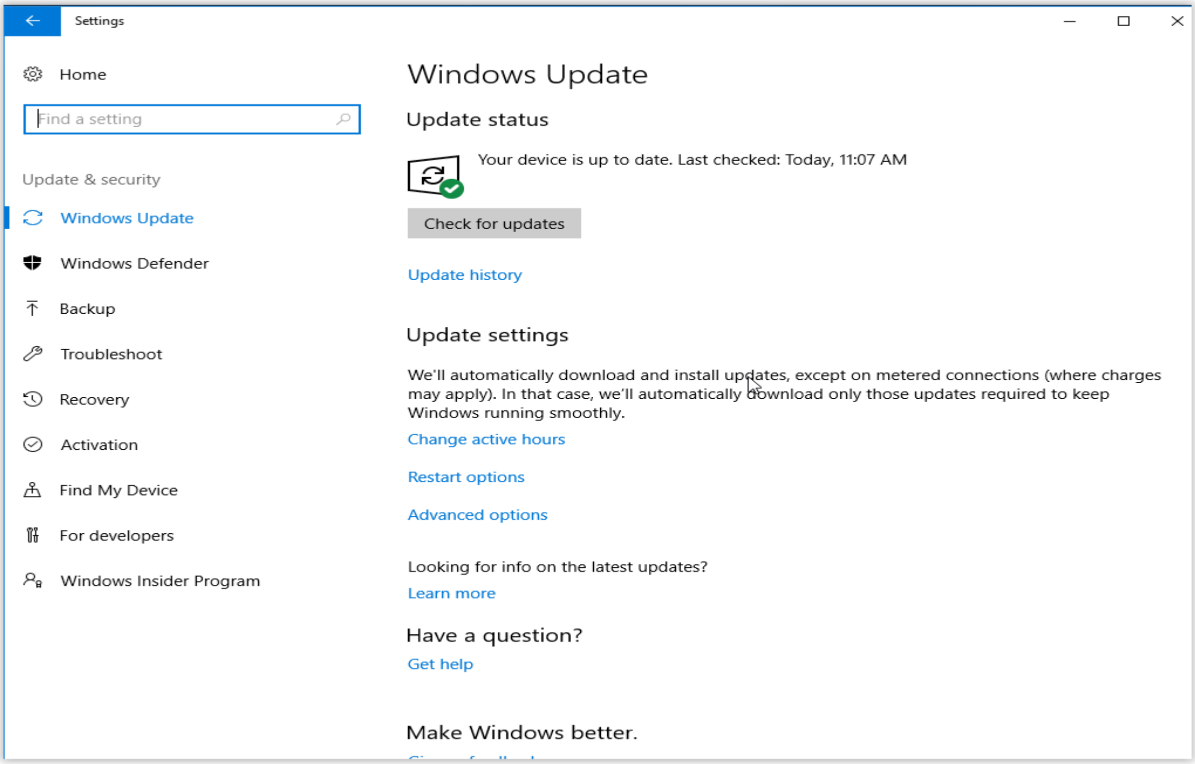
Your device is up to date. Last checked: Yesterday, 6:22 PM

*We'll automatically download and install updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly.

Looking for info on the latest updates?

If “Windows update” is centrally managed like in this example the computer will report that as can be seen over here.

This is the screen from a computer that’s running without a managed update:



Windows Update

Update status

Your device is up to date. Last checked: Today, 11:07 AM

Update settings

We'll automatically download and install updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly.

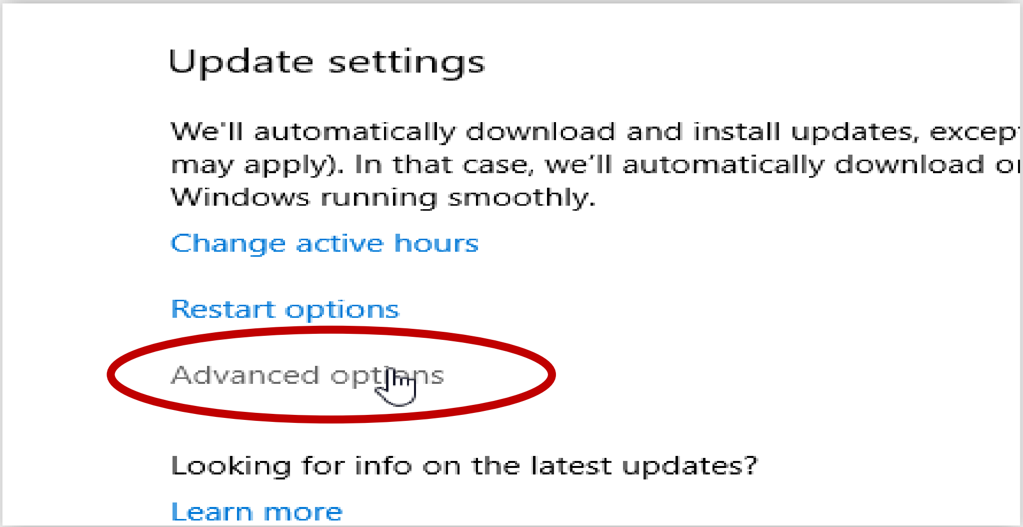
Looking for info on the latest updates?

Have a question?

Make Windows better.

In order to make sure a computer is getting all the updates for Microsoft products do the following:

Click on advance options:



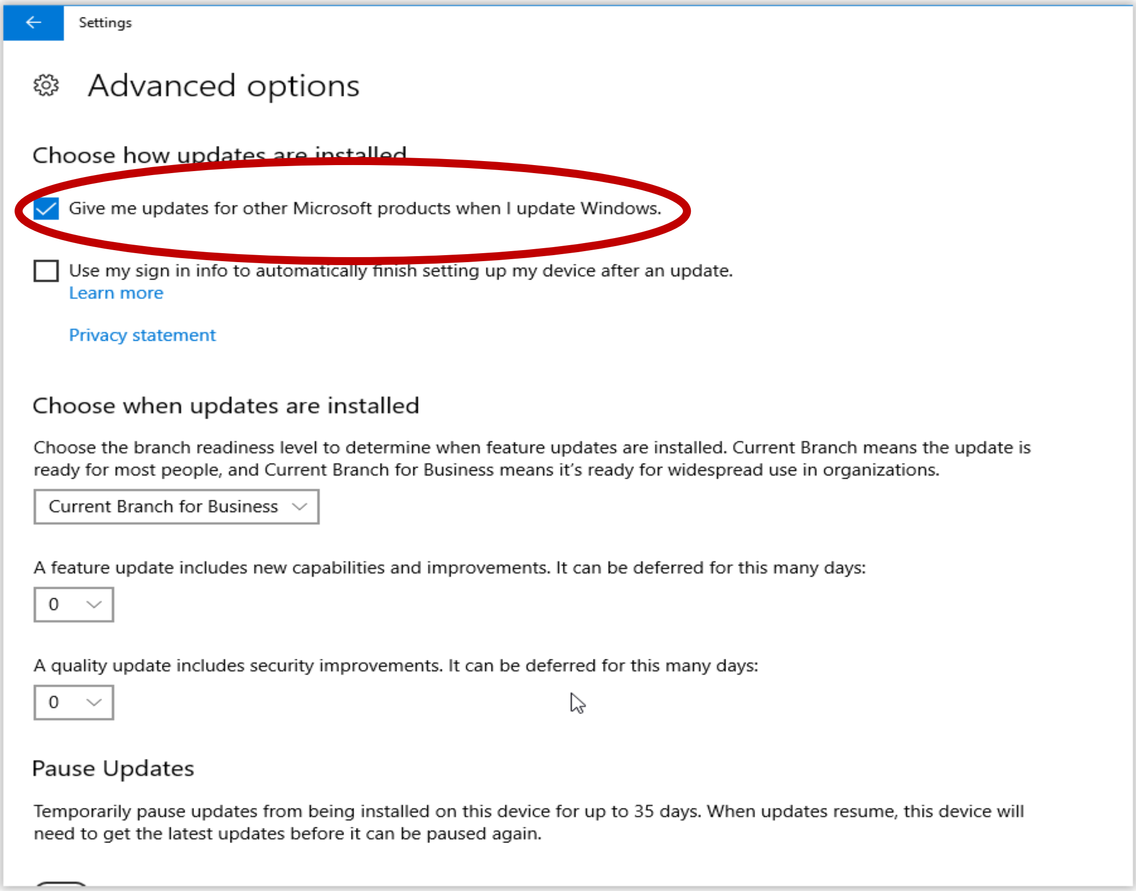
Update settings

We'll automatically download and install updates, excep
may apply). In that case, we'll automatically download o
Windows running smoothly.

Looking for info on the latest updates?

Make sure the box is checked at: “Give me updates for other Microsoft products when I update Windows”

For compatibility reasons, one might choose when updates are installed. The recommendation for business continuity would be to pick: “Current Branch for Business” as updates are able to cause problems as well, this way it will have been more thoroughly tested.



Advanced options

Choose how updates are installed

☑ Give me updates for other Microsoft products when I update Windows.

□ Use my sign in info to automatically finish setting up my device after an update.
Learn more

Privacy statement

Choose when updates are installed

Choose the branch readiness level to determine when feature updates are installed. Current Branch means the update is ready for most people, and Current Branch for Business means it’s ready for widespread use in organizations.

Current Branch for Business

A feature update includes new capabilities and improvements. It can be deferred for this many days:

0

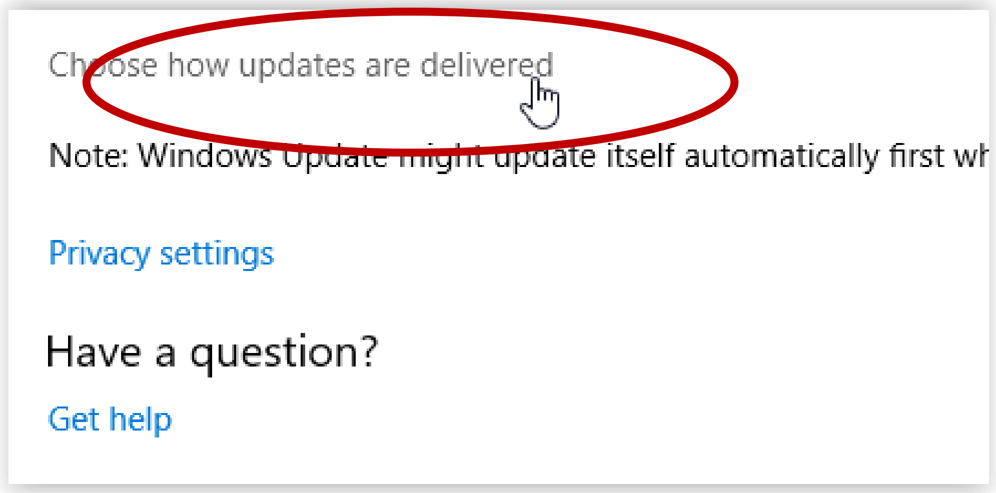
A quality update includes security improvements. It can be deferred for this many days:

0

Pause Updates

Temporarily pause updates from being installed on this device for up to 35 days. When updates resume, this device will need to get the latest updates before it can be paused again.

Scroll down and click on “Choose how updates are delivered”



Choose how updates are delivered

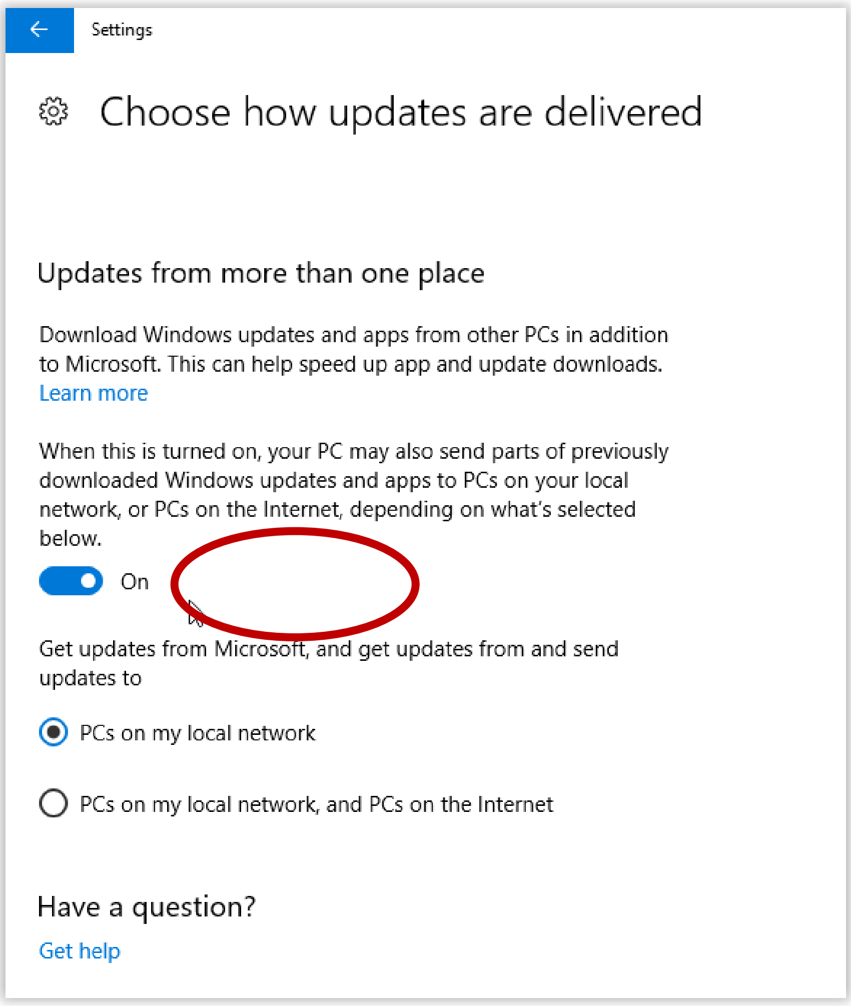
Note: Windows Update might update itself automatically first wh

Privacy settings

Have a question?

Get help

If there are multiple windows computers on the network leaving the setting like this will ensure it makes the most of your internet connection:



Settings

Choose how updates are delivered

Updates from more than one place

Download Windows updates and apps from other PCs in addition to Microsoft. This can help speed up app and update downloads. Learn more

When this is turned on, your PC may also send parts of previously downloaded Windows updates and apps to PCs on your local network, or PCs on the Internet, depending on what's selected below.

On

Get updates from Microsoft, and get updates from and send updates to

● PCs on my local network

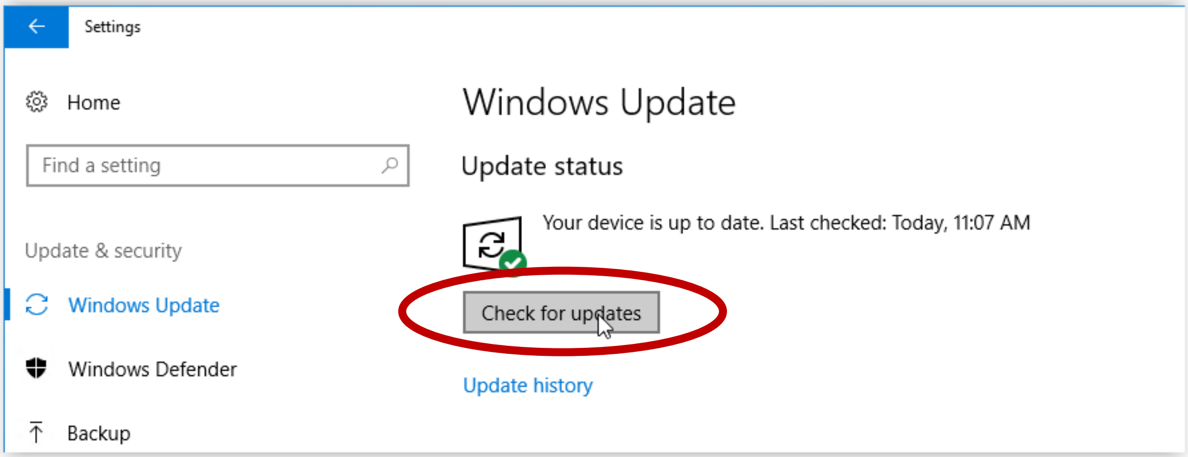
○ PCs on my local network, and PCs on the Internet

Have a question?

Get help

If there is just one Windows computer this setting can be turned off.

