SECURITY TWEAKS AND WHAT ARE THE REAL RISKS TO YOUR PC AND DATA?

How to ensure your PC is properly protected from todays risks.

Welcome

- Who am I?
  - Jonathan A Burt BSc Cert Mgmt HND FIAP IEng MBCS CITP
    - Batchelor of Science Degree (Open)
    - Professional Certificate in Management
    - Higher National Diploma in Computing
    - Fellow of the Institute of Analysts and Programmers
    - Incorporated Engineer with the Engineering Council
    - Member of the British Computer Society
    - Charted IT Professional
    - PRINCE2 Practitioner
    - Certified Novell Administrator (v5.x)
  - 25+ years experience of working in IT, now retired.
  - Long time member of the Isle of Wight PC User Group!


Warning!

- As with all my talks, I recommend that you do you own research before making any changes to your PC.

- Also, please ensure you have backed up all of your data before you make changes to your PC.

God Mode!

- In Windows 10, settings and controls are divided between the new Settings menu and the traditional Control Panel. Some settings, including touchscreen-specific settings and Windows Update, are found only in the Settings menu, while others, such as the Device Manager, are still mostly accessed through the Control Panel.

- If you're sick of switching between the Settings menu and the Control Panel, searching for your lost settings, there is a way to access all settings and controls in one place.

God Mode!

- To enable GodMode, right-click on the desktop and click New > Folder.

- Then paste the following as the folder name:

  GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}

- That's it!

Backup

- The most important thing you can do to protect yourself is to ensure you have backup's of your data.

- This can be done many ways, for example:
  - Burning data to CDs/DVDs
  - Copying data to external USB devices
  - Using secure cloud storage to backup your files

Software	Available From
CDBurnerXP	https://cdburnerxp.se/en/home
CrashPlan	https://www.crashplan.com
Fbackup	http://www.fbackup.com/

Physical: Drivers

- One way in which your data can be corrupted and/or lost is due to hardware failure. In most events, there is not much you can do to protect yourself from this.

- However, sometimes hardware failures occur because of incorrect drivers in Windows, therefore its important you keep your drivers up-to-date.

- Thankfully, this is easier to do nowadays than it used to be, most suppliers now offer software tools to allow you to do this.

Physical: Electricity Failure

- Another event which can cause physical damage and lead to corrupted/lost files is a power failure.
- An easy way to protect yourself against this is by using a Uninterruptable Power Supply (UPS).
- A UPS protects you from both power fluctuations (i.e. it cleans the power for you) and power failure.

Physical: Found devices

- What should I do if I find a USB device, CD, floppy disk in a car park (or any location)?

Pick it up and put it in the bin!

- Why?
  - You have no idea what is on it, and it could well have malicious software on it.
  - The main malicious software used this way is Remote Access Tools (RATs).

Patch, Patch, and Patch some more!

- I can’t stress enough the importance of making sure your Operating System and Software is patched up-to-date.
- Make use of Windows Update, and ensure you have enabled the option to “Give me updates for other Microsoft products when I update Windows.”.
- Some Applications/Games have options to automatically or manually check for updates, and you should use these.

Software Support Life Cycle

- You should be aware of the Support Life Cycle for your operating systems and software. Most major suppliers will have details about this somewhere on their websites!
- Why? This gives you a good guideline as to when the products you are using will stop being supported, i.e. patched by the supplier. It gives you an advance timetable to think about upgrading to new or alternative products.

