Passwords:

It is safer to use longer passwords, than more complex passwords, because with a piece of software it can guess hundreds of million password combinations per second and the shorter the password, the less time it takes to get each individual character. Using the same password for more than one account can be very dangerous because if a key logger is secretly running in the background, and you have the same password for everything the “hacker” can steal lots of sensitive data, and even bank details. It is also a bad idea to use any personal information for your passwords, like your name followed by your birthday, so for example “Callum1207” would be a bad password, to get around this use common words to make a sentence, remember space bar is your friend, “I am going for lunch at 12 O’clock with Bat Man!” or if that is too much just use the first letters, “Iagfla12O’cwBM!” This scores 99% in my password security test. But please do not use that password because it has probably just been sold to the password black market…

Threats:

Phishing:

Phishing is when a scammer pretends to be a reputable company or person to get valuable or personal information, such as login credentials or bank information, credit card numbers, etc. Phishing emails often contain code in the email or a document attached to the email, which when run, will open software secretly that can track activity and log key presses, meaning they can easily get your passwords.

Scams:

Scams come in many forms, often scams are hilariously stupid to you or me, but this is for a reason. By making them completely absurd, only the most gullible people fall for them, very clever. Sadly, these people are often the elderly who are completely defenceless against these attacks, leaving them out of pocket most times. An example of a scam is someone saying they have millions of pounds to transfer out of their country. They way these work is they ask you to open a “special account” and pay an account fee to open it of around £2000, and then never send you anything.

Unsafe Links:

These links are again often in emails, and when clicked on can do the same as phishing emails. The will send you to a webpage, that probably says an error message like “ERROR 404: Page Not Found” that secretly runs some code and can again activate a key logger and monitor your activity. Sometimes with unsafe links they will send you to a site that will not harm your computer, but will contain highly inappropriate images and adverts.

HTTPS:

Hyper Text Transfer Protocol Secure (or HTTPS), is what appears at the start of a web address, and means that all the data you send to the website you are on is encrypted at both ends, meaning that nobody can see what you send to the website. Sometimes though it is only HTTP, without the security. In this instance your web browser should warn you the site is unsafe, and this means the data you send to the site is not encrypted, meaning someone with the right tools can see what you typing and sending to the site. If you are purchasing goods online, always look for the HTTPS symbol. The number one rule for websites is, if you don’t trust the site, don’t use it.

2 Factor Authentication:

2FA is a service offered by most services which you must log onto, Google, Amazon, etc. 2FA is a service that offers a very secure way of logging in. 2FA means you need something as well as your password to log in, so if your password is compromised then your account is still partially safe, although you should still reset your password. The way 2FA works is it requires you to have another piece of information to log into your account, this could be in the form of a text, a backup code, or an authenticator app, provided by the service. To log in you first enter your password, then you need to enter the piece of information provided by the service, the text or code, etc. This is very simple to activate and makes it a million (not scientifically correct) times harder for someone to get into your account.

Viruses:

Malware:

Malware is often installed from dodgy websites, and this malware can do several things, like cause unexpected shutdowns, run programs in the background to slow you PC, I even fixed a PC where a virus had disabled the mouse! Viruses are generally, whilst annoying, safe. I recommend a program called Malwarebytes Anti-Malware, and a background anti-virus like Avast.

Ransomware:

Ransomware on the other hand is very dangerous. What a ransomware does is encrypt everything on your hard drive with a key only the person who gave you the ransomware has. To get the key and decrypt your files they often charge a fee. This fee is often asked to be payed by bitcoin, a system they can use without being caught. The best way to protect from ransomware, apart from not downloading suspicious thing online, is to make backups of everything. Every one of my files is backed up to server that is always online, an offline hard drive, in case the network is attacked, and numerous USB drives stored both on site and off site, in case of a fire or damage to the property, over the top? Maybe but my data as well as other family members can be crucial, especially for a business run from home, so I take no chances with data. As well as all this we have filters on our router to stop suspicious “packages” from entering, a firewall on the network and on every device, on top of that is full disk encryption on all phones and PC’s, in fact I go as far I go as far as having a spare bootable hard drive just in case, the one in any PC dies. This maybe a bit over kill, but at least one back up, will save you a lot of hassle if anything bad was to happen.