

Passwords/Data
Security/Spam/
Phishing/Pharming/
Spyware/Adware/
Viruses/Worms



e-crime

What your
business needs
to know

The Cyber Security Knowledge Transfer Network

has commissioned these guides to assist Small to Medium Businesses (SMEs) in the fight against e-crime. Based on the outcome of focus groups run across the UK, we and the Business Crime Reduction Centre are pleased to provide a series of IT security guides focussing on the key e-crime security threats to business.

In the focus groups, you told us:

- + 'It will never happen to us'
- + 'Why would someone want to target our business and computer systems?'
- + 'The business has nothing that a hacker would want to steal'
- + 'What is the threat? I cannot see it!'

Businesses cannot afford to be complacent. Many attacks are not specifically directed at your business but could affect it nonetheless. Theft of data and identity can lead to widespread damage to your clients, reputation and your bottom line.

This guide will show you:

- + Real examples of businesses like yours being affected
- + The reasons why someone would want to target your business
- + The assets that a hacker wants to steal
- + Details of the threats that face your business
- + The steps you can take to protect your assets

I hope that you find this guide informative and that it inspires you to protect your business from the e-crime threat. There are plenty of links to further information and assistance at the end of the guide, so use them – don't wait to become a victim of e-crime.

Nigel Jones
Director
Cyber Security Knowledge Transfer Network

Passwords

Consider the implications if your passwords were compromised and criminals gained access to your accounts. Money could be stolen, sensitive emails could be read and your business could be seriously damaged. With a 'weak' password in place this is a reality.



Top password tips:

- + Use a password at least 8 characters long, 14 is recommended, and utilise a combination of different cases, numbers and special characters such as !@#\$\$%^&*;,”
- + Use a password that is going to be difficult for anyone to guess
- + Use different passwords for different accounts
- + Change your password every 30 days and use a good selection of new characters
- + Choose a password that you are able to type out quickly so that anyone looking over your shoulder has difficulty in copying it
- + Utilise a password policy. Go to www.bcruc-uk.org for a sample policy
- + Don't use sequences or repeated characters like ZZZZZZ or 123456
- + Don't use your login details or any part of your name

Password Examples	Possible Combinations
Secure	308 Million
SeCuRe	19 Billion
SeCuRiTy	53 Trillion
S3c*R1Ty	6,095 Trillion

“A former member of staff used his account password to login and steal the client database, with the intention of stealing their custom”

CASE STUDY

Telecoms & Communications Business, Midlands

The company was the victim of internal data theft. The database housed all their client details. Every member of staff had access to the database. A former member of staff used his account password to login and steal the client database, with the intention of stealing their custom.

What they should have done was ensure a password policy was in place, outlining both the duties of the employee to ensure their password followed all of the usual security criteria and also ensured that as soon as an employee left, their account was deleted.

Data Security

Most businesses hold data on their computer systems. The threats to a business with respect to data loss include:

- + Loss of productivity, loss of business and in extreme cases a cessation of trading
- + Loss of reputation, where sensitive client details are stolen
- + Loss of data to competitors leading to a loss of clients
- + Possible legal implications under the Data Protection Act
- + Use passwords in accordance with a password policy
- + Control the use of data transfer devices, such as USB memory sticks
- + Ensure compliance with information security and ethical use policies, dictating acceptable usage by staff
- + Employ a backup device to prevent permanent data loss. Backup should be both offsite and onsite for enhanced protection
- + Formulate a 'Disaster Recovery Plan' so the business can continue trading in the event of disaster

There are steps that a business can take to mitigate the risk such as:

- + Use a hardware firewall
- + Encrypt sensitive data and control access to it

“Employ a backup device to prevent permanent data loss. Backup should be both offsite and onsite for enhanced protection”



CASE STUDY

Bespoke Furniture Wholesaler, London

The business was receiving high volumes of unsolicited email. Their employees had all been coached on not responding to these emails; however the volumes were causing significant problems.

A key member of the administration team went on leave and during that time the business received several telephone complaints from customers getting no response to their email 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.

The business has now opted for a server based anti-spam solution. Now the majority of spam never reaches individuals' inbox, and a member of staff checks those emails retained on the server regularly.

