



Computer Hacking

June 2007

Can you hack it....?

Our E-Business Advisers discuss the business risks posed by hackers (and crackers) - and what you can do to protect yourself:

1. Hacking is a real problem for businesses

Our computers access the Internet via communication channels, connecting our PCs up to a world-wide network of useful information - but also potentially opening up the risk of unauthorised access to your systems and the data held within them.

The term "hacking" has become commonplace to describe this activity, but IT purists say that many people use the term "hacker" when they really mean "cracker".

The difference, they say, is that a hacker does not have a specific purpose in mind when hacking. The hacker hacks mainly for fun, as a joke, or to expose security flaws, whereas the cracker has malicious intent.

The crackers' main aim is to make life difficult for others by breaking into computer systems to steal passwords or valuable information, or to create disturbances in these systems.

In actuality, a "joke" can still be a disruptive annoyance - you want neither a hacker nor a cracker in your systems: we'll just call this kind of activity "hacking" in this paper, in line with what most people call it.

Hackers, ranging from bored adolescents up to talented IT professionals, gain personal or

financial satisfaction, sensational accolade and sadly sometimes peer group 'respect' from 'hacking' into computer systems across the globe.

2. High profile hacking cases

There have been many high profile court cases involving hackers. Convicted hackers face tough sentences for their security intrusion and deliberate destruction of data held on many corporate computer systems.

A recent case is a British man, Gary McKinnon, suspected of hacking into NASA and US military networks. He is currently facing extradition to the USA for his efforts, after legal appeals failed.

He is charged with gaining illegal access and making unauthorised modifications to 53 computers belonging to the US government in 2001 and 2002.

The US government say these incidents caused major disruption and costs of over \$1m.

If found guilty, he faces five years in prison for reportedly stealing administrator identities, deleting 1,300 user accounts, deliberately crashing a network of 2,000 PCs and copying a file containing usernames and encrypted passwords.

The bad news for businesses, though, is that these high profile cases are just the tip of the iceberg.

Most hacking is directed at ordinary businesses and ordinary consumers.....



Fact Sheet

A BBC report of 27 April 2004 stated that “the DTI's Information Security Breaches Survey discovered that 74% of all businesses and 94% of large companies had an IT security incident in the last year, up from 44% of all businesses in 2002 and just 24% in 2000”.

As you can see, hacking is a growing problem for all businesses.

3. ...and all you need is a can of “Pringles”!

Hacking doesn't need to be high tech. You can get hacking “toolkits” from the web if you know where to look - and we're obviously not telling!

More technologically-savvy hackers even have a derogatory name for the kind of person who uses these tools: they call them “script kiddies”.....

Recently, the BBC also reported on how an empty can of “Pringle” crisps could be made to help malicious hackers spot wireless networks that are open to attack.

A security company helped demonstrate that a directional antenna, made with a “Pringles” can, significantly improves the chances of finding the wireless computer networks being used by firms in London's financial district.

The exercise, conducted using this homemade antenna found that over two-thirds of computer networks were doing nothing to protect themselves - they were open to all to spy on.

All the firms could easily have stopped hackers by making a few simple changes to the set-up of their wireless networks.

4. The risk none of us can afford to ignore!

The risk can be just as high and destructive for smaller companies.

They often do not have IT staff with the knowledge to appreciate and manage the risk - or cope with the chaos a hacker attack can cause.

This is a real issue for many businesses holding sensitive commercial or customer data.

Attempts may be made via the Internet to access the data on your PC, probe your systems, scan or test the vulnerability of your network, try to breach your security or password protection without authorisation.

If you have a wireless network, you too need to take steps to protect yourself.

You also need to be aware that hacking isn't something that is just a threat from the external world - unscrupulous staff members have been known to hack their own firms systems, e.g. to find out confidential data such as pay rates etc.

5. Avoiding the havoc.....

Tips to secure your Wireless network

- Disable broadcasting on wireless network hubs.
- Change default names.
- Avoid using a network name to identify your company.
- Move wireless network hubs away from windows.
- Use the built-in encryption facilities.



Fact Sheet

- Disable any networking features you don't use
- Install a firewall between the wireless network and your PC network.
- Regularly test the security of your wireless network.

Security and Passwords

- Ensure your passwords have both letters and numbers
- Try to keep passwords at least eight characters long
- Avoid common words: some hackers use programs that try every word in the dictionary
- Avoid using your personal information or your login name
- Avoid using adjacent keys on the keyboard as passwords
- Never share your passwords online or over the phone

Protect yourself against viruses

- Install anti-virus software
- Update your anti-virus software regularly (see Computer Virus Fact Sheet in this series)

Install a Firewall

- Install firewall software especially if you are a broadband user

- Configure firewall to make it tough for hackers to locate your computer (see the "Firewall" Fact Sheet in this series)

Update your Microsoft Systems

- Always make sure you have updated your Microsoft system to get at least all the critical updates they release.

To do this, in Microsoft Internet Explorer, go to "Tools" on the top menu bar, then "Windows Update", and follow the on-screen instructions.

6. Useful Links

See also "Firewalls", "Spyware / Malware" and "Computer Viruses" Fact Sheets in this series for more information.