Software Support Life Cycle - Microsoft

Software	Mainstream Support End Date	Extended Support End Date
Windows XP Professional SP3	14/04/2009	08/04/2014
Windows Vista SP2	10/04/2012	11/04/2017
Windows 7 SP1	13/01/2015	14/01/2020
Windows 8.1	09/01/2018	10/01/2023
Windows 10 (v1703)	13/10/2020	14/10/2025

- Mainstream Support is the first phase of the product lifecycle:
  - Incident support (no-charge incident support, paid incident support, support charged on an hourly basis, support for warranty claims)
  - Security update support
  - The ability to request non-security updates
- The Extended Support phase follows Mainstream Support for business, developer, and desktop operating system products:
  - Paid support
  - Security update support at no additional cost
  - Non-security related updates requires Extended Hotfix Support to be purchased (per-fix fees also apply).
- Self-help Online Support is available throughout a product's lifecycle and for a minimum of 12 months after the product reaches the end of its support.
  - Microsoft online knowledge base articles, FAQs, troubleshooting tools, and other resources, are provided to help customers resolve common issues.

Anti-Virus

- Do I need Anti-Virus software?
  - Yes! You need Anti-Virus software on your computer, no matter how “careful” you are. Being smart isn’t enough to protect you from threats.

- If you are using Windows 10, you will have Windows Defender installed by default, and this is an adequate, but simple, Anti-Virus package. However, all it gives is plain simple Anti-Virus protection, its doesn't have any extra “bells & whistles” like 3rd party software, nor is it necessary the best on the market.

Anti-Malicious Software (Malware)

- Why do I need separate Malicious Software protection software?
  - Anti-Virus software is very good at protecting your computer, however in my experience some Malware can be very hard to track, and even harder to remove.
  - I have had experiences where the Anti-Virus software gives the PC a clean bill-of-health, and yet Malwarebytes still finds Malware hidden deeply on the PC!

Firewall

- Do I need Firewall software?
  - Yes! You need Firewall software on your computer, no matter how “carefully” you use the Internet. A firewall works as a barrier, or a shield, between your computer network and Internet.

- If you are using Windows 10, you will have Windows Firewall installed by default, and this is an adequate Firewall package, but like its Anti-Virus protection, its doesn't have any extra “bells & whistles” like 3rd party software, and does have some limitations.

Internet Security Packages

- Basically, 3rd party software which covers Anti-Virus, Firewall and other security benefits, for example:
  - Phishing and Privacy (Identity) Protection
  - Spam Filtering
  - Parental Control
  - Backup and Tune-Up utilities
  - Multi-platform
  - Password management
  - Encryption
  - Secure file deletion
  - Software Updater/Cleaner
  - Vulnerability Scans
  - VPN
  - Pop-Up/Ad Blocker on browsers
  - Cloud Storage

Virtual Private Network (VPN)

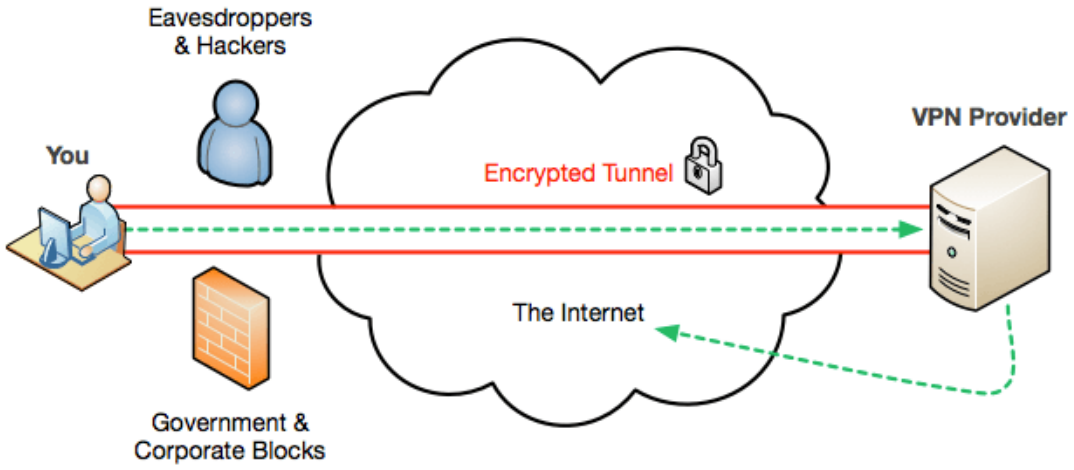
- So how does a VPN protect my PC?
  - What it does is help you in protecting your online identity.

