



Federation of Small Businesses
The UK's Leading Business Organisation

Birmingham Chamber
of Commerce and Industry



Protecting your business against fraud



Introduction

E-crime is among the most prevalent of fraudulent activities with the effects often devastating Small and Medium Enterprises (SMEs). Awareness of the risks, together with plain advice on measures to afford some protection are the first steps in combating exposure to e-crime and fraud.

The National Fraud Authority and Action Fraud, working in partnership with the Federation of Small Businesses, Birmingham Chamber of Commerce and Industry and Midlands Fraud Forum have produced and distributed e-crime cards to SMEs in the West Midlands with tips on protecting themselves against e-crime, and this document has now been created to provide further detailed guidance.

This document was written by **Lee Campbell** (Director of Camtech Solutions Limited), a freelance IT security consultant. Lee has over twenty years of IT experience at all levels. He has worked with a number of large financial institutions in the City of London providing network, infrastructure and security consultancy. Lee now runs his own company advising small businesses on IT security. Lee is also a committee member of the Home Affairs Policy Unit within the Federation of Small Businesses (FSB). This role involves advising, raising awareness and providing guidance on e-crime issues affecting small businesses in terms of government legalisation and technical matters.

How to protect your business from e-crime

Install anti-virus, a firewall and anti-spyware on all IT systems	Page 2
Use a password at least eight characters long and utilise a combination of different cases, numbers and characters	Page 3
Be cautious when opening all emails and attachments	Page 4
Introduce an acceptable use policy for internet and email	Page 5
Keep up-to-date with patches and software updates	Page 6
Secure your wireless network	Page 6
Ensure your clients are aware that your company would never request their personal or sensitive data	Page 8
Educate staff so they are aware of the threats	Page 8
Encrypt your data and control who has access to it	Page 8
Employ a backup data to guard against data loss	Page 9

Victims of Fraud

SMEs who have been victims of e-crime should contact Action Fraud (www.actionfraud.org.uk). Action Fraud is at the heart of National Fraud Authority's strategy to make the UK a more hostile environment for fraud and encourages small businesses and individuals who have been defrauded to come forward, call Action Fraud and report the crime.



1 Install anti-virus, a firewall and anti-spyware on all IT systems

This is a well documented security guideline. A number of security products are available on the market. It would be recommended to install a comprehensive security solution that includes anti-virus, anti-spam, firewall, spyware and malware (malicious software includes viruses, Trojans and worms), detection, removal, logging, quarantining and automatic updating. It should also include privacy protection measures. Privacy protection helps mitigate automated collection of user data and traffic analysis when using the internet.

This security product needs to be installed on **every** computer system within the network environment. It must also be installed and configured on systems connecting remotely into the network, either by employees, subcontractors, partners, suppliers or any other 3rd party requiring access to any internal network services. If a remote system is compromised it could infect the internal network, running the risk of a breach of any or all of the three main security properties *confidentially, integrity and availability*.

A security breach may also affect the reputation of the business, incur financial impact, a loss of customers, decreased productivity and induce legal liability. Under the proposed changes to the Data Protection Act (DPA) 1998 an organisation could be fined up to £500,000 for a “serious contravention of the data protection principles which are likely to cause substantial damage or substantial distress to individuals”. One of the eight principles of the act (principle 7) is personal data must be kept secure. The act states “appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”. Installing a comprehensive security solution that includes anti-virus, anti-spam, firewall, content filtering, privacy protection and malware detection would help protect data and privacy. Of course encrypting your data, managing and controlling access (authentication, authorisation and accounting), passwords and backups all help to keep data secure. These DPA changes are intended to be introduced in April 2010.

The anti-virus, spyware and malware signature and definition files need to be updated on a regular basis to help prevent new attacks. Within the small business environment companywide detection, isolation, monitoring updating and removal would be ideal. Any file, database or application servers should also have a security product installed which includes a host firewall. The email server should have anti-spam, anti-virus and content filtering software installed to detect, monitor, remove and report any email containing viruses, spam, inappropriate content or phishing attacks. Multiple lines of defence are the key to mitigate security breaches. As stated in many security articles you are only as strong as your weakest link.

A number of additional security products would help mitigate security vulnerabilities. A vulnerability is a weakness in a system (missing security updates, weak passwords, poor procedures, open ports etc). A threat is a potential source of attack (a hacker). The risk is the likelihood a vulnerability can be exploited by a threat with an associated impact. These additional products include end-point security, monitoring, controlling, reporting and authorisation of storage devices (USBs), removable media (CD's and DVD's), printers, keyboard, mice, scanners and cameras. These security products help to reduce the possibility of data leakage.