To perform a manual update of Microsoft applications and the Operating system click “Check for Updates”



Your device is up to date. Last checked: Today, 11:07 AM

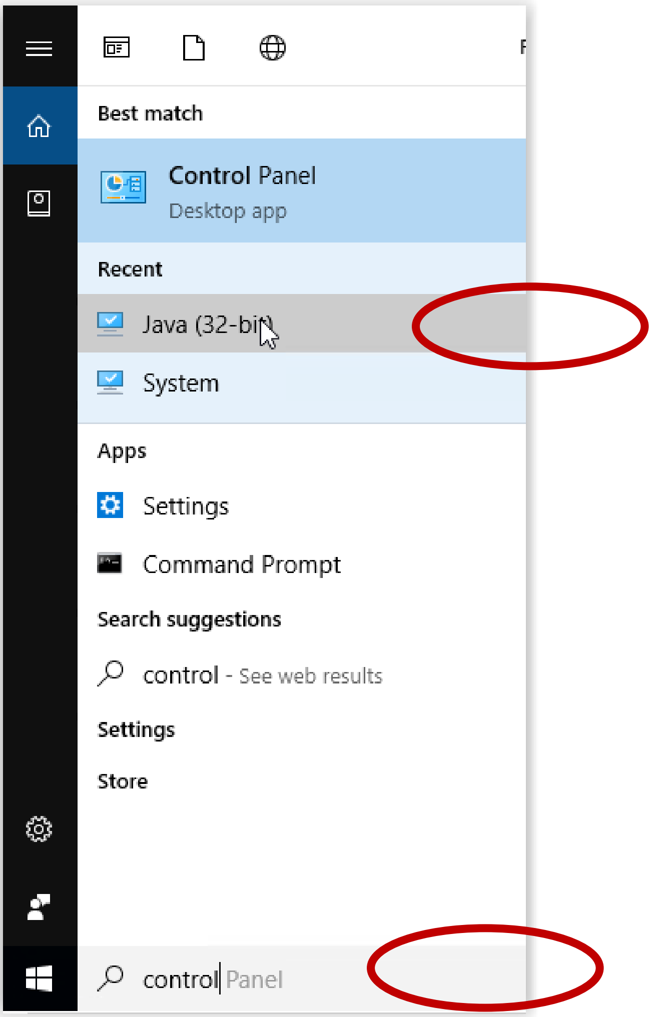
Keeping Commonly Used Applications up to Date

A lot of commonly available software needed to extend the functionality of the operating system tends to come with update functionality as well. It would be impossible to describe all of them but these would be the most common ones and targeted a lot by miscreants with malicious intent:

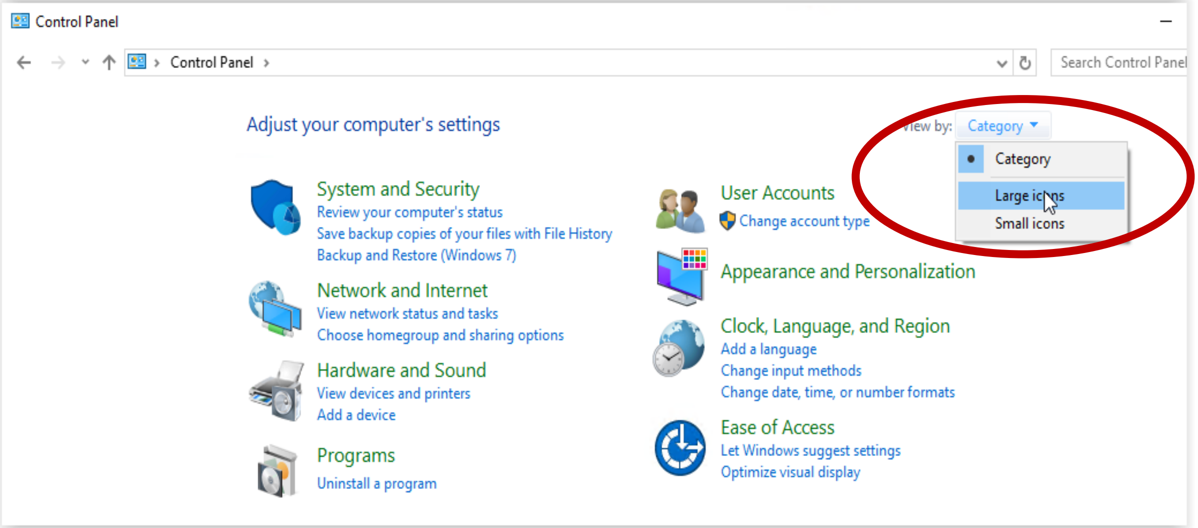
12.3.2: Java

Java has a management tool which can be found in the windows control panel

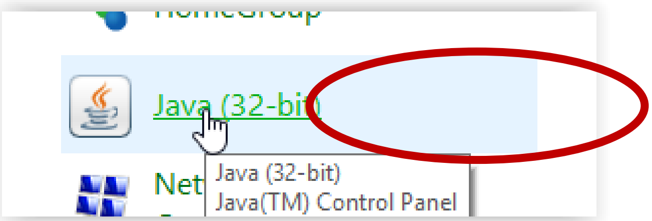
To access it start typing “control panel” in the windows search box and click on “Control Panel”



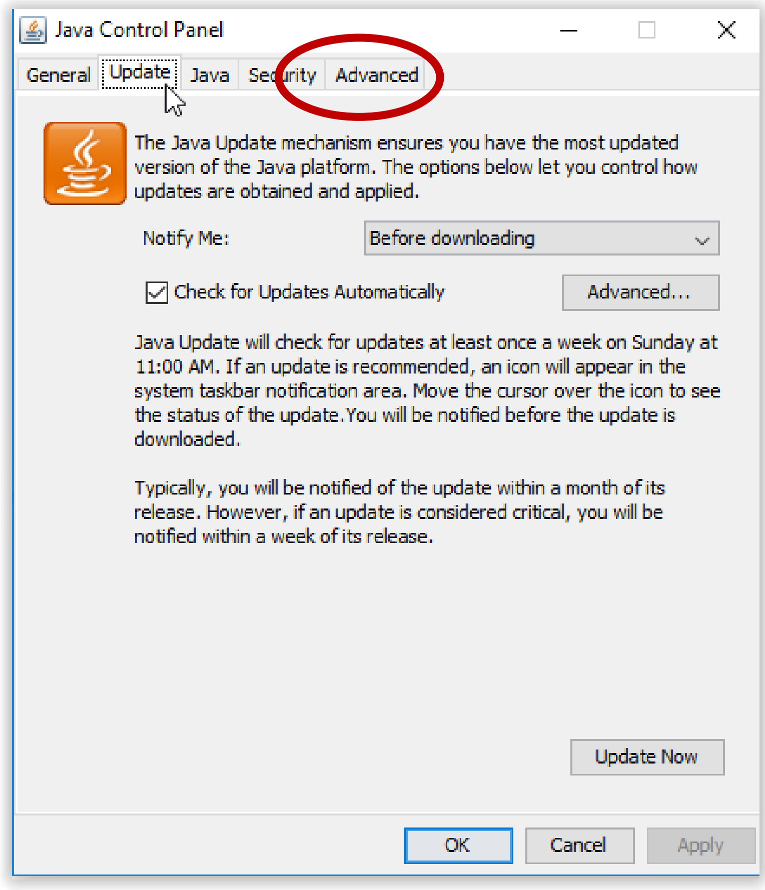
Change the View by to “Large icons”


Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
Category
Large icons
Small icons
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock, Language, and Region
Add a language
Change input methods
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

Open “Java (32-bit)



Select the “Update” tab in there and check the settings.



The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied.

Notify Me: Before downloading

☑ Check for Updates Automatically

Java Update will check for updates at least once a week on Sunday at 11:00 AM. If an update is recommended, an icon will appear in the system taskbar notification area. Move the cursor over the icon to see the status of the update.You will be notified before the update is downloaded.

Typically, you will be notified of the update within a month of its release. However, if an update is considered critical, you will be notified within a week of its release.

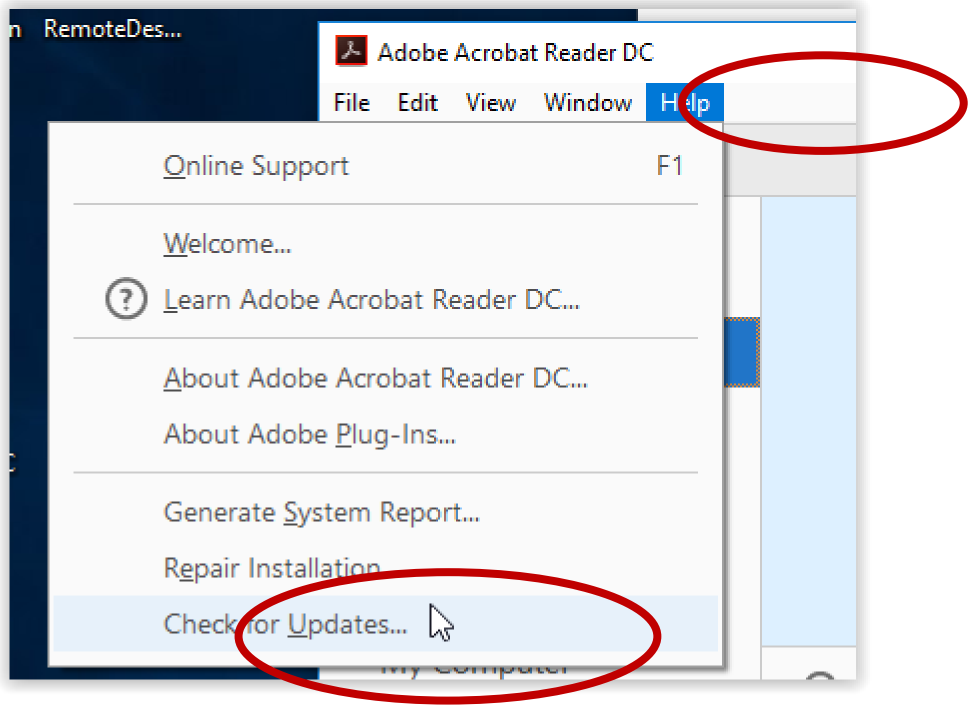
The default settings will have auto update on as well and there is a button to perform a manual update by clicking: “Update Now”

12.3.3: Adobe Reader

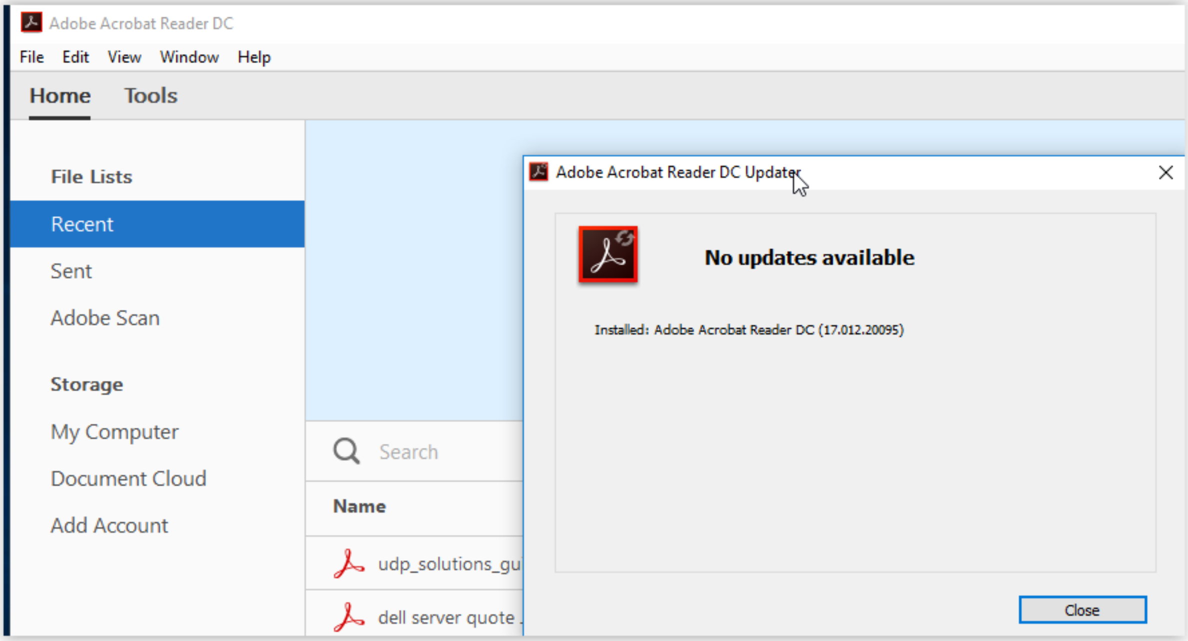
Adobe reader is a tool used to open PDF documents.

It’s been targeted a great deal by malware creators and other miscreants.

The update can be found in the program itself, go to “Help” and click: “Check for Updates…”



Running it will either update the software or return the up to date status:



No updates available

Installed: Adobe Acrobat Reader DC (17.012.20095)

12.4: Running Anti Malware Software

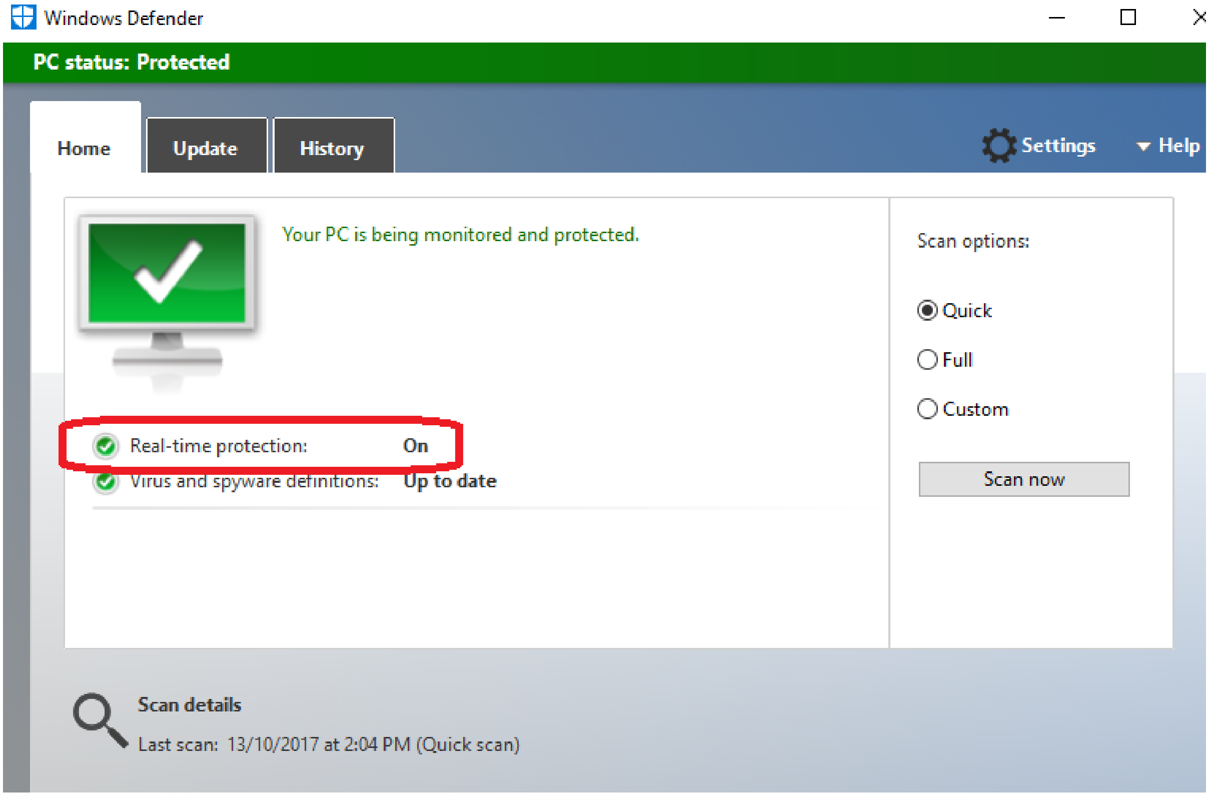
Microsoft Windows has an inbuilt anti-virus software that helps you identify and remove viruses, spyware, and other malicious software.

Windows Defender Antivirus is built-in to Windows. There's nothing to buy and nothing to install. No configuration, and no subscriptions.

