Securing Your Digital Business

Did you know?

90% of businesses that lose data from a disaster are forced to shut in 2 years[1]

33% of small business security breaches are a direct result of hacking attempts[2]

45% of small business security breaches are virus related[3]

£65k The average cost of a small business major security breach[3]

What is a virus?

A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data

Trojan

A trojan is generally a non-self-relicating program containing malicious code that typically causes loss or theft of data and possible system harm

Malware

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to a private computer systems

What is hacking?

A hacker is someone who seeks and exploits weaknesses in a computer system or computer network

XSS hacking

When someone infiltrates your website by tricking it into thinking it's you

SQL injection hacking

When someone exploits vulnerabilities in a database to gain access to the data

Denial-of-service attack

When someone attempts to make your network unavailable to you, including logging in and accessing your files

Defence strategy

Have a disaster recovery plan in place for all parts of your digital business

Plan for:

- Natural disasters
- Reputation crisis
- Staff disagreements
- Loss of data
- Hardware failure
- Online attack

Website health check

Ensure your website software is updated regularly. Check your web developer includes this activity in their maintenance fee.

Check your website analytics regularly. If you spot unusual activity from a country you don't trade with or excessive time spent on your website, ask your web developer to check it out.

Ensure your admin password is complex. Avoid recognisable words and keep the length as long as possible. Change it regularly.

Staff security

Include digital security as part of your induction process

Ensure regular training and updates take place as digital threats are constantly changing

Lock down systems and disable passwords and admin rights when staff leave

1 nshare.co.uk - business continuity http://bit.ly/1sNWJWo - 2 onlincolnshire.org - internet safety fears http://bit.ly/1wSxSPj - 3 pwc.co.uk - cyber security 2014 http://pwc.to/13Hh6sU