Safeguard your business by knowing the right IT security information

Cyber crime is a growing problem for businesses. Cyber attacks have doubled compared to the same period last year. This is only due to increase because of the accessibility of technology, information regarding it and because of the connectivity of our world.

Statistics suggest that for a data breach at a large company it will cost £20,000 to put the issues right. What this figure doesn't consider is the damage to your company reputation, the investment to stop it from happening again, and the marketing involved. Having to explain to clients that you can in fact trust your company, and reassuring new customers that they have nothing to fear. Issues with cyber-attacks are publicised and may have to be publicised, no matter the scale.

Cyber crime is more common and becomes larger scale as technology becomes more widely used to improve our world. Hackers have a lot to gain from successful breaches. Whether this be for data, for the thrill or to destroy a company just because they can. What doesn't help is that hacking tools are widely available on the internet if you know where to look. It gives even the lower skilled individuals chance to attack and win. Smart connectivity is a great tool and truly helps with modern age requirements and business efficiencies. But un protected and un managed this could be a direct gateway into your business. Another factor is GDPR. The stakes are higher for companies, those who are not investing in the right protection are potentially harming themselves and their customers. Those who are, are a challenge and therefore exciting to target.

Unit 8 - 9 Temple Bar Business Park, Strettington, Chichester, West Sussex, PO18 0TU
01243 773113
www.abm.uk.net
info@abm.uk.net

Terminology:

Phishing: Disguised as a trusted email sender they try to gain sensitive information. For example, disguised as a message from amazon, they will ask you to follow the link in their email, enter your username and password on to a fake site and therefore have your information available to them. These emails can be very convincing. It is good to check the email address to ensure it doesn't have any funny characters, or for example 'amazon.124-5sender', does the email look like another you know to be correct, does the footer have any weird misspelled words or location listings? How can this be stopped? Unfortunately, this is very difficult to stop. However, with high security setting within your email and blocking those pesky emails that slip through, is a good start. Just be mindful about giving your email address out and signing up to things with it. Established businesses should have a privacy policy or GDPR notice, ensure they are not sharing your data.

Identity Theft: Using data they have collected via phishing; these people can access your life. Using your personal data, they can potentially obtain loans, credit cards and even make purchases using your details. For instance, if you clicked through on the 'Amazon' email, entered your details they could get into your account. If you have a card stored here, then they would be able to buy from Amazon at your expense.

Open Network: Essentially a public Wi-Fi. Generally, a free service lots of businesses offer to their clients, without using password access and allows everyone to use it freely. Lots of companies now have password protection. However, you use it once, whilst sitting to have a coffee, and then it is saved within your device to remember for next time. Hackers love using these networks. People who think they are safe because of the password protection, and access for instance, their bank account could be

under the risk of identity theft and malware attacks for their information.

Hacking: Gaining unauthorised access to one or more devices. This happens most often through unsecured public Wi-Fi, or as before, by clicking a link in an email. The hacker will guide you to downloading their malware, and then use it to control your systems. Depending on the virus, it will complete different actions and aim for different goals.

Malware: Gains unauthorised access to your machine through downloading a malicious software on to your device. Malware is the general term for a virus and there are many different types.

Ransomware: Blocks the user from gaining access to their personal files. Essentially encrypting (meaning to prevent access through changing the data into a code) your files. Locking them away from you. The only way to then get those files back is to pay a ransom. Even then it is not certain that they will unlock those files. You may have lost them forever. This is partly why we encourage a backup of all your files, saved in a separate location, not linked to your main set up.

Spyware: Do you remember the nanny cam and computer cam hackings? This was an example of literal Spyware. However, it basically spies on what you are doing and relays your data to the hacker.

Worm: One of the worst malware in terms of the amount of damage it can do to a large number of people at once. Once implanted in your machine, a worm replicates itself and then uses the network to spread to other devices.

Keylogger: Once secretly installed, it runs in the background, recording all of the keystrokes you make. Recording and sending this data straight to the hacker to use your credentials.

Unit 8 - 9 Temple Bar Business Park, Strettington, Chichester, West Sussex, PO18 0TU
01243 773113
www.abm.uk.net
info@abm.uk.net

Trojan Horse: Much like the original tale, the Trojan Horse disguises itself as a safe program that's users want. Once installed however, it reveals its true self and causes havoc.

Adware: As in its title, it is installed to cause pop up ads on your screen. Because they are at random and pop up around your screen, it is hard to avoid clicking on them further, and becomes tedious to try and close them all.

What can you do? It seems bleak, but truthfully if you well manage your IT security (or outsource to people who can), invest where required and educate all members of your business, on the importance of following security regulation, you won't have many issues that can't be thwarted. Due to high security software or settings, lots of attacks you wont even know about. There are also many cost-effective simple options for a business environment that can give you peace of mind, without breaking your budget.

Surely the cost of investing is better than losing your reputation as a safe company to do business with, having to rebuild your systems, clean them completely and then protect them to ensure nothing happens again. You then have to consider those customers who leave you because of this. The cost in insurance because you have lost data, or even worse, lost your client's data. Its an endless spiral that can be prevented for a little more budget in your system security.

To find out more please visit our blog page (www.abm-computer-solutions.co.uk/it-security). We regularly post about the latest scams, malware, security tips and products that we use to help with business security. If you want ABM to complete a system survey and recommend some security changes you could implement to safeguard your business, then please call us on

01243 773113

Or email: info@abm.uk.net

Unit 8 - 9 Temple Bar Business Park, Strettington, Chichester, West Sussex, PO18 0TU
01243 773113
www.abm.uk.net
info@abm.uk.net