Windows Defender runs in the background and notifies you when you need to take specific action. However, you can use it anytime to scan for malware if your computer isn't working properly or if you clicked a suspicious link online or in an email message.

Question: How do I know whether Windows Defender is running or not?

Answer: Just ask Cortana or type "Windows Defender" in the task bar search box. If you see a "Real-time protection: On" message, you're good to go.



PC status: Protected

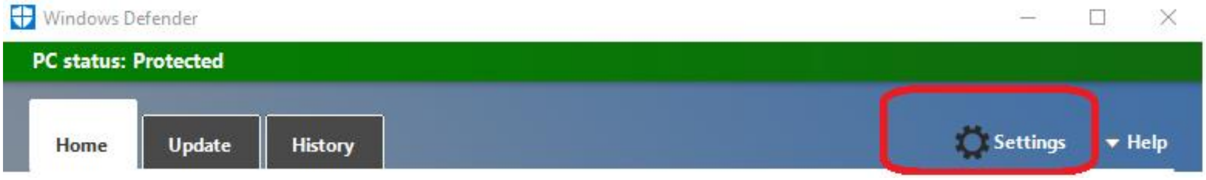
Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Up to date

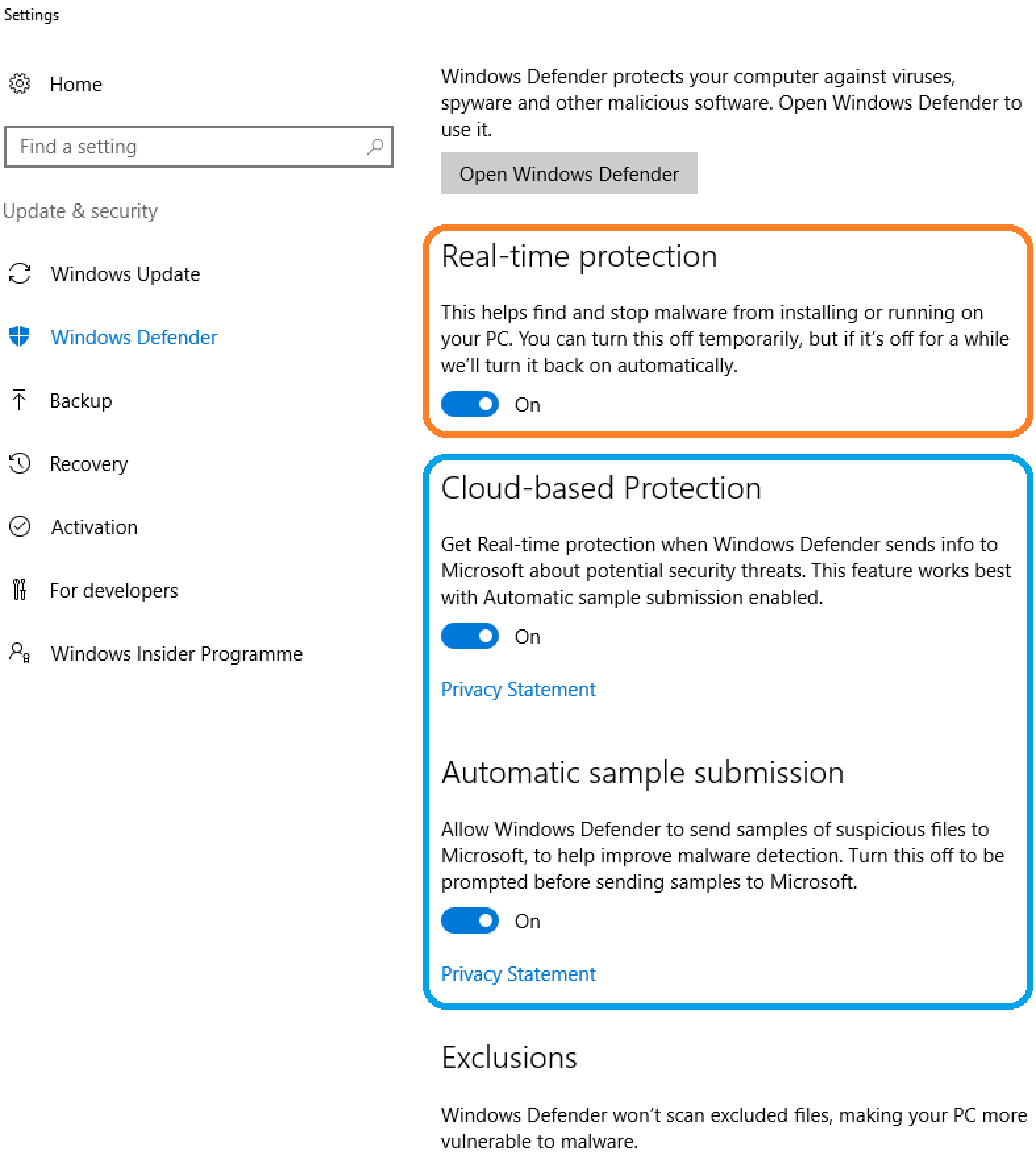
Last scan: 13/10/2017 at 2:04 PM (Quick scan)

Click on "Settings" and you will get the following:



PC status: Protected

Make sure that “Real-time protection” is set to On



Settings

Windows Defender protects your computer against viruses, spyware and other malicious software. Open Windows Defender to use it.

Real-time protection

This helps find and stop malware from installing or running on your PC. You can turn this off temporarily, but if it’s off for a while we’ll turn it back on automatically.

● On

Cloud-based Protection

Get Real-time protection when Windows Defender sends info to Microsoft about potential security threats. This feature works best with Automatic sample submission enabled.

● On

Automatic sample submission

Allow Windows Defender to send samples of suspicious files to Microsoft, to help improve malware detection. Turn this off to be prompted before sending samples to Microsoft.

● On

Exclusions

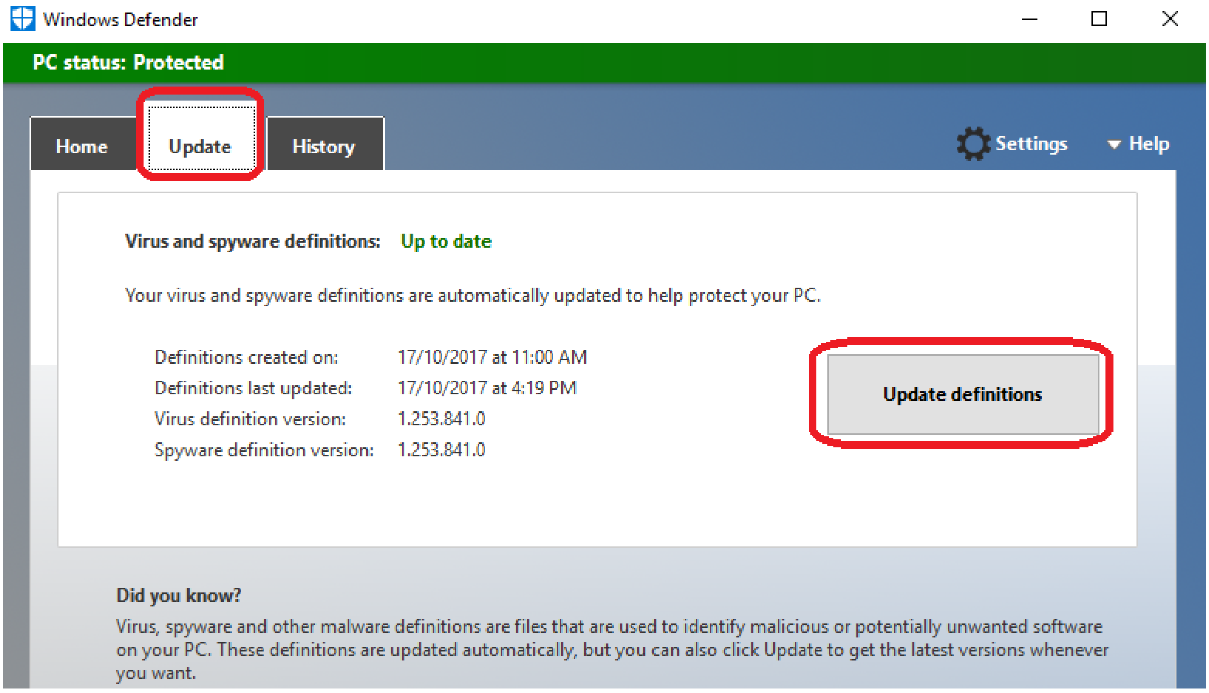
Windows Defender won’t scan excluded files, making your PC more vulnerable to malware.

Question: I’m having Problems with My Windows Defender running?

Answer: It maybe because you may already have another anti virus software. If you want to use Windows Defender Antivirus, uninstall all of your other antivirus programs and Windows Defender Antivirus will automatically turn on. You may be asked to restart your device.

Question: Am I up to date?

Answer: You can manually get the latest update by clicking on “Update definitions”



Virus and spyware definitions: Up to date

Your virus and spyware definitions are automatically updated to help protect your PC.

Definitions created on:	17/10/2017 at 11:00 AM
Definitions last updated:	17/10/2017 at 4:19 PM
Virus definition version:	1.253.841.0
Spyware definition version:	1.253.841.0

Did you know?

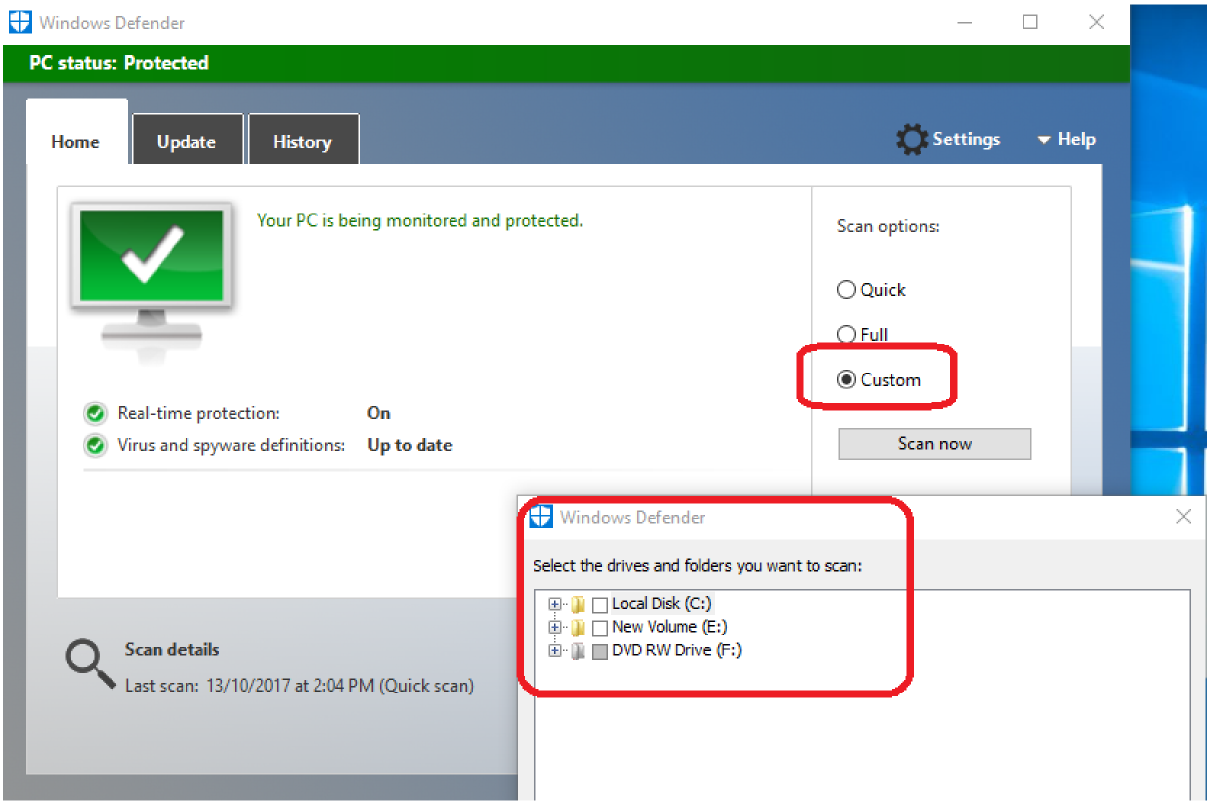
Virus, spyware and other malware definitions are files that are used to identify malicious or potentially unwanted software on your PC. These definitions are updated automatically, but you can also click Update to get the latest versions whenever you want.

Question: How do run a scan and how often?

Answer: It is suggested to run a Full scan on your machine once a week. This is going to be by far more accurate than quick scan.

Question: How do I scan attached drives?

Answer: You can “custom scan”. This will provide you with options of what you want to scan



Windows Defender

PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

○ Quick

○ Full

● Custom

Scan details

Last scan: 13/10/2017 at 2:04 PM (Quick scan)

Windows Defender

Select the drives and folders you want to scan:

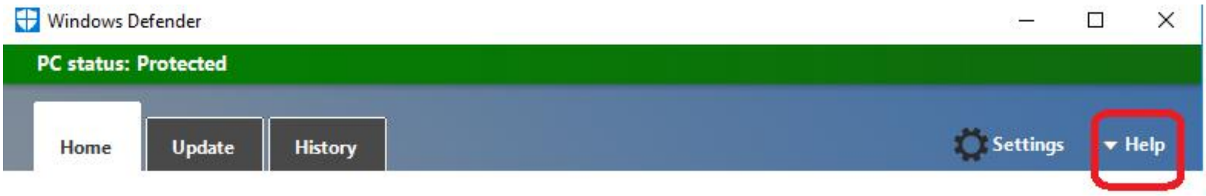
□ Local Disk (C:)

□ New Volume (E:)

□ DVD RW Drive (F:)

Question: How do I submit malicious software samples?

Answer: Under the “Help”, you can then click on “Submit Malicious Software samples”. This will then take you to a Microsoft web site. Then follow the process for submitting a file.



Windows Defender

PC status: Protected

Question: Where else can I find more information about Windows Defender?

Answer: By clicking on “Community” under the Help button.

Question: What is Action Centre?

Answer: Action Centre, previously known as Windows Security Centre, monitors the security status of the computer

- On the right end of the taskbar, select the Action Centre 🗨 icon OR
- Press the Windows logo key Windows logo Start button +A OR
- On a touchscreen device, swipe in from the right edge of the screen

Question: What is the difference between Anti-Malware & Anti-Virus?

Answer: Malware is an umbrella term for any kind of malicious code, made to do harm to your computer, steal data or serve any other criminal purpose. That includes Trojans, worms, ransomware, spyware and viruses. This means viruses are malware, but not all malware are viruses.

Viruses are malicious programs meant to replicate themselves and spread. They are categorised as infectious malware, along with worms and Trojans. They infect the computer and replicate themselves to spread to more files to do damage.

Question: What is Next Generation Anti-Virus (Next Gen AV)?

Answer: Antivirus has long been the most pervasive endpoint-security technology in the world. And, for a time, it was enough. Antivirus was able to stop “most” malware attacks. As attacks evolved, antivirus remained stagnant.

Today, signature and heuristic-based antivirus, the very kind that protected us for years, catches less than half of noteworthy malicious events.

Next Gen AV is the natural evolution of traditional AV that protects computers from the full spectrum of modern cyber-attacks, delivering the best endpoint protection. It looks at two critical components:

1. Prevents unknown malware and sophisticated attacks by evaluating the context of an entire attack resulting in better prevention.
2. Remediates attacks

Question: Is Windows Defender a Next Generation Anti-Malware?

Answer: Windows Defender does a reasonably good job. However, there are other 3rd party software solutions that specialise in endpoint protection to a higher degree.

12.5: Ensuring a Fully Functional Backup and Restore Process

12.5.1: Performing a Backup

To have a safeguard against the more common crypto viruses or just data accidental loss, it is important to have a backup of all files and folders at a location inaccessible to the computer.

A portable hard drive or USB stick with enough capacity should be enough for most small businesses.

