IT WORKS
Technology Solutions

A Practical Guide to IT security

IT Works Practical Guide to IT Security for Small Business

Small businesses are increasingly coming under attack from cybercriminals. According to Internet security experts Symantec, the number of SMEs suffering damage from cyber-attacks doubled in the year to June 2012. These attacks come through a number of routes including via email, network attacks, SQL injections (malicious code entering databases via website forms) and increasingly through social media interaction. Why are SMEs suffering? The primary reason is that they are less likely to take adequate precautions for IT security in general and cyber-crime in particular.

Online Attack

Online criminal activity takes a wide variety of forms including most commonly:

- Phishing - where an attempt is made to gain access to information such as user names and passwords by electronic communications purporting to be from a valid source such as a bank or social media site. The victim is tricked into disclosing information which can then result in theft. These are increasingly being targeted at businesses.

- Trojans - A Trojan is a piece of code that can provide a hacker with access to your computer which can then be used to steal information or do harm to your system. These may arrive in emails or be downloaded from websites or games.

- Scareware or Ransomware - These may be encountered while online and often take the form of a bogus warning via a pop-up warning the user that they have a virus or infection or have performed an illegal act online. The user will then be directed to purchase an often useless piece of software which will resolve the bogus issue.

- Viruses and works - These are self-replicating programs that can spread from one computer to another infecting existing programs. Worms are similarly self-replicating but are stand- alone programs. While some are relatively harmless others can cause system damage and severe disruption.

- BotNet infections - BotNets or Robot Networks consist of computers that have been infected often via worms or viruses with software that allows criminals to control a large network of computers to perform illegal activities such as email spamming. Often the computer owner is completely unaware that their systems are being used for illegal activities.

There is More to IT security than just cyber attacks

Of course it`s not just digital vulnerabilities that are exploited by criminals. Theft or malicious damage of computer equipment may also occur. And it`s not just criminals who create issues. Your own staff through carelessness or malicious intent may be responsible for losing, damaging or even stealing equipment and information. There are many examples of laptops or memory sticks containing confidential information being left on trains or in other public places.

Last but by no means least there is the risk posed by simple accidental damage such as fire or flooding which can cause severe disruption to businesses.

Why should I care?

Every business needs to consider seriously the potential consequences of poor IT Security. The impact can be devastating. These are the main issues to consider:

- Reputation damage - Imagine how your customers (and prospective customers) would feel if they knew that their confidential information was lost by you or worse got into the hands of criminals.
- Direct Financial loss - Small businesses are increasingly being targeted by online scammers trying to part you from your hard earned revenue.
- Interruption to normal business activity - How much would it cost you if you had to stop doing business for a day? Or even a week?
- ICO fines - Businesses have a duty to maintain the confidentiality of customer`s personal data. The Information Commissioner`s Office can fine businesses up to £500,000 for breaches.

What can I do?

The short answer is lots of things - the starting point is working out which ones apply to you.

Start with a risk assessment.

A risk assessment is the first step in creating effective IT Security. Ask yourself the following questions:

- What information do you hold?
- How valuable is it?
- How is it stored?
- How is it accessed and who normally has access to it?
- How might others access it?

Answering these questions will help you develop an IT Security plan that minimises the risk of unauthorised access or information theft.

You will need a multi-layered approach.

Unless you have a very simple business without an internet connection to the outside world you will need to take a multi-layered approach as a “single-pack” solution to IT Security simply doesn`t exist. Your risk assessment will help you decide which of the approaches below is right for you.

In the office.

1. Create an IT security policy that sets out how in principle you plan to keep your systems secure - and make sure its implemented and regularly reviewed by senior management.

2. Maintain good physical security - make sure equipment is well protected from theft and other damage.

3. Raise employee awareness - make sure your employees are aware of the seriousness of IT security and also provide them with information and training so they can take an active part in combating cyber-crime.

4. Review your access control procedures - regularly check who has access to systems and information. Make sure this is kept up to date - ex-employees rights removed for example - and that passwords are sufficiently complex (i.e. not Pa55w0rd!) and are changed regularly.

5. Segment and separate information - don`t keep everything in one place and don`t give everyone in your business access to everything unless it`s absolutely necessary for the efficient operation of your business.

6. Make sure you have good firewall protection - to control who has access to your network and stop hackers penetrating your systems.

7. Install good anti-virus software - and make sure you keep it up to date. Regularly check that your virus definitions are up to date also.

8. Have your system tested - penetration testing is a way of identifying if your system is vulnerable to attack from outsiders or even from your own staff. Penetration testing is however a specialist skill and may require outside assistance.

On the move.

More and more business is being done on the move and this will increase further as mobile devices become more powerful and business friendly. This presents a growing IT security risk. However there are a number of sensible precautions that you can take.

1. Ensure staff are aware of the risks - point out the potential consequences should they lose their laptop or phone.

2. Consider encrypting data - on laptops mobile devices and memory sticks in case of loss or theft.

3. Use remote wipe functions on mobiles in the event of theft - many mobile devices have the ability to have their memories wiped remotely to prevent unauthorised access.

Get expert advice - it`s worth it

Hopefully this guide has provided an insight into the issue of IT security. Although there are some simple and straightforward things you can do to minimise risk, it makes sense to get an outside view. At IT works we can provide a full IT Security Audit and Risk Assessment which will help you determine the best course of action to keep your company secure.

IT WORKS

2 George Square
Dunfermline
Fife, KY11 8QF

T: 01383 749 966
E: enquiries@itworks.co.uk