Email Spam

Spam is unsolicited email. In the UK spam is not illegal when sent to businesses. The majority of spam is likely to be blanket marketing; however some of it may contain malicious code, such as viruses, trojans or worms.

Spam can have a number of negative effects on your business such as:

- + Loss of productivity when separating legitimate email from spam
- + Clogging up and slowing down computer systems. In the worst case spam can cause a system or server to crash
- + Spam can contain malicious code that leads to more severe damage to systems and loss of data

It is difficult to eliminate spam altogether, there are however a number of solutions to help alleviate the problem:

- + Internet security software packages (from companies such as those referenced at the end of this guide) often include anti-spam solutions. This can mean that legitimate email is sometimes placed in a 'Junk e-mail' folder, so the folder will still need checking
- + For larger organisations with a network, server based anti-spam solutions are available. The advantage of this is that email deemed to be spam will not reach an individual users' computer. The disadvantage with this is that an individual

will need to maintain the server and check the spam folder centrally

- + For larger organisations there are solutions utilising remote third party servers operating a rule based system to filter out spam, so it never reaches the businesses server or systems. Again these can be overly effective, blocking legitimate email
- + Spam can also be limited by ensuring that staff do not give out their email addresses over the internet unless necessary for explicit business reasons
- + Always view suspicious emails with the preview pane and delete if dubious

“Spam can be limited by ensuring that staff do not give out their email addresses over the internet”



Phishing & Pharming

Phishing involves criminals sending out large volumes of emails. The majority of these are sent from 'Botnets'. The spoof emails use fraudulent websites to trick people into giving out personal financial data. The branded email may appear credible but its aim is to steal your data and money. They may also contain malware scripts such as viruses and spyware that execute when the message is opened.

Remember:

- + It is highly unlikely that a reputable company would have lost account information and if they had, they would never request the information via email
- + Ensure your clients are aware that as a company you would never request their personal or sensitive data and to treat any such request with extreme caution
- + Regularly check financial accounts for unusual activity
- + Phishing emails can contain grammatical or spelling errors
- + If you believe you've opened a bogus email then do not click on any links, instead immediately restart your computer and scan with your anti-virus to remove any hidden malware scripts



“The branded email may appear credible but its aim is to steal your data and money”

“Users are directed to fake websites via a bogus email, a virus or spyware, whilst trying to access legitimate websites”

Pharming is similar to a phishing attack. Users are directed to fake web sites via a bogus email, a virus or spyware, whilst trying to access legitimate websites. Viruses can swap legitimate websites in your favourites list to scam sites so what looks like a familiar internet banking site is actually a fraudulent one.

- + Install anti-virus, a firewall and anti-spyware software and run updates
- + Exercise caution over which programmes are run
- + On a website that is secure, there are signs to look for. In the bottom right of the screen there should be a small padlock

(this indicates the website is certified secure) and in the address bar, the http: should have changed to https: the extra s indicating the site is secure. N.B. By clicking on the padlock, the certificate details will be displayed. If nothing happens then exercise caution

Spyware & Adware

Spyware are hidden programmes running on a computer without your knowledge or consent. The programmes track and communicate all on-line activity to a third party. More malicious ones are able to log everything you type, which may include credit card details, important client data and online banking passwords, before sending it back to the creator. If your system runs slowly or becomes less stable it could be a sign that spyware is active.

Spyware is often attached to a free programme aimed at enhancing your computer, such as a screen-saver, or toolbar. Emails are also used to tempt naïve users to open them before installing the malware.

What you can do:

- + Ensure that in addition to anti-virus software, your computer also has anti-spyware capabilities. Newer versions of anti-virus now include anti-spyware
- + Be cautious when clicking on sites, downloading or opening emails and ensure employees and colleagues are aware of the threat



Adware is a piece of software that sits on a computer undetected bringing up adverts, often opening in new windows. It is generally installed in the same way as spyware, however some file sharing sites require users to install adware to subsidise costs.

Whilst adware is annoying and it can take up valuable processing power, it is not malicious and that's what differentiates it from spyware. It will monitor your surfing activity and then tailor new adverts based on that activity but it won't steal private data.