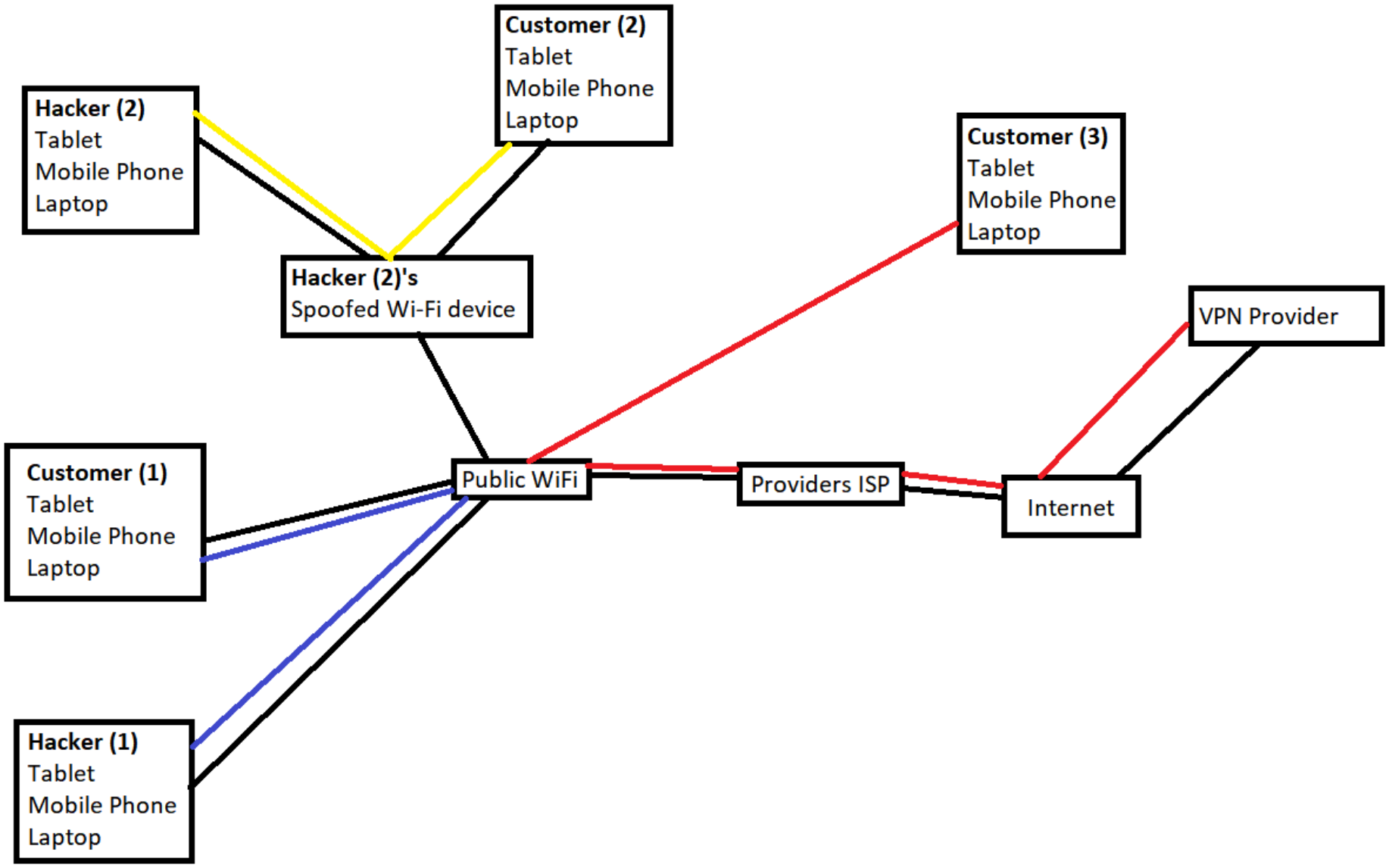
- More and more of the stuff you do online is tracked and recorded, from your IP address, to the websites you visit, the files you download, and if you use torrents!