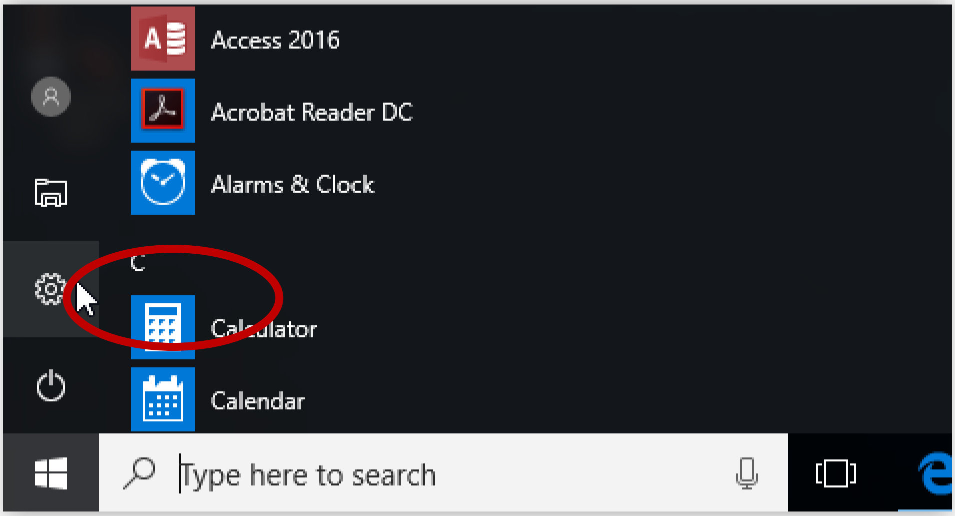
Question: Why do we want to separate the backup from the machine?

Answer: By having a physical separation you minimise the ability for malware to target your backup.

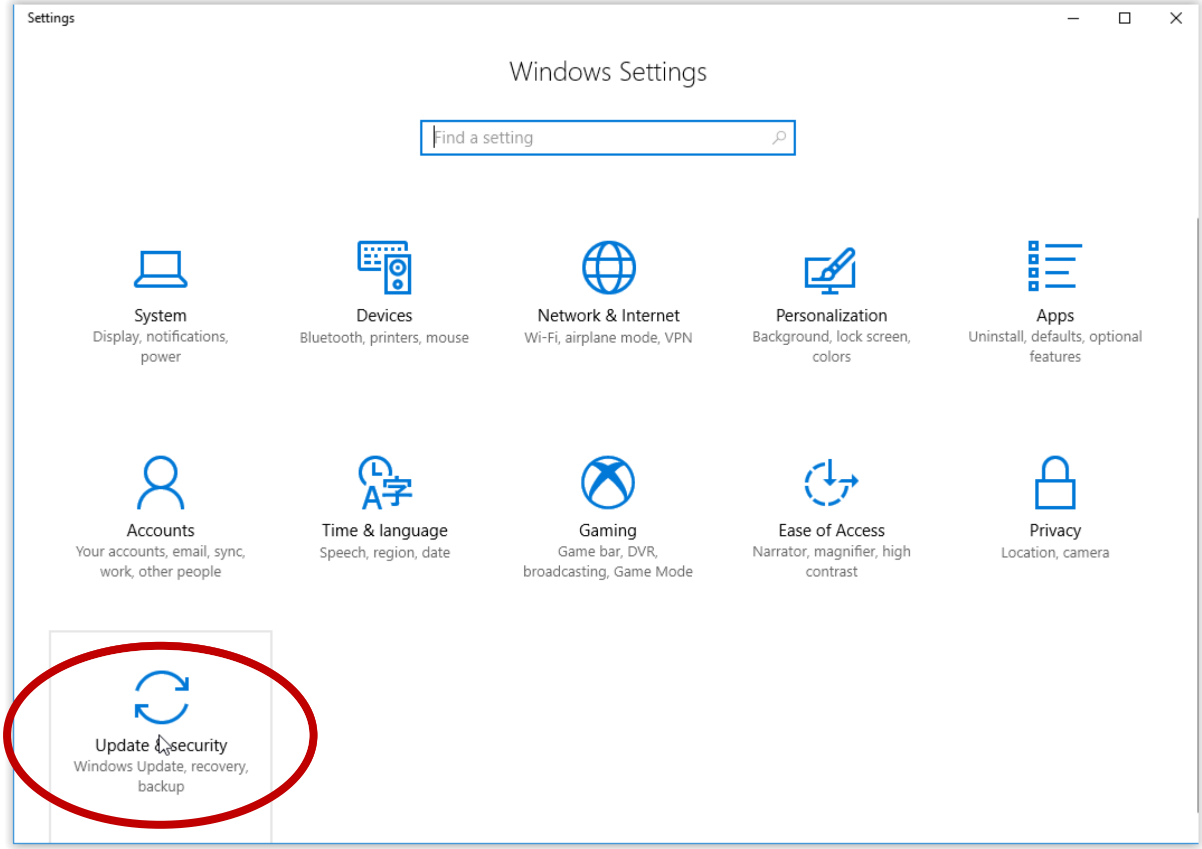
Windows 10 comes with a build-in backup functionality that is able to make use of these portable media.

Insert a portable drive into the computer first.

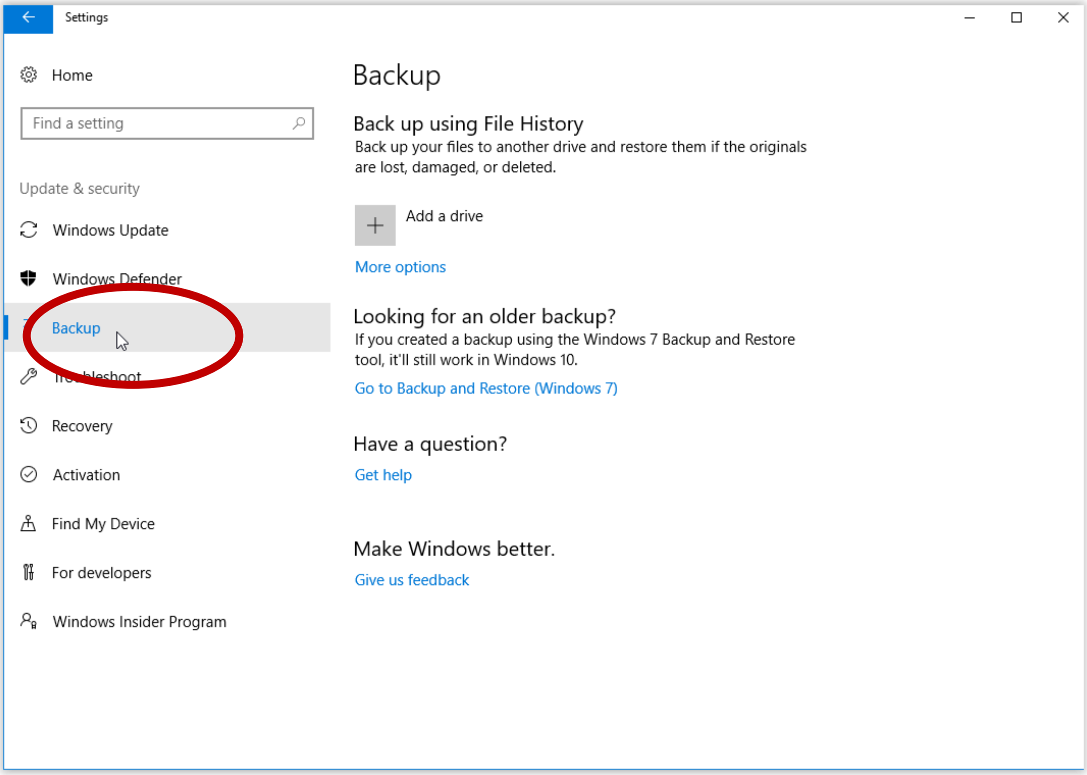
To use it click the start button and choose “Settings”



Click on “Update & security”:


Settings
Windows Settings
Find a setting
System
Display, notifications, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, other people
Time & language
Speech, region, date
Gaming
Game bar, DVR, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & security
Windows Update, recovery, backup

Choose “Backup”



Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

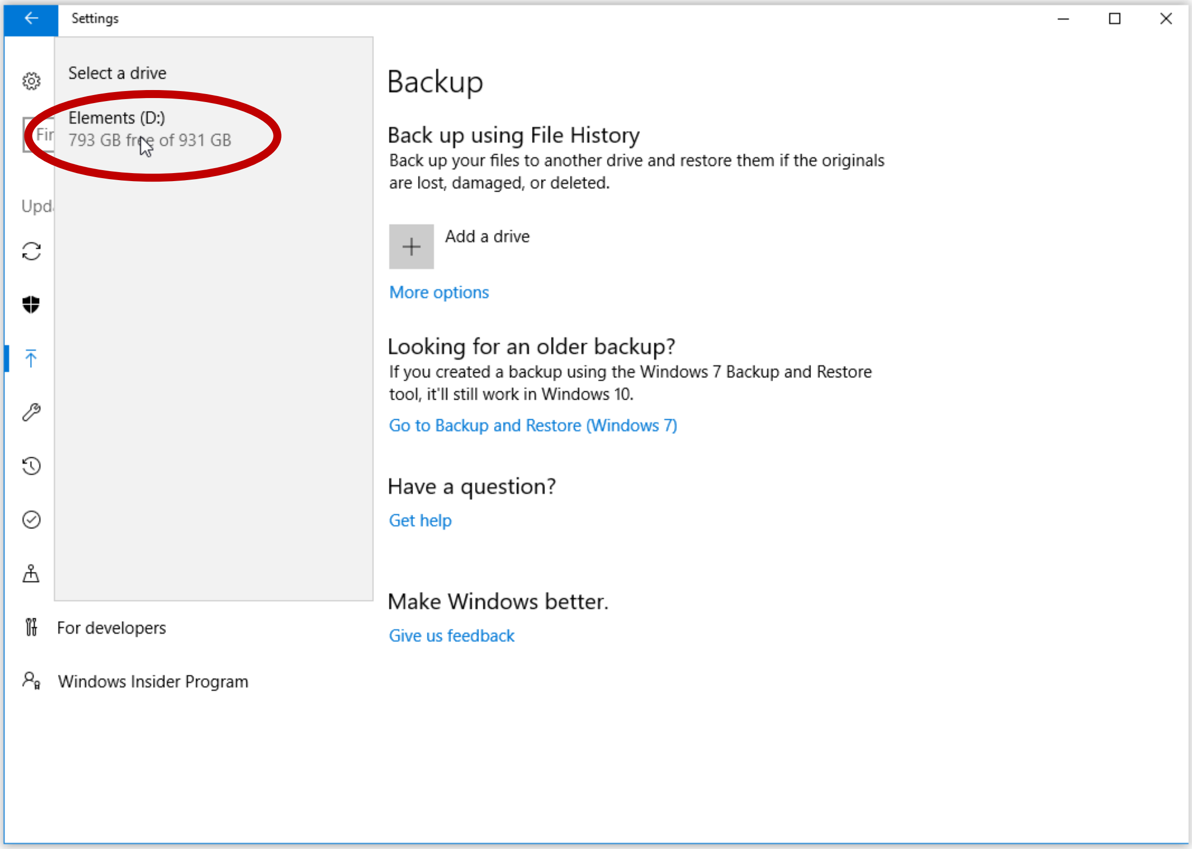
Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Have a question?

Make Windows better.

Select the drive that was inserted (It should show up in the list)



Settings

Select a drive

Elements (D:)
793 GB free of 931 GB

Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Add a drive

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

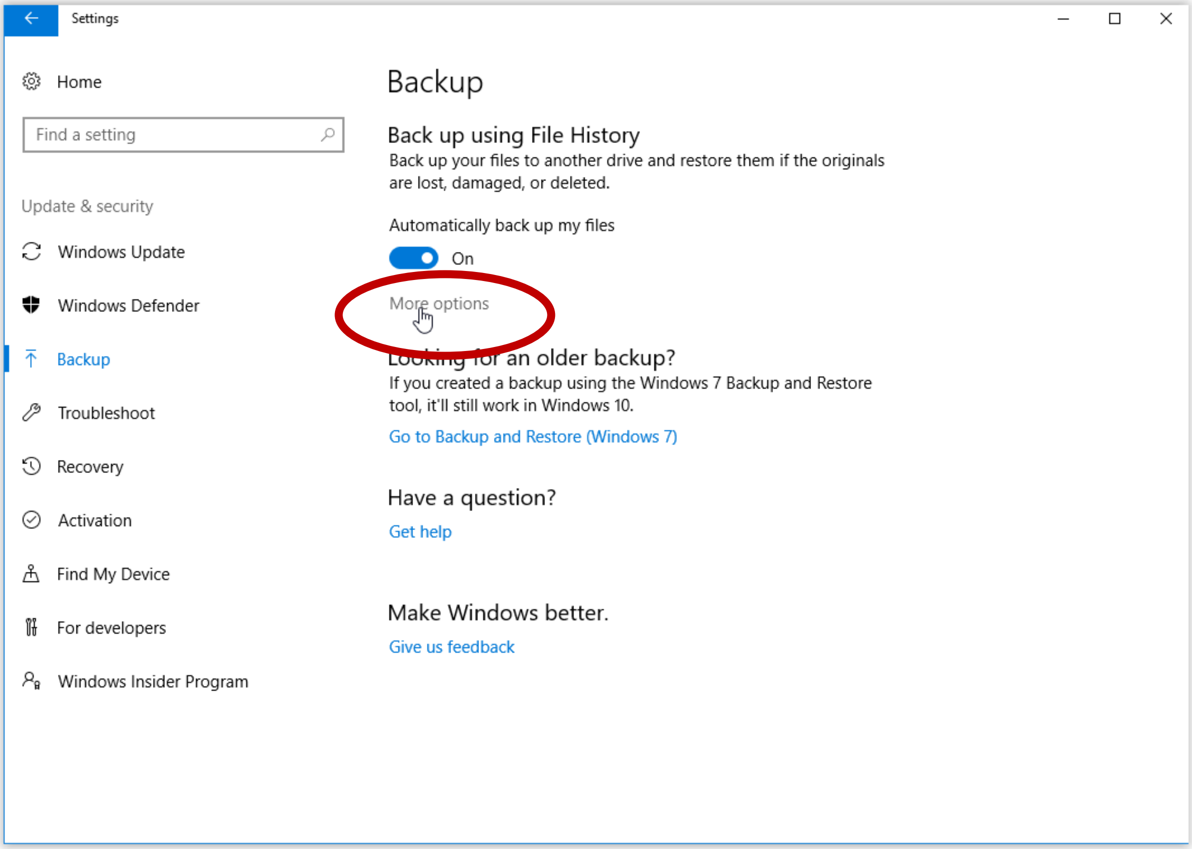
Have a question?

Get help

Make Windows better.

Give us feedback

Click on “More options”



Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Automatically back up my files

On

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

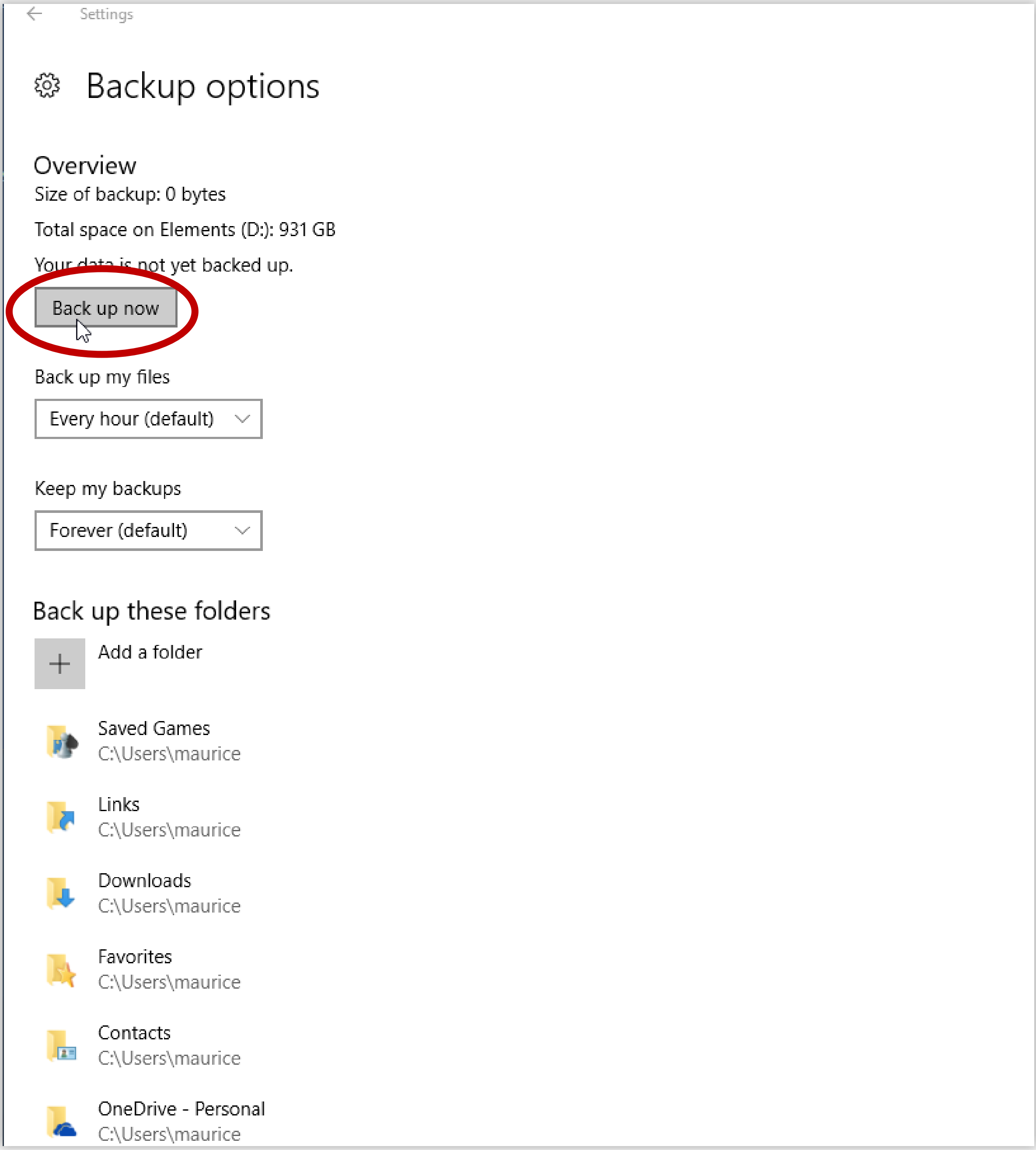
Have a question?

