

Wireless Network Security & Hacking

- Do you operate a wireless computer network?
- Do you have a wireless router or access point?
- Do you retain information on your network that falls under the Data Protection Act?
- Do you use your computers for online banking?
- Do you send sensitive data via email?

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

CASE STUDY

Commercial Electrical Engineers, Birmingham

Having recently expanded into new premises the business installed a wireless network to allow remote workers to log on when in the office. It was a very busy period, setting up the new office as well as the day to day work. The business banks online and when paying wages one week; noticed a large amount of money was missing from the business account.

The Director contacted the bank immediately; however, they were unable to trace the money in the short term causing serious cash flow problems. Someone had been intercepting bank details and passwords over the wireless network whilst they were doing the banking. The bank eventually agreed to repay the full value of the loss, but it was 'touch and go' for a while. They were fortunate, that their employees were tolerant about the late wages and there were no major bills in the time it took to rectify the problem. If the bank had not extended their overdraft and eventually underwritten the loss, the business would have had to cease trading.

The shock of what can happen caused them to take more drastic action. The company now uses a wired network and have disabled the wireless facility.

Solutions

- + Your router may have wireless functionality even if not used. Disable the wireless feature if not required
- + If using a wireless network, adopt the latest standard of wireless encryption, currently WPA2¹
- + Give your router an obscure ID/Name. Do not leave the default name as this is broadcast visibly and makes it easier for hackers to break into the router itself
- + Do not broadcast the router Service Set Identifier (SSID)²
- + Use Media Access Control filtering (MAC)³, enabling the inclusion of set computers on the wireless network and excluding others
- + Employ a 'firewall'. These vary in complexity and can be software or hardware based. A firewall on its default settings is better than none at all, but a professional may be required to configure more complex settings
- + Always make sure you backup and that the backup is kept offsite. Regularly check that you can restore backed up files

Cost/Risk

- + The risks to a business in failing to protect a wireless network include theft of bandwidth and slowing systems – impacting on productivity
- + Unauthorised remote access of illegal content leaves the business owner open to prosecution and theft of data transmitted over the network, such as online banking details
- + How much you spend on a firewall will depend on the value you place on information that you transmit and hold on that network
- + Ensure that any security software employed has a current license and receives regular updates
- + If data falls under the auspices of the Data Protection Act, you must ensure it is adequately defended, or in the event of its loss suffer fines
- + The cost of encrypting a network and applying MAC address filtering is low

| Business Type | Method of Attack | Negative Consequences | Solution | Cost |
|---|--|---|--|--|
| BASIC + Not linked to the internet + Administration only | + N/A | + N/A | + N/A | + N/A |
| ONLINE COMPUTER USER + Single machine linked to the internet + Receive email/transact online + Wireless internet access (includes laptops, smart-phones, Blackberrys, PDA's) | + Theft of bandwidth + Unauthorised access to illegal content + Interception and theft of data | + Loss of system resources + Slowing down use of internet and email + Legal implications for business owners/directors + Loss/theft of sensitive client data & subsequent damage to reputation + Identity theft of information stolen relating to staff & clients + Malicious damage (perhaps by competitor or disgruntled ex member of staff) + Theft of bank details and online banking passwords | + Use wireless encryption, WPA2 standard, keep abreast of latest standards and upgrade if necessary + Change the default administrative password on the router/access point + Turn off service set identifier (SSID) broadcasting + If your access point allows it, restrict wireless access to the hours that you are likely to use it + MAC address filtering + Limit the IP address pool in the DHCP ⁴ section of your firewall + Do not use a wireless device that projects its signal beyond the boundaries of your premises + Install a firewall that can manage incoming and outgoing traffic + Install good anti-virus software + Ensure regular updates | + Low cost, some expertise may be required + No cost, some expertise may be required + As above + As above + As above + As above + As above + Low to High cost, some expertise may be required + Low cost + No 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) | + As above | + As above | Solutions the same as the above but also: + Consider more sophisticated firewall | + Low to medium cost |
| ONLINE TRADER + Uses an e-commerce strategy to sell products to a global audience (Risk is again generally enhanced as the business and turnover is totally reliant on computer systems functioning correctly) | + Risks the same as above | + As above, plus + Enhanced risk of theft of credit card details and client sensitive financial data + Severe reputational damage | Solutions the same as above, but should become more robust at managing the risks | |

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 further information on secure networks

- <http://www.microsoft.com/uk/smallbusiness/technology-in-business/security/managing-network-security.mspx>

¹ See Get Safe Online http://www.getsafeonline.org/nqcontent.cfm?a_name=glossary_1&letter=W#term_345
² http://www.getsafeonline.org/nqcontent.cfm?a_name=glossary_1&letter=5
³ See Get Safe Online http://www.getsafeonline.org/nqcontent.cfm?a_name=glossary_1&letter=M#term_252
⁴ See <http://www.dhcp.org/>