- However if you use a VPN, all of your internet traffic is encrypted between your PC and the VPN provider, and if the provider keeps no logs, there is no evidence of what you have been doing.

Virtual Private Network (VPN)

- However, another even more important benefit of VPNs is if you use “free public Wi-Fi”, or even a friends Wi-Fi!
  - As you know, when using free public Wi-Fi, the connection between your phone, tablet, laptop and the router is unprotected and open for eavesdropping and back-hacking to your device.
  - But by using a VPN, you ensure that anything you do is hidden and protected.





Created using Jonathan's brilliant artistic skills!!!

3rd Party Tools

- Bellarc Advisor
  - The Belarc Advisor builds a detailed profile of your installed software and hardware, network inventory, any missing Microsoft hotfixes, anti-virus status, security benchmarks, and displays the results in your Web browser.

- Adblock Plus
  - Adblock Plus is a free extension that allows you to - among other things - block annoying ads, disable tracking and block domains known to spread malware. Available for Android, Chrome, Firefox, Internet Explorer, Maxthon, Opera, Safari and Yandex, Adblock Plus uses filters that you choose to block all unwanted elements.

3rd Party Tools

- Flexera Personal Software Inspector
  - Personal Software Inspector is a free computer security solution that identifies vulnerabilities in applications on your private PC. Vulnerable programs can leave your PC open to attacks, against which your antivirus solution may not be effective. Simply put, it scans software on your system and identifies programs in need of security updates to safeguard your PC against cybercriminals. It then supplies your computer with the necessary software security updates to keep it safe.

- There are many more, just search on the internet for “tools to scan for vulnerabilities”, but research them before you install them! ☺

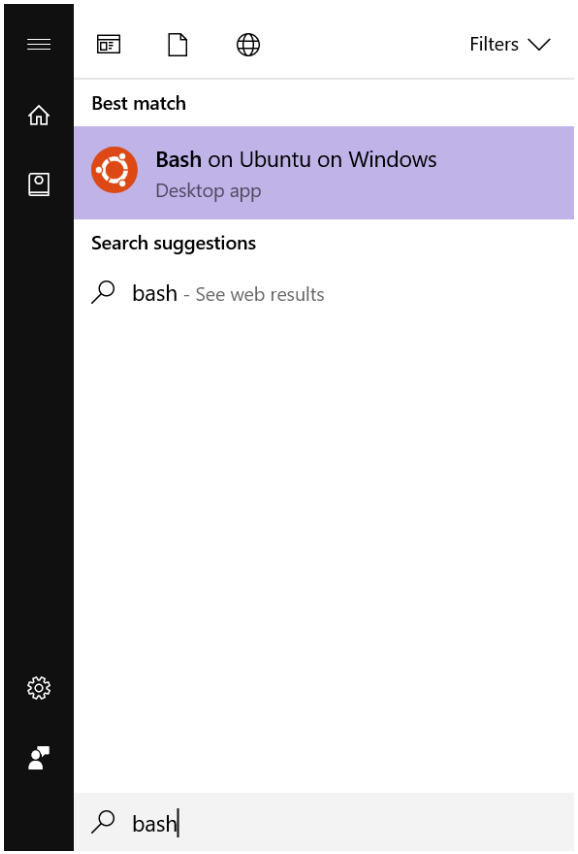
Checking your downloads!

https://virustotal.com/

- VirusTotal, a subsidiary of Google, is a free online service that analyses files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. At the same time, it may be used as a means to detect false positives, i.e. innocuous resources detected as malicious by one or more scanners.