An intrusion detection system (IDS) can be installed on systems requiring an additional layer of protection from threats. The IDS sensors monitor and report malicious or suspicious activity occurring on the network or systems. This information is collected and reported to a management station for analysis and an appropriate course of action

can then be taken. The IDS sensors can be located on specific network points, for example, between the external firewall and internal firewall interfaces, and this allows traffic entering and leaving the organisation's network to be monitored. The IDS sensors can also be placed on vulnerable public facing systems such as email and web servers, as well as on internal database servers holding sensitive information.

1.1 Some useful links

www.microsoft.com/security/malwareremove/default.aspx

(Microsoft malicious software removal tool)

www.securityfocus.com/infocus/1266

(Evaluating anti-virus software for small businesses)

www.businesslink.gov.uk/bdotg/action/detail?type=CASE_STUDIES&itemId=1075070335

(Case study of how anti-virus security protected a business)

www.sans.org/security-resources/policies/Anti-virus_Guidelines.pdf

(Guideline on anti-virus processes)

www.microsoft.com/security/antivirus/prevent.aspx

(Help preventing computer viruses)

www.ico.gov.uk/what_we_cover/data_protection.aspx

(An overview of the Data Protection Act)

www.getsafeonline.org/nqcontent.cfm?a_id=1147

(Install anti-virus software)

2 Use a password at least eight characters long and utilise a combination of different cases, numbers and characters

Passwords provide an access control, authentication and authorisation mechanism. Other types of access control mechanisms include security tokens (key fobs) and biometric (fingerprint and iris scans for example). Additional access controls are also available. Passwords allow a system to identify the user, allow or deny access, control when or what can be accessed, monitor access (who logged on when) and provide different levels of access to the system or data.

2.1 Recommendations

- Use passwords with a minimum length of 8 characters, greater if possible
- Make sure all passwords contain a mixture of numeric (0-9), upper case (A-Z) and lower case (a-z) and non-alphanumeric characters (!, ", £, \$, %, *, =)
- Avoid using dictionary words, pet names, relatives names or birthdays as passwords
- Don't use the same password to access different systems
- Change all default passwords, many default passwords are available on the internet
- Change your passwords on a regular basis
- Don't record passwords on pieces of paper
- Do not share, reveal or display your passwords to anyone
- Do not email passwords
- Do not store passwords on computers
- Do not reveal your password to anyone, even when out of the office

SMEs should introduce a password policy similar to the recommendations detailed in which users of the network must adhere to. A password policy could include an account password length, password complexity, frequency to enforce password changes, account lockout threshold (number of failed logon attempts that will cause a user account to be locked out), password history (number of passwords remembered, this prevents users using the same password) and an account lockout duration (how long usually in minutes the account remains locked out after which the account will automatically unlock, if the timeframe is 0 the account will remain locked out indefinitely until an administrator unlocks the account). Many other password policies are also available.

2.2 Some useful links

www.sans.org/security-resources/policies/Password_Policy.pdf

(Password policy template)

www.microsoft.com/uk/protect/yourself/password/create.mspx

(How to create a strong password)

<http://www.threadwatch.org/node/14095>

(Ten most common passwords according to PC Magazine)

3 Be cautious when opening all emails and attachments

The transmission of infectious or phishing emails are popular sources of attack against IT systems and people. The email is used to carry malware (malicious programs such as viruses, Trojans and worms) which are used to infect computer systems. These attacks are designed to corrupt/destroy data, impact the performance reliability and availability of systems. They are also used to monitor and obtain user activity e.g. capturing the key strokes of a password for online banking or email logon. Phishing emails are emails that claim to be from an organisation you trust, typically a bank or other financial institution. The email can look very genuine with the use of the banks logos. The email would request the account holder click on a hyperlink contained within the email to the fake website to confirm their logon credentials (username and password). The email may state that the customer's logon credentials need to be confirmed following a recent upgrade to the banks systems. This account logon credentials entered are captured by the adversary allowing them to gain access to the account holders' genuine bank account.