Get help

Make Windows better.

Give us feedback

Click on: “Back up now” in order to create a backup of the selected folders:



Settings

Backup options

Overview

Size of backup: 0 bytes

Total space on Elements (D:): 931 GB

Your data is not yet backed up.

Back up my files: Every hour (default)

Keep my backups: Forever (default)

Back up these folders

Saved Games
C:\Users\maurice

Links
C:\Users\maurice

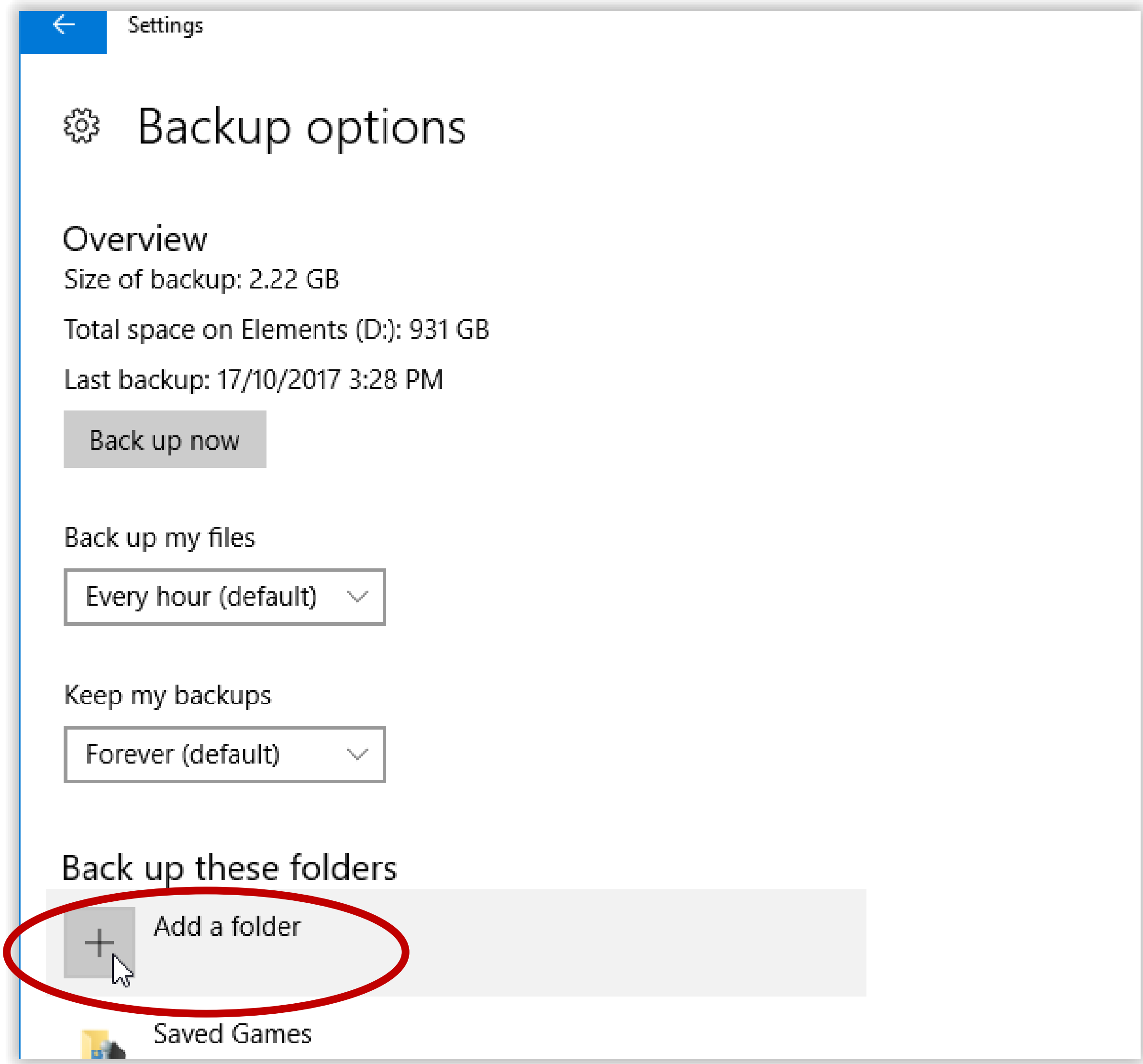
Downloads
C:\Users\maurice

Favorites
C:\Users\maurice

Contacts
C:\Users\maurice

OneDrive - Personal
C:\Users\maurice

It might be necessary to add other locations used to store data other than the default ones used by Windows. This can be done by adding these folders to the backup procedure. To do this click on: “Add a folder”:



Settings

Backup options

Overview

Size of backup: 2.22 GB

Total space on Elements (D:): 931 GB

Last backup: 17/10/2017 3:28 PM

Back up my files

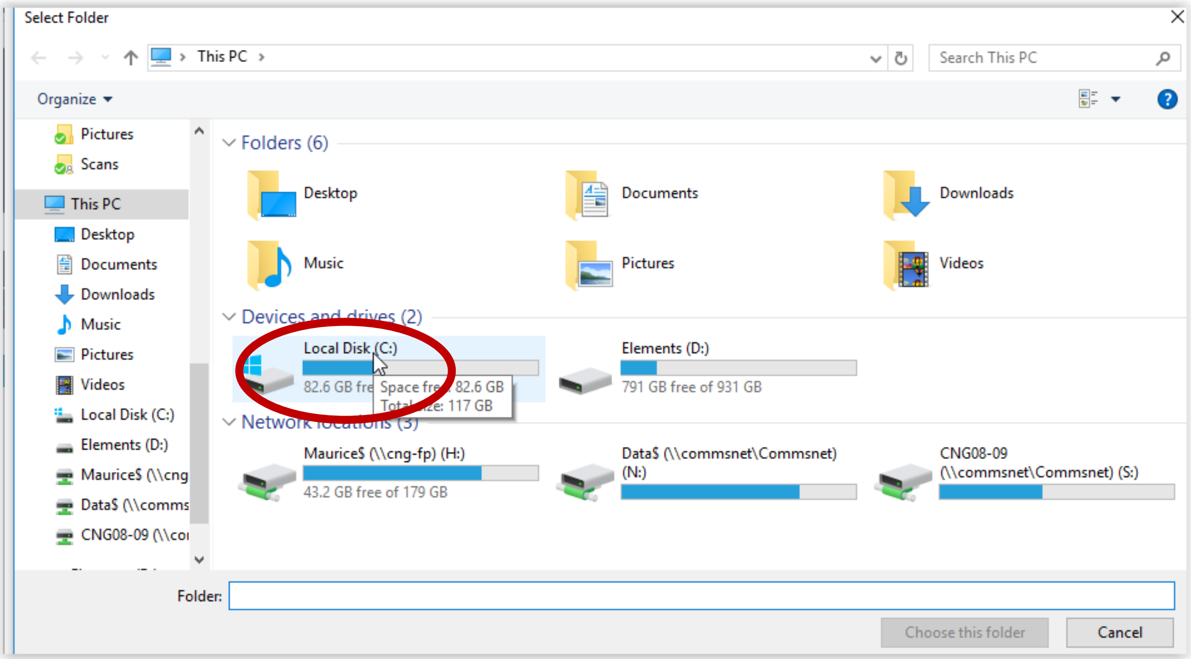
Every hour (default)

Keep my backups

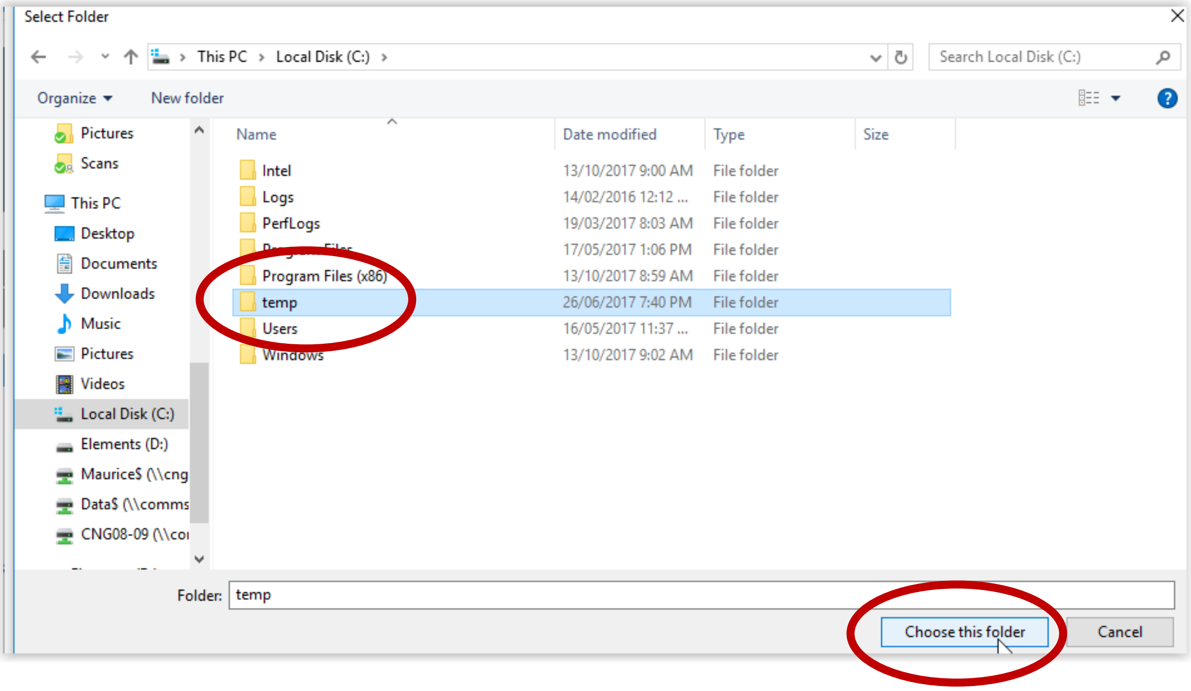
Forever (default)

Back up these folders

Go to the folder that needs backing up using the browser window:



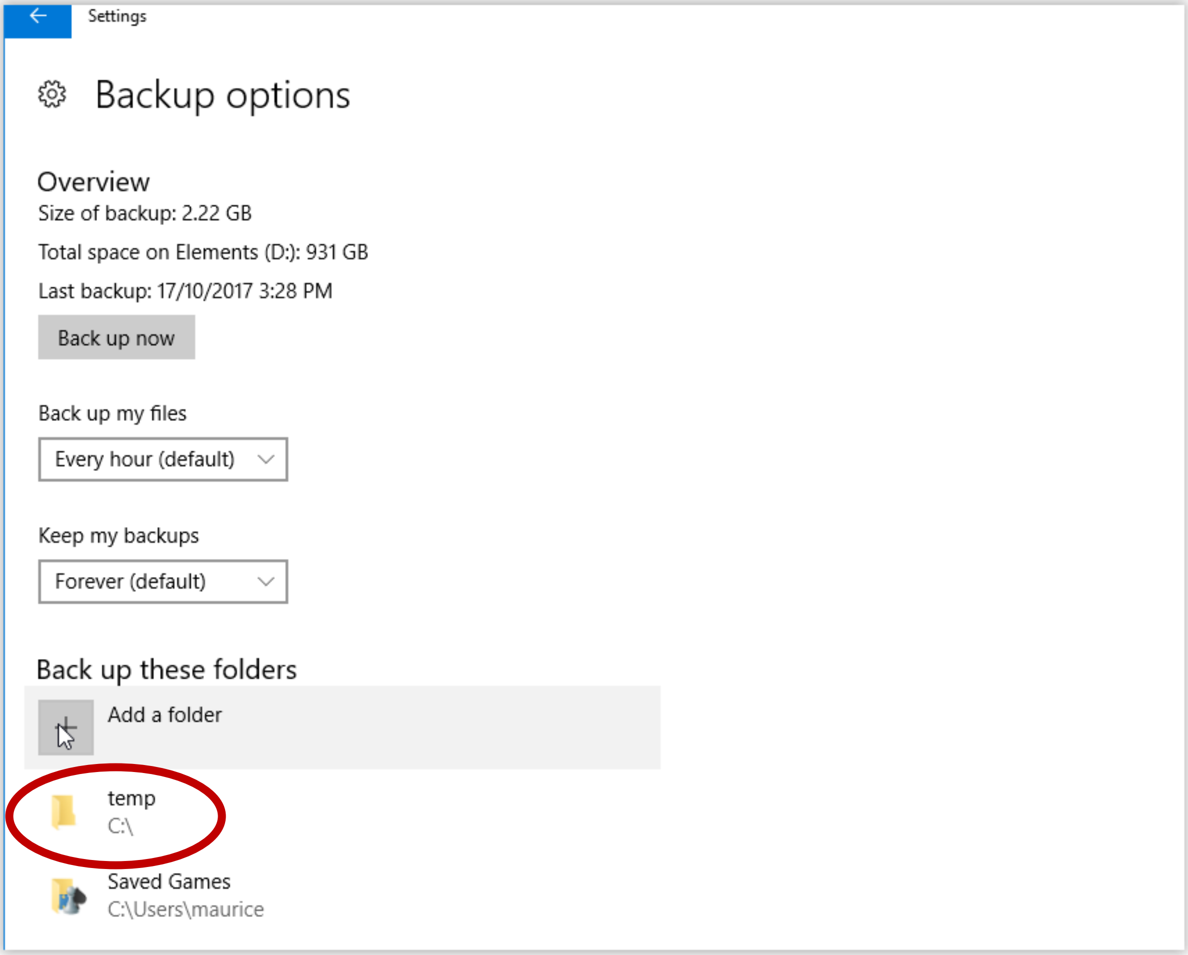
Select the folder required and click on: “Choose this folder”



Name	Date modified	Type	Size
Intel	13/10/2017 9:00 AM	File folder	
Logs	14/02/2016 12:12 ...	File folder	
PerfLogs	19/03/2017 8:03 AM	File folder	
Program Files	17/05/2017 1:06 PM	File folder	
Program Files (x86)	13/10/2017 8:59 AM	File folder	
temp	26/06/2017 7:40 PM	File folder	
Users	16/05/2017 11:37 ...	File folder	
Windows	13/10/2017 9:02 AM	File folder	

Folder: temp

The folders should now show up in the list of folders:



Backup options

Overview

Size of backup: 2.22 GB

Total space on Elements (D:): 931 GB

Last backup: 17/10/2017 3:28 PM

Back up my files: Every hour (default)