Updating the Windows Subsystem for Linux

- If you have installed the "*Windows subsystem for Linux*" on your Windows 10 PC, which allows you to run Bash and other Linux apps on Windows 10, then you need to ensure it is kept up to date.
- Once Bash has started up, you need to update the local package repositories: **sudo apt-get update**
- Once this has completed it is time to install the updated packages: **sudo apt-get upgrade**



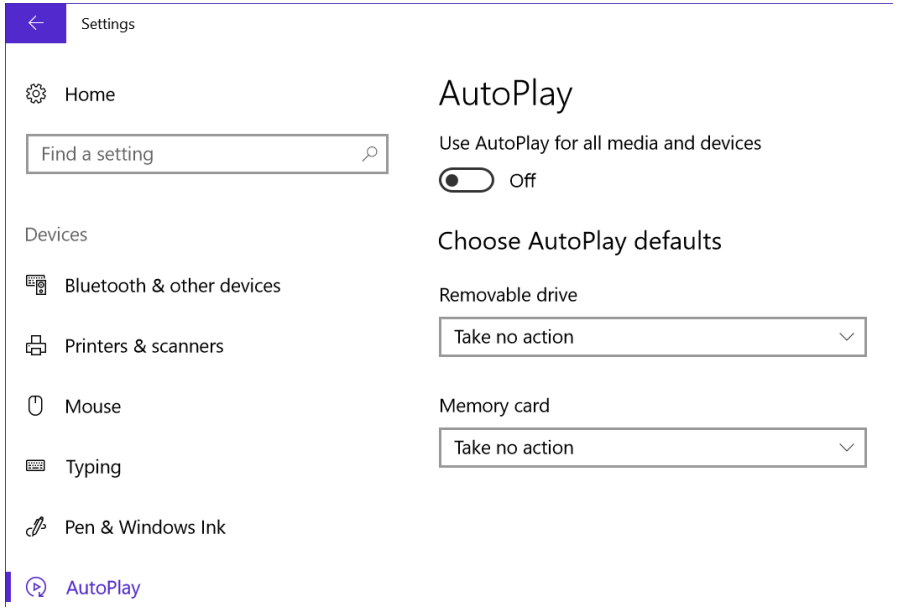
Tweaks

- Are there any additional tweaks which I can do to secure my computers and data?
  - Yes ☺

- There are quite a few different tweaks which you can do to protect your computer and data, it all depends on what level of protection you want.
  - For example, you could do none of additional tweaks, and still be confident that your PC is protected if you implement the software/changes previously mentioned.
  - Or you could go to the extreme, and “harden” your Windows installation, with severe levels of tweaking and changes!

Tweaks: AutoRun/AutoPlay

- AutoRun and the companion feature AutoPlay are components of the Microsoft Windows operating system that dictate what actions the system takes when a drive is mounted.
- AutoRun was introduced in Windows 95 to ease application installation for non-technical users and reduce the cost of software support calls.
- I recommend that this is disabled.

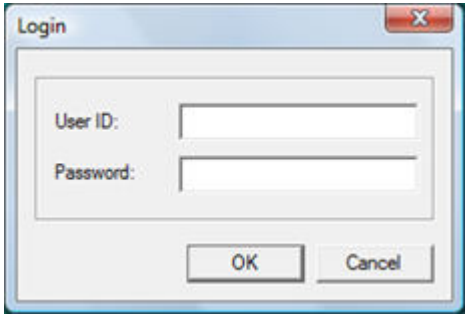


Tweaks: Universal Plug and Play (UPnP)

- Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment. UPnP is intended primarily for residential networks without enterprise-class devices.
- I recommend that this is disabled.

