

Spam

- Do you ever receive unsolicited emails?
- Do you spend a significant amount of time trawling your inbox to find legitimate business emails?
- Do you ever open emails without validating the source?
- Do you or your staff ever respond to unsolicited emails?
- Do you or your staff ever follow hyper-links embedded in unsolicited emails?
- If your computer systems were rendered unusable for a number of days would your business trade be affected?

If you answered yes to any of the above questions then your business is at risk of being affected by spam.



CASE STUDY

Bespoke Furniture Wholesaler, London

The business was receiving fairly high volumes of unsolicited email, ranging from marketing mail, mostly from the US to emails requesting banking details. Their employees had all been coached to not respond to these emails; however the volumes were causing significant problems.

A key member of the administration team went on leave and during that time her role had to be filled by a less experienced member of staff. The business received several telephone complaints during her vacation from customers getting no response to their emails and taking their business elsewhere. The member of staff admitted that the volumes of spam received were making it difficult

to work efficiently and provide an effective service to clients. Without a working knowledge of key clients it was very difficult to separate legitimate email from spam. Speculative enquiries were even more difficult to isolate.

The business has now opted for a server based anti-spam solution. Now the majority of spam never reaches individuals' inbox, and although a member of staff still checks those emails retained on the server regularly, it is unlikely that they will lose custom or have their reputation damaged in this way again.

Solutions

- + Employ anti-spam software. Software licenses for individual computers can be purchased from well known companies such as McAfee and Symantec whose internet security suites incorporate an anti spam element
- + If your business is larger consider a server based anti-spam solution, or third party server based solution to prevent spam from reaching your network at all
- + Train staff on how to deal with Spam i.e. delete and not to follow links
- + Introduce an email policy and train staff. Incorporate a short, but regular test to ensure procedures are understood and adhered to
- + Do not give away email addresses needlessly on the internet. Ensure business email addresses are used for that purpose i.e. advise staff not to register for products or services using the business email unless vital to the business
- + When sending group emails externally, use the Blind Carbon Copy (BCC) function to keep email addresses private

- + If you deal with certain people regularly and need to be able to respond expediently, set up 'rules' and individual folders within Microsoft Outlook to separate the most important messages. Deal with the rest of your inbox later
- + Always make sure you backup and that the backup is kept offsite. Regularly check that you can retrieve backed up files

Cost/Risk

- + The cost of solutions is relatively low. Much can be done with an investment in time and effective policies/procedures
- + The risk of receiving spam is high. The risk of serious damage to the business is relatively low as the majority of spam will be marketing emails. If not dealt with correctly spam can lead to data loss and systems failure on top of lost productivity

Business Type	Method of Attack	Negative Consequences	Solution	Cost
BASIC + Not linked to the internet + Administration only	+ Users cannot receive spam	+ Data transferred via media storage from an infected computer	+ Anti-virus still recommended	+ Low cost
ONLINE COMPUTER USER + Single machine linked to the internet + Receive email/transact online + Wireless internet access (includes laptops, smart-phones, Blackberrys, PDA's)	+ Email	+ Loss of productivity + Loss of data + Down time + General disruption + Potentially more serious implications via associated viruses & Trojans	+ Install anti-spam and anti-virus software + Ensure automatic regular updates set + Set Microsoft Outlook rules + Staff training on how to deal with spam/unsolicited email i.e. delete, do not open attachments, do not follow embedded links, use viewing pane + Backup, copies onsite & offsite	+ Low cost + No cost + No cost. Some expertise required + No cost. Some expertise required + Low to medium cost
NETWORKED + Same as above, but a collection of computers form a network (The risk increases as there are potentially more staff, increased computer business activity, therefore increased exposure to the risks)	Risks the same as above	As above	Solutions the same as the above but also: + anti-spam solution, probably located on the server, perhaps more sophisticated external solution, dependent on business needs	+ Low to medium cost
ONLINE TRADER + Uses an e-commerce strategy to sell products to a global audience	Risks the same as above	As above	Solutions the same as above	

Useful Websites

- <http://www.ktn.qinetiq-tim.net/>
- <http://www.berr.gov.uk/whatwedo/sectors/infosec>
- <http://www.bcr-uk.org>
- <http://www.businesslink.gov.uk>
- <http://www.getsafeonline.org/>
- <http://www.sophos.com/security>
- <http://www.zdnet.co.uk/toolkits/securitythreats>

For more information about Spam

<http://www.spamfo.co.uk>