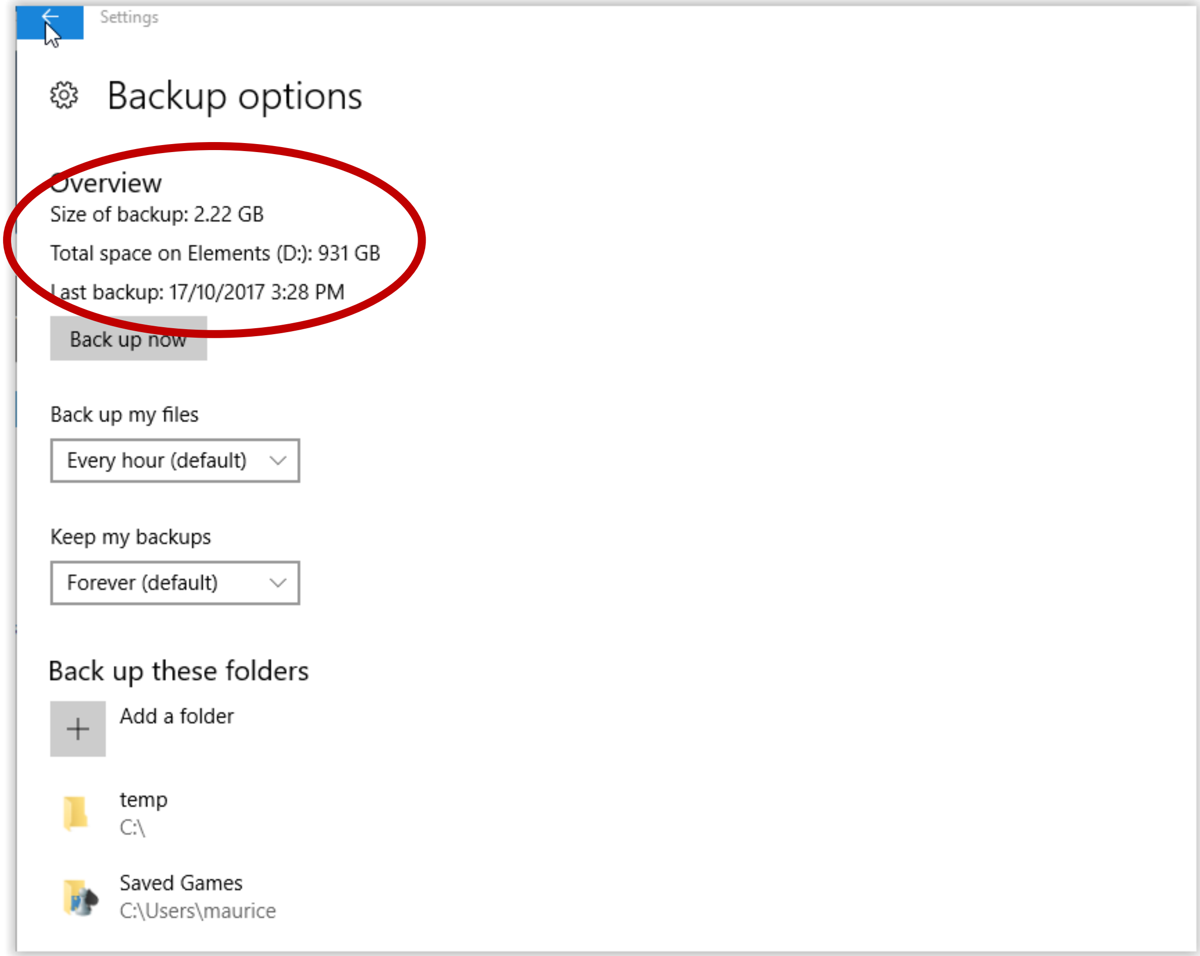
Keep my backups: Forever (default)

Back up these folders

temp
C:\

Saved Games
C:\Users\maurice

This window will now show the last created backup:



Settings

Backup options

Overview

Size of backup: 2.22 GB

Total space on Elements (D:): 931 GB

Last backup: 17/10/2017 3:28 PM

Back up my files: Every hour (default)

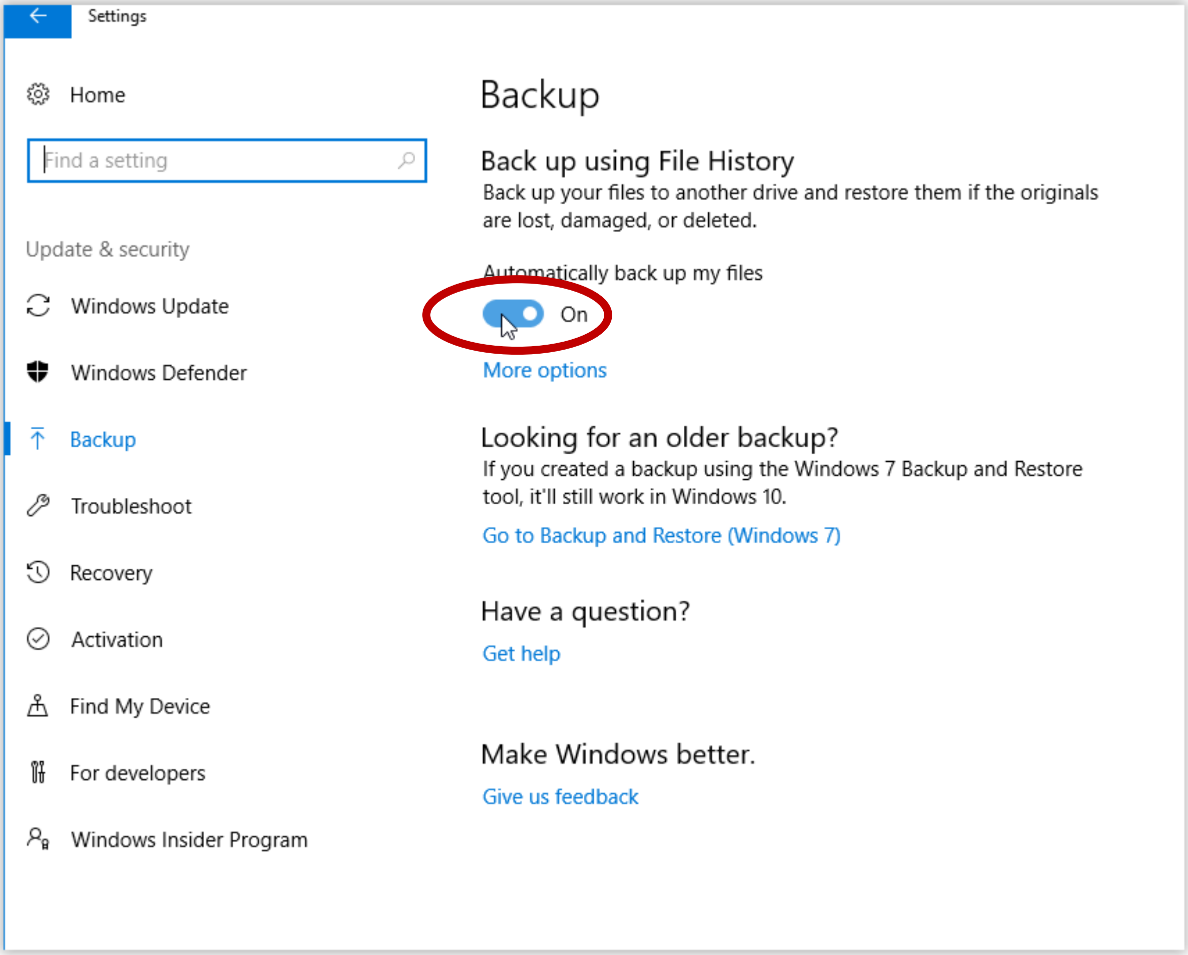
Keep my backups: Forever (default)

Back up these folders

temp
C:\

Saved Games
C:\Users\maurice

It might be a good idea to disable the automatic backup when the portable drive will be removed from the system to secure it against crypto viruses and other malware, this can be done by moving the "On" slider to the Off position, this slider will need to be moved back to the "On" position again when creating a backup:



Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Automatically back up my files

On

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

Have a question?

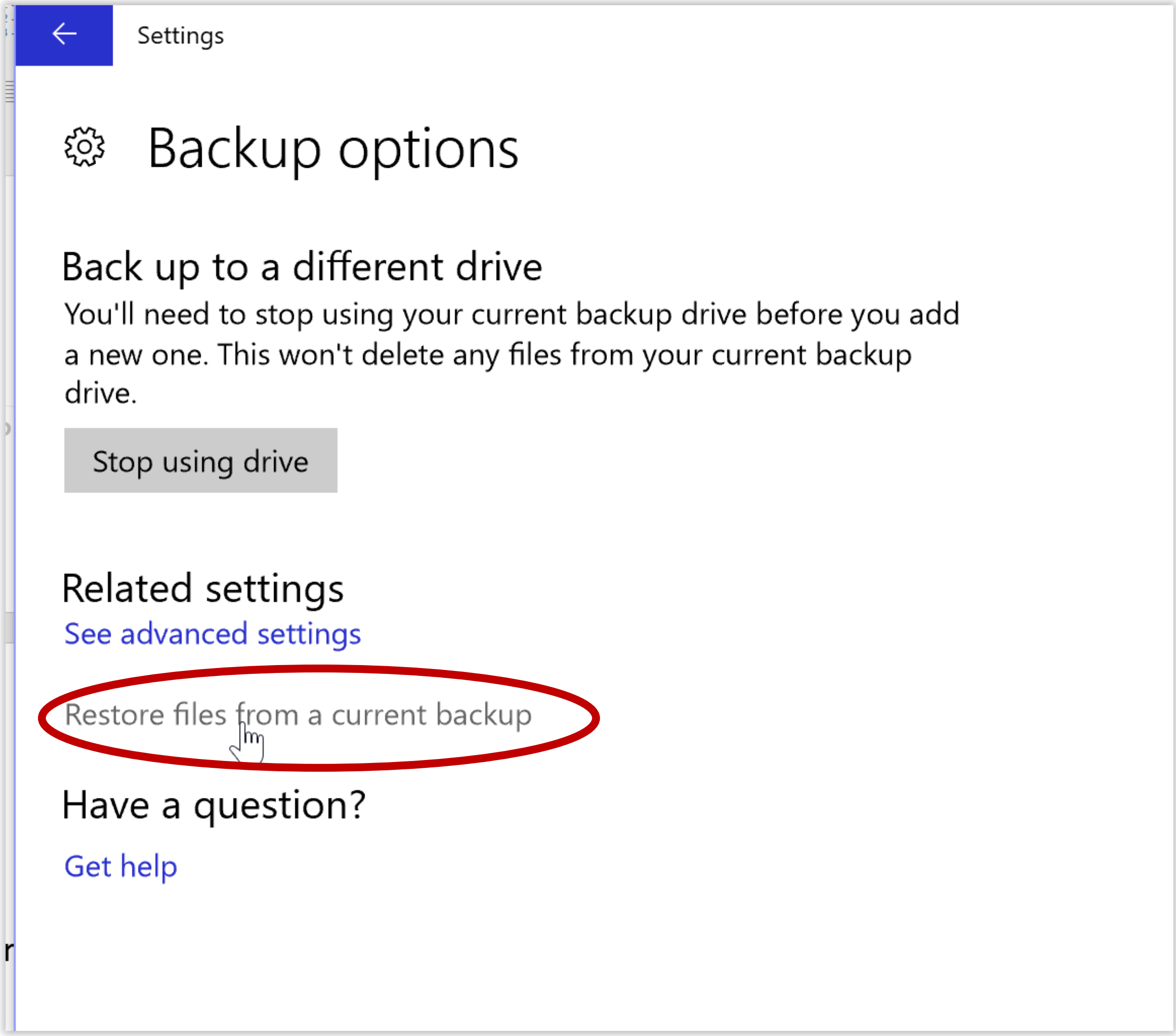
Get help

Make Windows better.

Give us feedback

12.5.2: Performing a Restore

Scroll all the way down in the backup options screen until you reach: "Restore files from a current backup" and click on it



Settings

Backup options

Back up to a different drive

You'll need to stop using your current backup drive before you add a new one. This won't delete any files from your current backup drive.

Stop using drive

Related settings

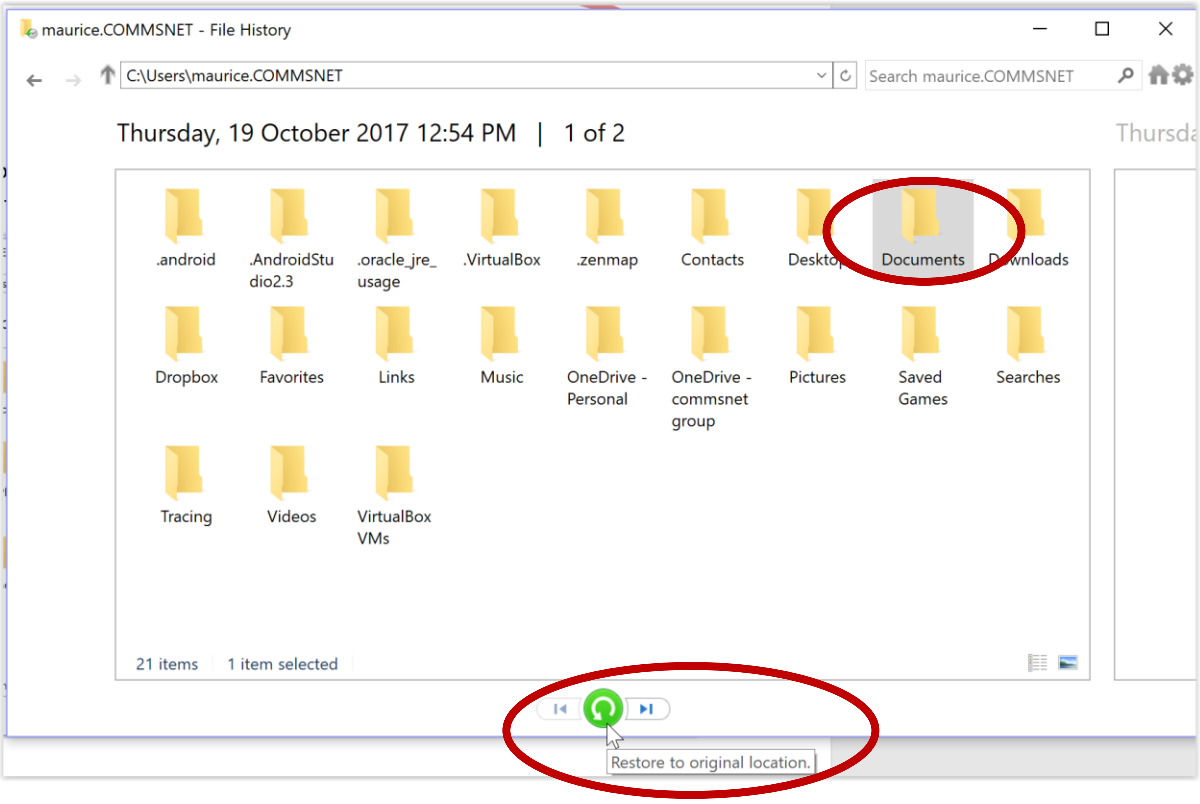
See advanced settings

Restore files from a current backup

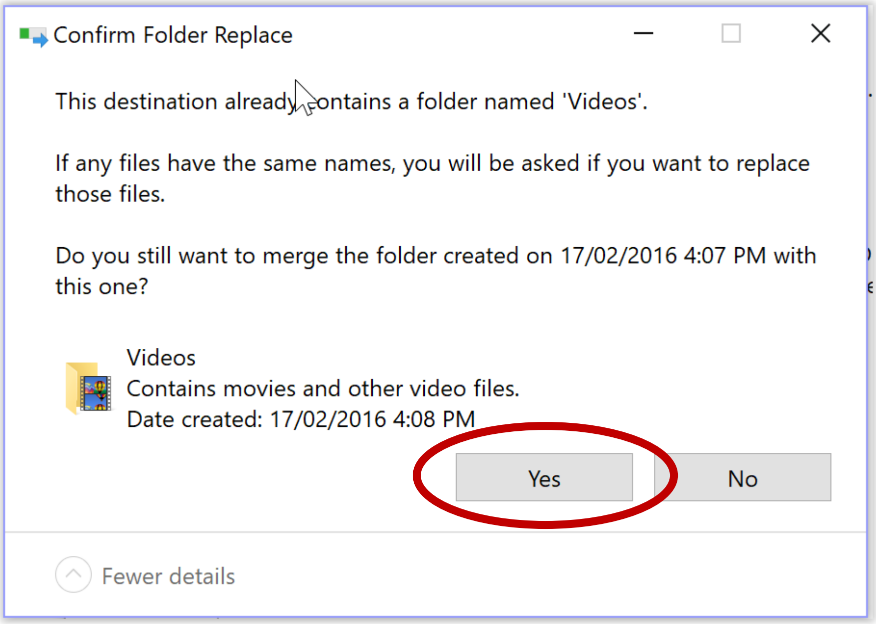
Have a question?