What you can do:

- + Check if your anti-virus software has built in anti-adware capabilities, if not then buy an off the shelf package and enable regular updates
- + Clicking anywhere but the 'X' in the top right corner of an adware window can open up further pop-ups.

“If your system runs slowly or becomes less stable it could be a sign that spyware is active”

“Whilst adware is annoying and it can take up valuable processing power, it is not malicious and that's what differentiates it from spyware”

Viruses & Worms

“There are over 1 million viruses and malicious codes in circulation.”

Symantec Internet Security Threat Report Autumn 2007

A computer virus is software written for the sole purpose of infecting a computer.

Viruses are most commonly spread via email. Other methods such as pictures, screensavers, CD-ROM's and USB memory sticks, present a similar threat.

An email based virus can scan your address book, forwarding the virus to friends, clients and colleagues. In this way a virus can circle the globe in a matter of hours.

A worm is an advanced virus that self replicates and spreads via the internet. In theory it can spread to all computers connected to the internet.

- + The first piece of security software every computer user needs is anti-virus software – it is essential that every computer is protected
- + The anti-virus software must have the ability to receive updates to keep up with the virus writers. It is important to set it so updates are received automatically daily
- + Exercise caution when opening all emails and attachments. Viruses use social engineering tricks to tempt users into opening them
- + Keep up-to-date with patches and software updates



CASE STUDY

Accountants, Birmingham

The business has a list of longstanding clients. They were hit by a virus known as 'Blackworm' or 'Nyxem.E' which spreads via email attachments. The virus targeted Word documents and Excel spreadsheets. Blackworm also disables security features of anti-virus software enabling further infections. The virus destroyed all the .xls and .doc files stored on the hard drives. The loss of client data would have been enough to close the business down.

Fortunately they had a backup system in place. At the end of each week, all data was collated from each employees computer over the network and copied to DVD, dated and stored offsite. The infection highlighted a need for staff training and a review of backup procedure to ensure files could be retrieved.

“A computer virus is software written for the sole purpose of infecting a computer”

Bots and Zombies

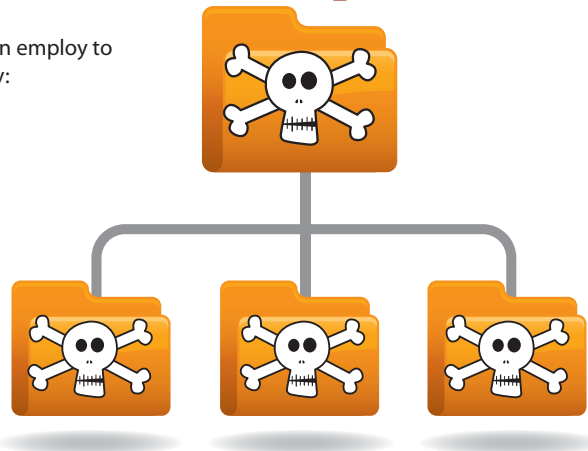
Criminals use viruses and Trojans to exploit weaknesses in software code to gain access to computers and their processing power. The aim is to create a network of slave or 'Zombie' computers; this is called a 'Botnet.' The practical implications for a business having its computers used in such a way include:

- + A loss in processing power and hence productivity
- + 'Zombie' computers are often used to harvest email addresses and send out fake mail. This may affect those that an organisation has direct links with as well as those it doesn't (see spam). This will also dramatically affect the speed of your internet access
- + Botnets are used to bring down company systems and websites

“Criminals use viruses and Trojans to exploit weaknesses in software code to gain access to computers and their processing power”

There are a variety of measures that a business can employ to minimise the risk of becoming a victim in this way:

- + Install anti-virus software and a firewall. Ensure updates are being received and run the anti virus software regularly
- + Monitor computer performance. If the processor is working hard without good reason, it may have been affected (seek professional help)
- + Use the most up to date website browser
- + If not required for business activity, disable 'Activex' and 'java script'
- + Do not allow file sharing applications, as they can download Trojans and other malicious applications
- + Ensure that staff are aware of ethical internet use conditions
- + Produce a security policy



CASE STUDY

Design Company, Manchester

'We just assumed that the computers were slow. It never occurred to us that our computers had become Zombies!'

