A Small Business Guide to Cyber Security

There is a lot of ambiguity and “buzzwords” used currently regarding business IT Security and combined with compliance and guidelines issued by the government these can be a headache for small business so we have done this handy guide to IT Security.

Business IT Security is based on a layered defence to protect against both Cyber Attacks and physical threats which could result in data loss.

Firewall (Hardware)

Most routers have a basic firewall to protect against malicious attacks from the internet which are suitable for home use, however for business use we would always recommend a good brand firewall. These have the advantage of much more frequent updates and a considerably higher level of protection from internet threats, they have active monitoring and some of them can even report on what your staff are doing. A good firewall can protect against viruses, malicious web sites, intrusion attempts (Hacking) and more.

Firewall (Software)

A software firewall is one that is resident on your PC, Mac or laptop and has essentially the same function as the above. You may ask why you need 2. The answer is simple, if it is a laptop / Macbook you have protection when out and about, if it is a desktop then this provides additional protection for anyone clever enough to get through your hardware firewall and also protects in case someone connects another system into your work network directly.

Antivirus

Antivirus helps identify, isolate and destroy virus software on your system, a good antivirus system will update regularly and notify you not only of virus threats but also out of date Windows updates and will generally have anti malware and anti-spam included. Viruses are generally software which will self-replicate and spread. If you use Office 365 or other online email systems and file storage it is worthwhile investing in a cloud based antivirus to protect the data where it is held.

Anti-Malware

Malware is software with malicious intent and covers viruses as well, the difference is these are designed to sit on just the one system and do not self-replicate. A good antivirus software will protect you against these as well as more traditional viruses.

Anti-spam

Spam as you probably know is unsolicited emails designed to either target a lot of people or individuals and they generally have funky names (Phishing, Spear fishing) and are designed to trick you into clicking links to take you to false web sites or to make you send money by pretending to be someone from within your organisation. A good antivirus with a spam filter will help reduce this the spam you receive. If you utilise Office 365 you can add an extra layer of defence with a good cloud based spam system as part of your cloud antivirus package.

You can also reduce spam being sent as your business by having correct SPF records (Sender Protection Framework) with your web domain host that correctly identify where your emails are being sent from.

Encryption

Disk Encryption is a form of software that encodes your data so that anyone stealing your systems physically, or systems that are lost accidentally cannot be accessed without an additional password. If you have full disk encryption (FDE) this also means that any lost system is not counted as a breach under GDPR guidelines and does not have to be reported.

Email Encryption is a similar system that encrypts your emails which you may not need unless you are in the medical, dental, defence or other sector that deals with very sensitive and requires recipients to have a “key” or password to access emails.

2 Factor Authentication (2FA) / Multi Factor Authentication (MFA)

This is a system based on users having some information they know (A password) and something they have such as a key card, mobile phone with an authenticator app on it. It is relatively easy to crack a simple password and relatively easy to steal a phone, but it is considerably harder to do both. Office 365 comes with a free 2FA system which works with mobiles and these systems are becoming much more widely used in banking and other applications and help seriously reduce people gaining access to your system.

User Accounts

User accounts come in 2 general flavours – user and administrator. User accounts are restricted in what they can do however administrator accounts have full access to system. It is strongly recommended that staff do not use administrator accounts for day to day use as they allow viruses and malware to infiltrate a lot easier and a lot further than a standard user account.

Policies

Policies cover 2 separate parts of your IT security.

Password policies which are set on the PC ensure users have more complex passwords which are changed regularly. These can be controlled by a server or by Microsoft Azure (a free part of Office 365) or by a company policy.

Company Policies are written documentation to instruct employee's / users how to operate their systems and are designed to give general guidance on IT use but also to restrict users on any parts of the IT systems that cannot be governed or controlled in other manners. An example of this would be a Security Operations policy which would stipulate an employee with administrative level access would be subject to disciplinary policy if it was misused.

Physical Security

Physical security can be a simple as a Kensington style lock to secure a screen / laptop or PC to a full clamping system to hold a system to the floor to prevent / delay theft. This is generally not required in secure offices but is essential in a retail environment or for systems that are easily viewable by the public. Physical security can be augmented with IP based camera systems to detect intrusions and professional camera systems are good enough for facial identification by law enforcement.

Training

Training is probably the most overlooked part of any cyber security. Staff training on the importance of all of the above and also on how to identify suspicious emails, dodgy web sites and how to get these checked is absolutely essential. Staff training can easily and quickly identify threats and help negate them. Staff training on general IT systems as well and the importance of Windows Updates and maintaining antivirus systems will make it considerably harder for anyone external to the business to gain access to your systems and will help prevent a lot of business downtime.