Get help

Select the folder you want to restore and if you want it to be restored to the original location click on the green button in the bottom mid section



This will pop up a warning, if you want to overwrite click “Yes”:



Confirm Folder Replace

This destination already contains a folder named 'Videos'.

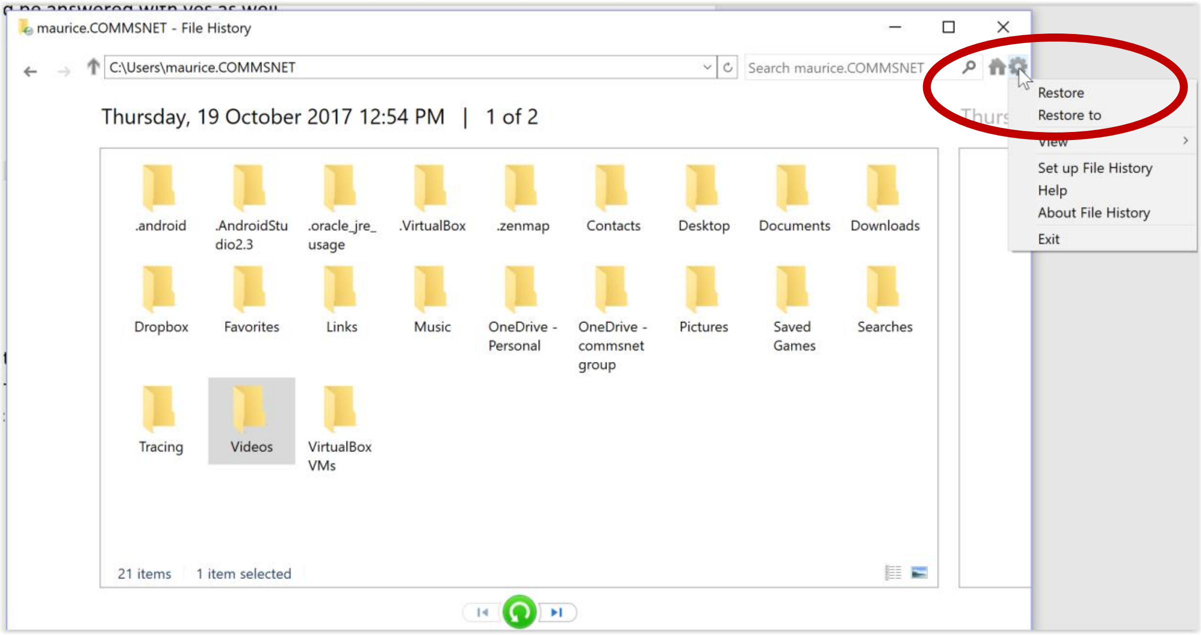
If any files have the same names, you will be asked if you want to replace those files.

Do you still want to merge the folder created on 17/02/2016 4:07 PM with this one?

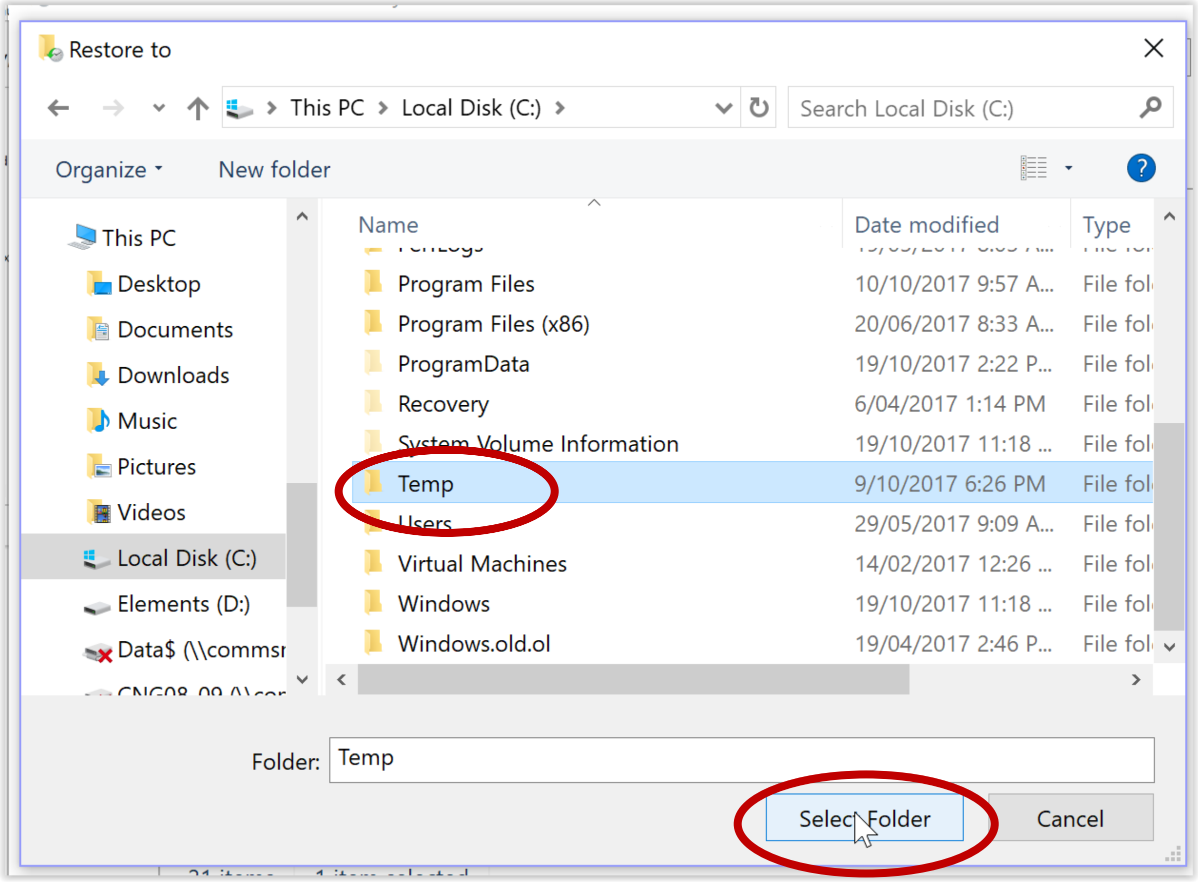
Videos
Contains movies and other video files.
Date created: 17/02/2016 4:08 PM

This will restore the files and might ask for confirmation during the process which should be answered with yes as well.

If you do not want to overwrite the current location (e.g. you want to restore a previous version because you want to compare you can opt for a restore to a different location, this is done by clicking on the option cogwheel and choosing “Restore to”:



Select the alternative location where you want to perform the restore and click: “Select Folder”:



Name	Date modified	Type
Program Files	10/10/2017 9:57 A...	File fol
Program Files (x86)	20/06/2017 8:33 A...	File fol
ProgramData	19/10/2017 2:22 P...	File fol
Recovery	6/04/2017 1:14 PM	File fol
System Volume Information	19/10/2017 11:18 ...	File fol
Temp	9/10/2017 6:26 PM	File fol
Users	29/05/2017 9:09 A...	File fol
Virtual Machines	14/02/2017 12:26 ...	File fol
Windows	19/10/2017 11:18 ...	File fol
Windows.old.ol	19/04/2017 2:46 P...	File fol

Folder: Temp

This will restore the required folder to the selected location and will open it in the Windows Explorer.

Close all remaining backup windows afterwards.

12.6: Adopting Best Practice User Awareness

12.6.1: Password Best Practice

We all know that strong passwords are all that stands between us and a potential security breach. The number one most commonly used password is “123456,” and the fourth most commonly used is “Password.” Your own name is also a common choice. So, any password attacker and cracker would try these three passwords immediately.

Other weaknesses are how users choose and manage them:

- ✘ Simple passwords—Short in length, that use words found in dictionaries
- ✘ Passwords others can find—On sticky notes on monitors, in a notepad by
- ✘ Using the same password—Using the same password for multiple sites, never
- ✘ Shared passwords—Users posting password notes on their screens; sending unencrypted emails with password information; using same password for all their accounts.
- ✘ Allowing your browsers to save your logins and basic information for automatic form-filling. This convenient, but definitely not a secure option.

Choosing a good password is an important part of lowering the risk of becoming the victim. The following guidelines should help you when choosing passwords for your online accounts.

- ✓ Make your passwords memorable, so that you don’t have to write them down or store them in a file on your computer
- ✓ Never use real words that a hacker or cybercriminal can find in a dictionary.
- ✓ Don’t use obvious passwords that can be easily guessed, such as your spouse’s name, your child’s name, pet’s name, car registration, postcode, etc.
- ✓ Use a mixture of uppercase and lowercase letters, numbers and non- alphanumeric characters such as punctuation marks.
- ✓ Don’t recycle passwords, e.g. don’t use ‘password1’, ‘password2’, ‘password3’, etc. for different accounts.
- ✓ If possible, use a passphrase, rather than a single word, e.g. “this is how it is done.”
- ✓ Make the password long. Many sites enforce a minimum password length and often add additional requirements (such as a mixture of lower case, upper case, number, and punctuation).
- ✓ Don’t use the same password for multiple accounts. If a cybercriminal finds the password to one account, they can use it to access other accounts.
- ✓ Don’t share your passwords with others.
- ✓ Changing passwords on regular basis is a good idea, but it is troublesome to remember. Suggestion: develop a strong password instead.

Having troubles remembering password for too many accounts?

Remembering a single password is relatively easy. However, remembering twenty unique passwords or even more is a tough challenge.

Use a Password Manager. A password manager is a software application that is used to store and manage the passwords that a user has for various online accounts and security features. Password managers store the passwords in an encrypted format and provide secure access to all the password information with the help of a master password.

12.6.2: Internet Usage Best Practice

Like the real physical world, the Internet present a mirror image of the benefits as well as the dangers that it provides.

Just as you take the physical precautions to protect your wellbeing, your family, and your assets, you need to take similar precautions regarding your digital life.

The Internet presents amazing opportunities. But with that comes the horror of deceit, scams, identity theft, financial theft, ransomware, hacktivism, fraudsters, espionage, and much more.

How well you manage not to be duped & tricked will all be down to you. Using the Internet is easy. But using the Internet safely is by far more difficult than it looks.

There are a number of key thumb rules that you must adopt. Think of it like the road rules. By following these rules, you will ensure that your business, yourself and associated assets will be relatively safe.

1. Only access the Internet only from safe device.
2. Only access sensitive websites such as bank websites from non-public Wi-Fi sites. Public Wi-Fi allows hackers to sniff the network and thereby copying your credentials
3. Only browse known websites. Check the website address to see if it is genuine;
4. If the web browser asks you to save your password, ignore. Keep your passwords safe by using a Password Manager. There are many free 3rd party solutions, like Lastpass (www.lastpass.com)
5. If the website requests your personal details, ignore;
6. If you receive a warning notification asking you to install software on your machine, ignore;
7. If you receive a “pop-up” add, ignore it.
8. Be very wary of websites promoting schemes, especially those that involve recruitment of others, receiving money for other people or advance payments;
9. Only download software from reputable sites. Be aware that files download from Torrent or other peer-to-peer can be infected with malware.
10. Scan all download attachments. Save it in “downloadable folder” and then scan it with your AV before opening it.
11. Never post personal information anywhere on the Internet, including social media sites such as: Where you live, your data of birth, credit card details, driver’s license, and any other sensitive data;
12. Do not share other personal information online;
13. Don’t believe everything your read is real. There are many scams.
14. Disallow employees to download or upload obscene, offensive or illegal material
15. Disallow employees to download music, videos and other 3rd party pirated programmes.

12.6.3: Email Usage Best Practice

Let's be clear about this. Email is the number one application on the Internet today. Email is the digital entry point to every business. For this reason, it is also the number one vehicle uses by miscreants to attack you.

"*90% of targeted attacks continue to reach victims through email*"

Here is a list of safety tips you need to adopt

1. Never click on a link or open an attachment or do something if someone has asked you to do it.

    - If you receive an attachment from someone you don't know, don't open it. Delete email.
    - If you receive an email asking you to verify your credentials (for example your online bank internet access has been disabled and it requires you to authenticate for verification), do not click on link. Delete email.
    - If you receive an email asking for your personal details, ignore & delete email.
    - If you receive an email where it instructs you to visit a website, ignore it and delete email.

Note: if you think it is a legitimate email, then verify with the sender by calling them first.

2. Learn how to recognise and ignore phishing emails.

    - Ignore messages that threaten you
    - Ignore messages that suggest urgency
    - Ignore messages that suggest amazing news discoveries (for example, Michael Jackson seen alive)
    - Ignore messages with poor or bad grammar
    - Ignore messages using forged email addresses (for example, an email coming from you, using your email address)
    - Don't click on "unsubscribe" link is a spam email. This would let the spammer know that your address is legitimate, which could result in your receiving more spam and potential malicious emails.

3. Some good practices

    - Don't share passwords via email.
    - Don't share personal details about in an email.
    - Don't share your email address to sites that you don't trust.
    - Hover your mouse over the link before you click on it to see if the URL looks legitimate.
    - Instead of clicking on the link that is provided by the email, open a new browser and manually type in the address.

12.6.4: Remove Admin Rights from Desktops

When users have local admin rights, they have the power to do almost anything they want to their workstations. They can download any application, use any program, and even ignore or undo anything IT administrators do to their devices. Many users, especially the power users don't want to feel handcuffed or slighted because they don't have complete control, so organisation management let users be the masters of their own devices.

So why restrict local administrator rights?

Local admin rights give the user too much power. Endpoints are where many of the greatest risks to organisation security lie, and giving users control over those endpoints only opens networks to more risk.

Malware is around every corner. Regular Web browsing and email phishing put Windows workstations at constant risk. If users have local admin rights, the risk is even greater because malware can veto IT security measures.

The solution is to make admin rights a software-based approach – not a user-based one.

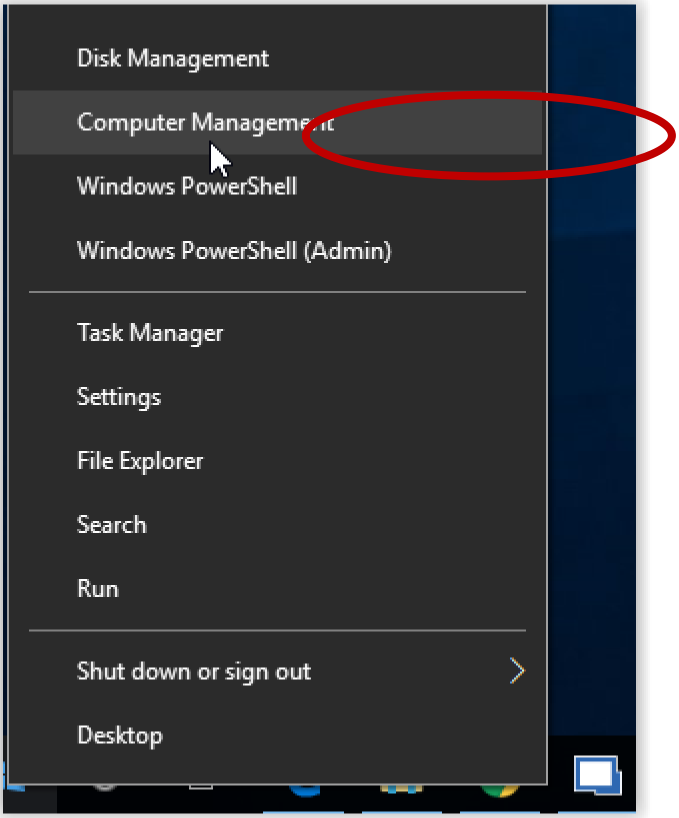
By adopting this approach ensures that if an attacker managed to gain access to a user’s credentials through malware or otherwise, they would be limited in the damage they could cause. Once an admin account is breached, the attacker has the keys to the kingdom and can freely gain access to the core network, configurations, documents and data.

What You Need To Do?