Tweaks: Modem/Router

- Most modem/routers use a simple default username/password, often admin/admin or even admin/password.
- The problem is that someone could try to connect to your router via the internet using the default username/password, and then once connected to the router would have access to your network.
- I recommend that these are changed from the default.
  - Note, unfortunately not all modem/routers all you to change the username and only the password.



Tweaks: Wi-Fi Sense

- Wi-Fi Sense is a feature in Windows 10 that allows you to connect to your friends shared Wi-Fi connections. That is, you and your friends may opt to share your or their Wi-Fi connections. Friends, according to Microsoft, are people on your Facebook friend list, your Outlook contacts and Skype contacts. By default, all these 3 are pre-checked.
- These ‘friends’ can connect to your Wi-Fi without having to know your password. This means three things:
  - The Friends should be in the range of the Wi-Fi being shared.
  - The password is sent encrypted to the other computers, but could be potentially hacked.
  - The password is also stored in a Microsoft’s database (“in encrypted format so that no one can hack it”, says Microsoft).
- I recommend that this is disabled.

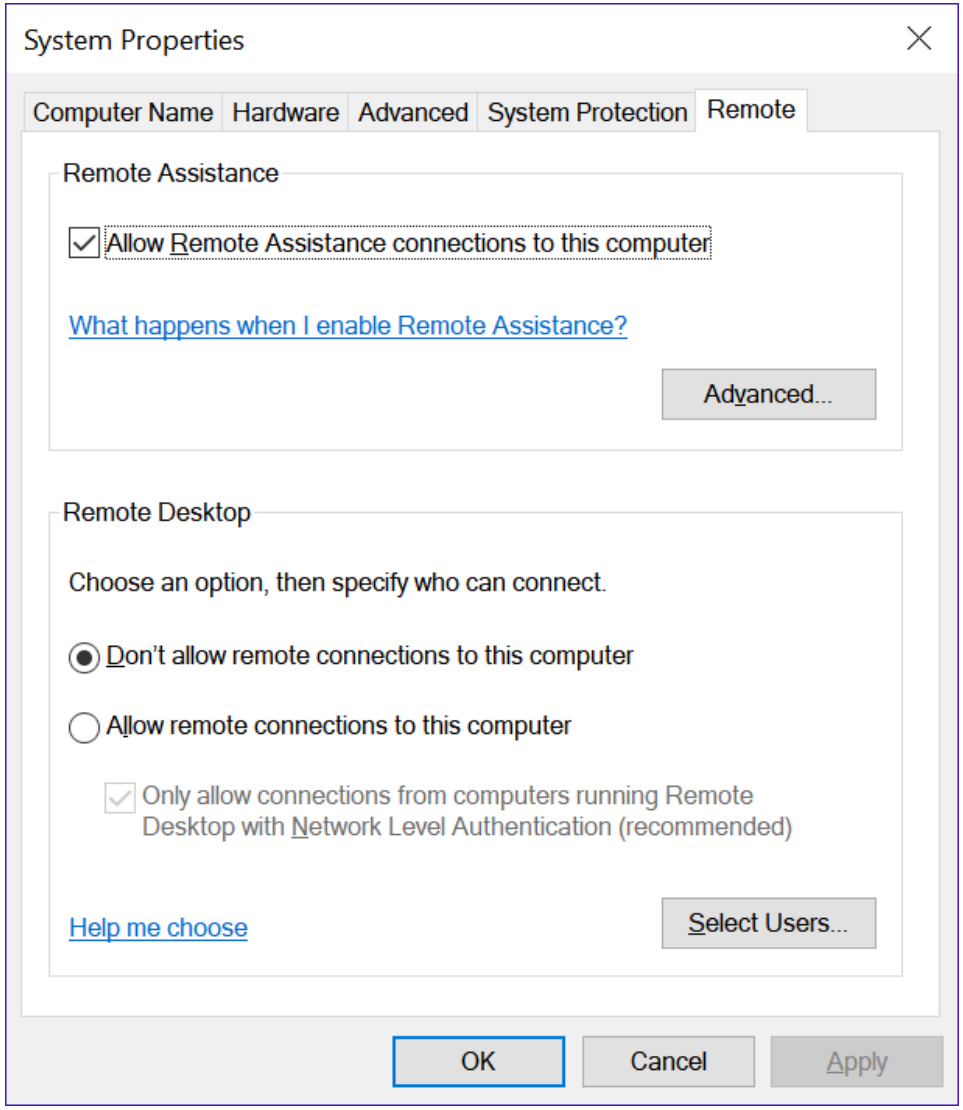
Tweaks: BIOS

- Another tweak, which protects your PC/Laptop is setting a password within the BIOS.