It was only when an employee became so frustrated with the speed of her computer and looked online for a solution that she found out about Botnets. The company hired an ICT Security Specialist to come in and investigate, and the problem was found.

'We were very fortunate only to have lost productivity through inefficient computers, it could have been much worse. We now ensure that we have all the correct solutions, and most importantly, that all software is regularly updated.'

Wireless Network Security & Hacking



Wireless network security measures are vital to protect the usage of bandwidth and access to a wireless network. If unprotected, the implications can include:

- + Illegal use of broadband by individuals in range of the wireless signal slowing down legitimate internet and email usage
- + Illegal downloading, which when using a wireless connection will rest with the network owner i.e. the business. This includes staff activity and the downloading of unlicensed software
- + Criminals can monitor activity over a wireless network and intercept information, such as banking access codes



It is possible to protect your wireless network and make it less vulnerable to unauthorised access:

- + Businesses should adopt the latest standard of wireless network encryption. Most modern routers will allow this
- + Media Access Control address filtering (MAC) enables the inclusion and exclusion of computers/network cards on the basis of their individual MAC addresses
- + A firewall should be employed to block unauthorised access. A software firewall is a bare minimum, however if a business holds sensitive data a more robust hardware firewall will be necessary. Professional help will be required to configure this effectively
- + Switching off the router at night is a simple and effective security measure

CASE STUDY

Engineers, Birmingham

The business installed a wireless network in their office. They bank online and when paying wages one week, noticed a large debit.

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. The bank eventually agreed to repay the full value of the loss. 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 drastic action. The company now uses a wired network and have disabled the wireless facility.

More Information

Useful Websites

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

List of solutions providers

Please note, this list is not comprehensive, or a recommendation, only a cross section of the market. We recommend that you research thoroughly before making a purchase.

Internet Security Packages

Includes: anti-virus, anti-spyware, a firewall and anti-spam
<http://www.symantec.com/en/uk/norton>
<http://www.mcafee-online.com/uk/store>
<http://www.kaspersky.co.uk/store>
<http://uk.trendmicro.com/uk/home>

Freeware

Free for individuals, businesses usually need to purchase licences.

Anti-virus

<http://www.avg.co.uk/>
<http://www.avastuk.com/>

Anti-spyware

<http://safer-networking.org/en/>

Anti-adware

<http://www.adware-2009.com/v2/>

Firewall

<http://www.personalfirewall.comodo.com/>

e-security Checklist

- Do you have an ICT security policy?
- Do you have anti-virus software?
- Does the anti-virus software receive regular updates?
- Do you regularly scan your computer systems?
- Do you have a Firewall?
- Do you have a hardware Firewall separate from your router?
- Does your Firewall receive regular updates?
- Do you have anti-spam, anti-spyware/adware software?
- Do you use the latest version of your internet browser?
- If you have one, is the wireless network encrypted to Wi-Fi Protected Access standard (WPA2)?
- Is your wireless network protected by Media Access Control address filtering (MAC)?
- Do you restrict access to sensitive data amongst staff?
- Do you encrypt sensitive data?
- Do you take your backups offsite?
- Do you ever try to recover data from your backup?
- Do you train staff on how to deal with suspicious emails?
- Do you have a password policy and do you enforce it?

If you answer no to any of these questions, you need to address your security and procedures. Read through the booklet to find explanation of the reasons why you need to take precautions. If your business is exposed, seek professional help or access further information.

Sources can be found on page 9.

For more information on the Business Crime Reduction Centre, please visit www.bcrc-uk.org or e-mail info@bcrc-uk.org

For more information on the Cyber Security Knowledge Transfer Network, please visit <http://www.ktn.qinetiq-tim.net/>

© Cyber Security Knowledge Transfer Network and People United Against Crime, 2008
Registered Charity No. 1052889

Design by: www.vividcreative.com ©2008

Document last revised March 2009

**BUSINESS CRIME
REDUCTION
CENTRE** ↓

People ↓ United
Against ↓ Crime