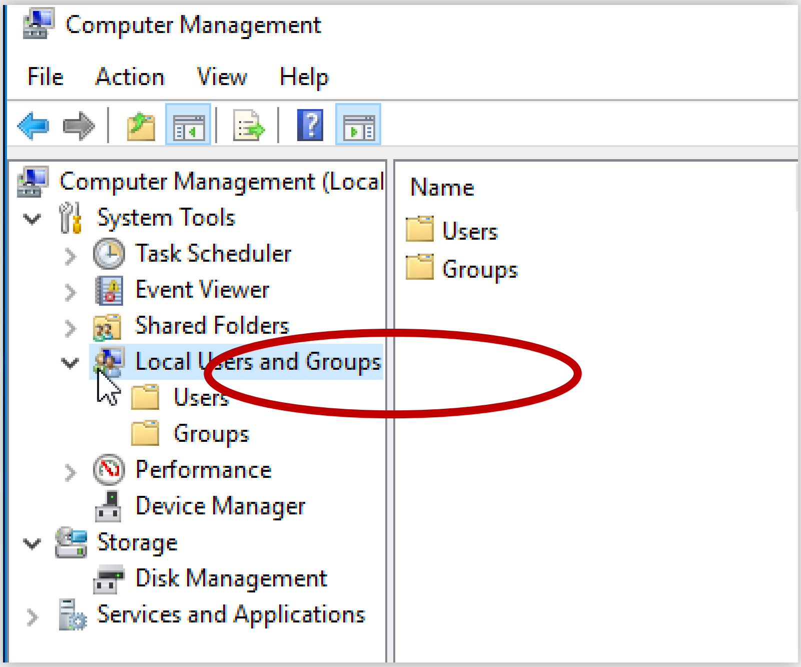
Instead of removing admin rights, the easiest and safest way is to create a new user. By default this new users will not have any Admin rights. So, the next time you log onto your machine, just use this new user to access your machine.

How Do You Create A New User?

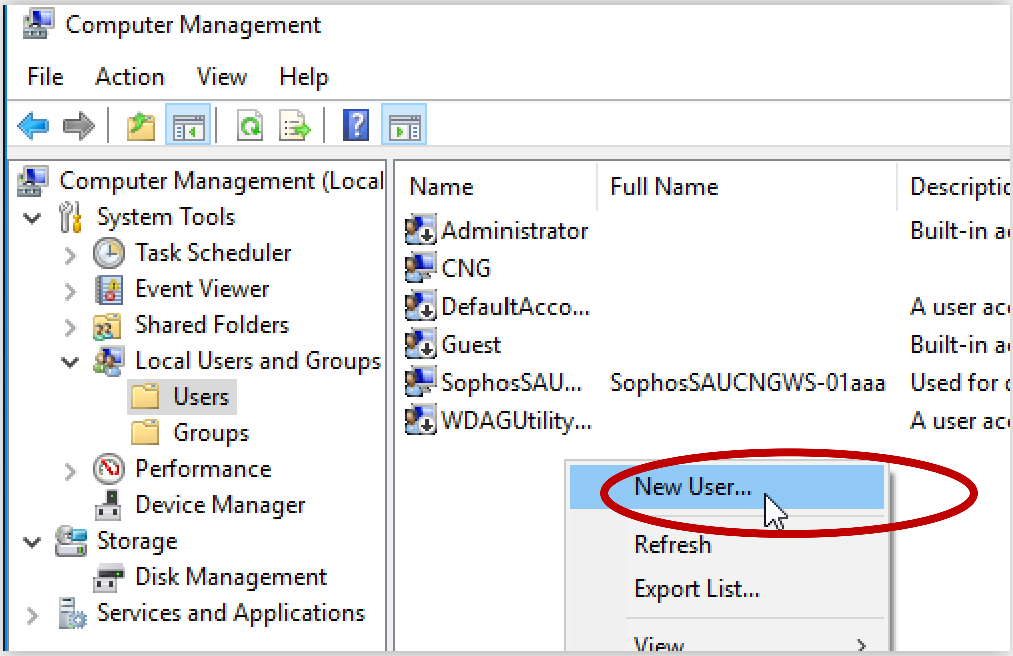
Right Click Start and Choose “Computer Management”:



Open “Local Users and Groups”:

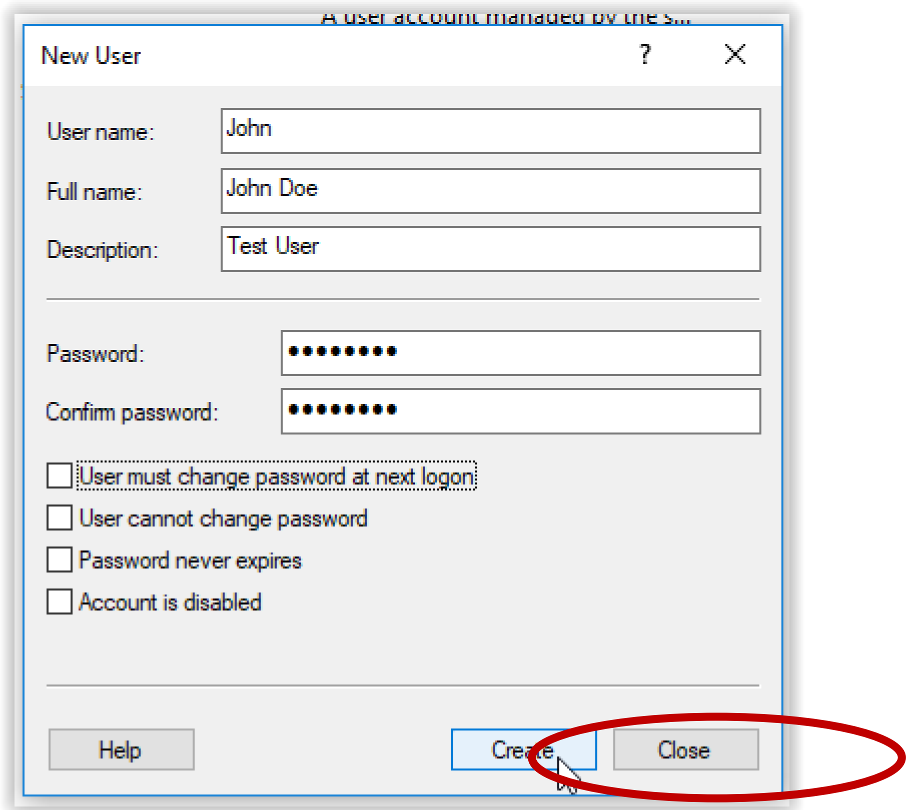


Choose “Users”, right click in the spot without text and choose “New User…”:



Name	Full Name	Descriptic
Administrator		Built-in a
CNG		
DefaultAcco...		A user ac
Guest		Built-in a
SophosSAU...	SophosSAUCNGWS-01aaa	Used for
WDAGUtility...		A user ac

Type the name of the New User and all necessary details. Check next to “User must change password at next logon” and click “Create”:



New User

User name: John

Full name: John Doe

Description: Test User

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

□ User must change password at next logon

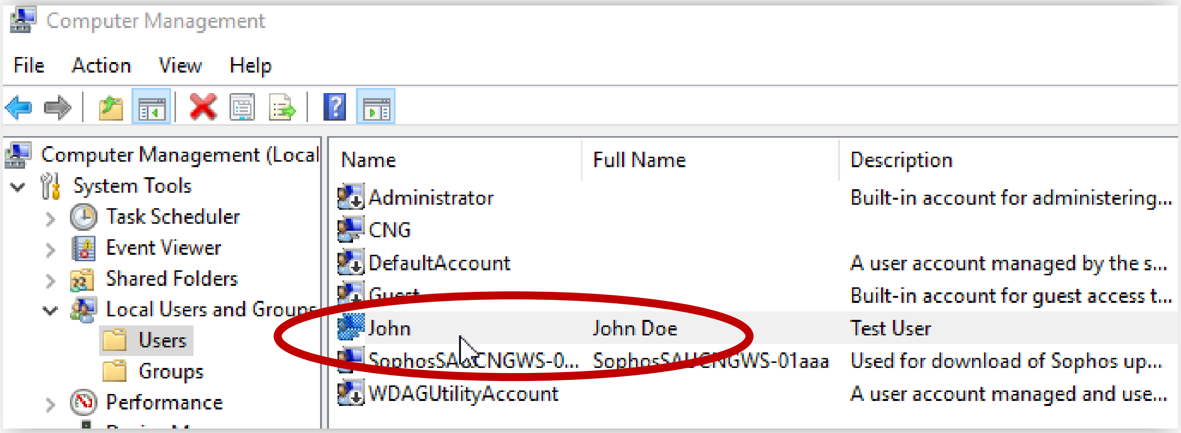
□ User cannot change password

□ Password never expires

□ Account is disabled

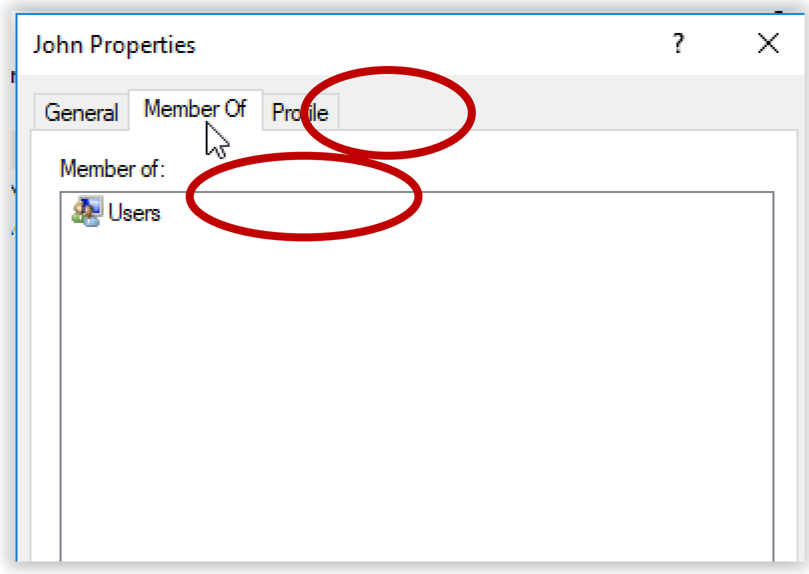
Click on “Close”

This will create a new user John Doe with login name: John



Name	Full Name	Description
Administrator		Built-in account for administering...
CNG		
DefaultAccount		A user account managed by the s...
Guest		Built-in account for guest access t...
John	John Doe	Test User
SophosSAUCNGWS-0...	SophosSAUCNGWS-01aaa	Used for download of Sophos up...
WDAGUtilityAccount		A user account managed and use...

By default John will have limited permissions on the computer hence minimizing the risk. This can be checked by double clicking on John and choosing the “Member Of” tab:



As you can see in the screenshot above, John is only a member of the Users group and not the administrators.

Close Computer management again and log off. Use the newly created user for all daily tasks.

12.7: Overview – Landscape Threat

When we describe the environment of a cyber-attack, we need to define some key definitions.

- A Threat is a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.
- An Incident is an adverse event on an information system or network, or the threat of the occurrence of such an event.
- A Data Breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorised to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property."
- Zero-Day Attack refers to a vulnerability in software that is unknown to the vendor. This security vulnerability is then exploited by hackers before the vendor becomes aware and hurries to fix it. This exploit is called a "zero day attack".
- Malware is short for "malicious software". They are software programs designed to infiltrate and damage computers without the users consent.
- Security Vulnerability is a weakness in a product (due to human errors) that could allow an attacker to compromise the integrity, availability, or confidentiality of that product. For example, an unintended flaw in software code.
- Targeted Attack can be considered a targeted attack when it fulfils three main criteria:
    1. The attackers have a specific target in mind within an organisation
    2. The target could be any asset.
    3. The attack is persistent, with the attackers expending considerable effort to ensure that they have managed to compromise the target.

12.8: Overview – Email Phishing

Email favoured attack channel.

Malicious emails are the weapon of choice for a wide range of cyber-attacks, used by everyone from state sponsored cyber espionage groups to mass-mailing ransomware gangs. Today, one in 131 emails sent are malicious (Symantec Internet Security Threat Report April 2017), the highest rate in five years.

Email is a proven attack channel. It doesn't rely on vulnerabilities, but instead uses simple deception to lure victims into opening attachments, following links, or disclosing their credentials.

For example: *Malicious emails disguised as routine correspondence, such as invoices or delivery notifications, were meanwhile the favoured means of spreading ransomware. The availability of spam botnets-for-hire, allows ransomware groups to mount massive email campaigns, pumping out hundreds of thousands of malicious emails daily.*

12.9: Overview – Ransomware

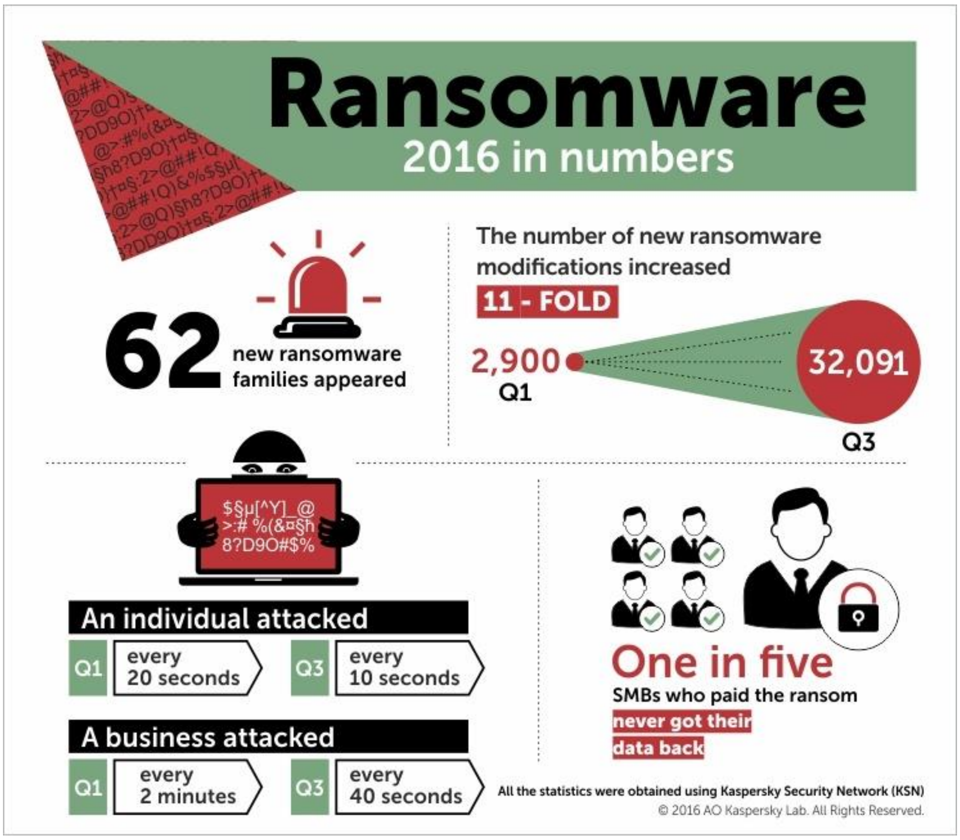
Ransomware is a malware threat that seems to be showing up more in the news because of recent high profile attacks, and is attracting an increasing number of malware authors because of its lucrative and highly rewarding results.

The modus operandi of ransomware is deceptively simple: Infect a device, and then deny the person access to their devices or files unless they pay a ransom.

For example: *In 2012, Russian hackers held Gold Coast Medical Centre to ransom, demanding $4,000 to decrypt their sensitive information held at their Miami Family Medical centre*.

How bad is it? Microsoft has identified a 400% increase in the number of ransomware encounters from December 2015 to December 2016.

Early 2017, Kaspersky one the leading end point security vendors developed a Ransomware infographics image of “Ransomware 2016 in numbers. It is well worth the read.


Ransomware
2016 in numbers
62 new ransomware families appeared
The number of new ransomware modifications increased
11 - FOLD
Q1
Q3
$§µ[^Y]_@
>:# %(&¤§h
8?D9O#$%
An individual attacked
Q1 every 20 seconds
Q3 every 10 seconds
A business attacked
Q1 every 2 minutes
Q3 every 40 seconds
One in five
SMBs who paid the ransom
never got their data back
All the statistics were obtained using Kaspersky Security Network (KSN)
© 2016 AO Kaspersky Lab. All Rights Reserved.