- You can set a BIOS password for logging into the BIOS as well as for accessing the PC/Laptop (not all BIOS support this).

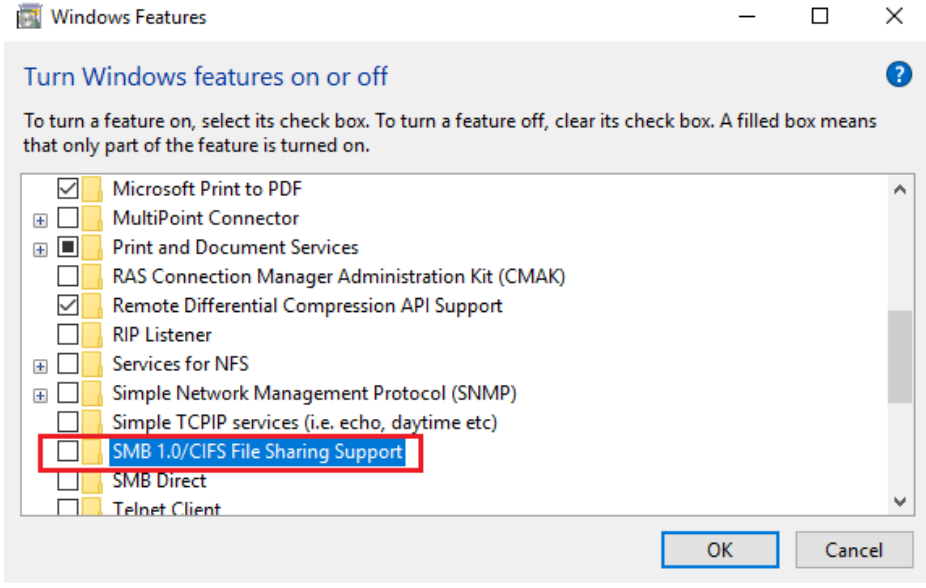
Tweaks: Disable RDP

- The Remote Desktop Protocol in Windows provides a graphical interface to the user, when he connects his or her computer to another computer over a network connection, using the Remote Desktop Connection client software.
- I recommend this is disabled.



Tweaks: Disabling SMB1

- The Wannacrypt and NotPetya ransomware targets the vulnerabilities of the SMB service of the Windows operating system to propagate.
- Open Control Panel > Programs & Features > Turn Windows features on or off.
- In the list of options, one option is *SMB 1.0/CIFS File Sharing Support*. Uncheck the checkbox associated with it and press OK, then reboot your PC.



Tweaks: Harden Windows 10

http://hardenwindows10forsecurity.com/

- This website has a very large guide on how to “harden” your installation of Windows 10.
- Basically, this long and at times complex guide will take you through many different settings, tweaks, and add-ons to lock-down and secure your Windows 10 PC.
- Its well worth a look at, but I would avoid implementing this fully if you don’t have a high-level technical knowledge.

Further Information

- Wikipedia
  - https://en.wikipedia.org/
- Lots of useful tutorials
  - http://www.howtogeek.com/
- TechRadar has a good selection of reviews.
  - http://www.techradar.com/

Questions?

Does anyone have any questions?