3.1 Recommendations

Ensure an email security scanner is correctly configured, operational and up to date on the email hosting server and workstations opening the email. The scanner should scan for viruses, spam, Trojans, worms, malware and malicious content and phishing attacks. This provides a multi-layer email security solution. In a SME environment all emails could also be scanned by an integrated gateway security product. This product may contain both a firewall and email scanning system, therefore, providing an additional layer of email security to the organisation. The gateway security device would scan, quarantine, disinfect or remove any unwanted email before entering the network. If an organisation manages and operates its own mail server (Microsoft Exchange for example) the email server should exist within the demilitarized zone (an area of the network that is isolated from the the internal network). If an organisation implements the Microsoft Outlook client and Microsoft Exchange server it's possible to encrypt the data between the Outlook client and the Exchange server. By accessing the email account properties, selecting more settings, then clicking the security tab, the encryption box can be selected.

If home users or small business are collecting email from a POP (Post Office Protocol) server on the internet, additional security measures need to be considered. When a POP email client connects to the internet to collect email the POP account details, username and password are sent in clear text, e.g., <pop_username>, <password>. Therefore, an adversary could listen to this public communication and capture the POP account details, permitting access to the email account. If possible the POP connection should be protected between the POP email client and the POP server using an encrypted connection such as SSL (Secure Sockets Layer). When banking online SSL is used to encrypt the network traffic between the web browser and the bank.

3.2 Additional email recommendations

- Only open email and attachments from senders you know and trust. Of course this is not always possible.
- Setting up a secondary email address using a webmail based email account for public usage, for example online directories, purchases made online and suppliers. This will help reduce the exposure of your real email identity. Of course, this email account may also receive spam and phishing emails.
- Only provide your main email address to trusted people.
- Don't provide your main email address on your web site.

By implementing these security measures it will help to mitigate the level of unsolicited email entering a mailbox. This will help prevent possible infections entering the network by email. This includes viruses, malware and worms. It will also help prevent phishing attacks.

3.3 Some useful links

<http://news.bbc.co.uk/1/hi/technology/7988579.stm>

(More than 97% of all emails sent over the net are unwanted, according to a Microsoft security report)

www.computerweekly.com/Articles/2009/08/13/237068/Email-security-Essential-Guide.htm

(Email security an essential guide)

www.banksafeonline.org.uk/phishing_examples.html

(Example phishing emails)

4 Introduce an acceptable use policy for internet and email

The purpose of an “acceptable use policy” for internet and email usage is to inform network users what is permitted and not permitted behaviour of the organisation computing and network resources. It is designed to remove any misunderstanding and clarify internet and email usage. For example, network users are permitted to access the internet that supports the goals and objectives of the business. The internet cannot be used for undertaking deliberate activities that waste staff effort or networked resources, [example acceptable use policy]. The policy would need to be signed by all members of staff, subcontractors and temporary staff accessing the email or internet from the organisations systems. This would also include remote access. If a person failed to comply with the policy then disciplinary procedures would need to commence.

4.1 Some useful links

www.sans.org/security-resources/policies/Acceptable_Use_Policy.pdf

(Example acceptable use policy)

www.businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1074402879

(Additional information on acceptable use policy)

http://online.businesslink.gov.uk/Growth_and_Innovation_files/Sample__Internet_acceptable_use_policy2.doc

(An example acceptable use policy from business link)

5 Keep up-to-date with patches and software updates

It's important to download and install any operating system and application security updates and patches. Most major software vendors release patches and updates on a regular basis. Microsoft releases updates and patches every month for all its products, if required. These include the various client operating systems (XP, Vista and Windows 7), the Office application suite (Word, Excel, Outlook, PowerPoint, Publisher etc) and Internet Explorer. Updates and patches are also released for the Microsoft server applications, databases and operating systems.

It is possible to automate the download and installation of Microsoft updates by specifying a day. It's also possible to manually download and install updates and patches by clicking the Windows update or Microsoft update application icon on the system to be updated. The Microsoft update application icon provides operating system related patches and updates. The Windows update icon provides a more comprehensive list of Microsoft and hardware updates and patches to be installed. In a SME environment it's possible to use Microsoft deployment utilities such as Windows Software Update Services (WSUS). This Microsoft application provides automated and managed scheduling and deployment of updates and patches to systems on the network.

Computer systems can be exploited by zero-day attacks. A zero-day attack is the threat exploiting a software component vulnerability that has not yet been resolved and made available to the end users. One method to mitigate this type of attack is to use heuristic scanning software. This security product looks for particular attack patterns, rather than relying on traditional signature-based scanning.

5.1 Some useful links

<http://update.microsoft.com>

(Allows manual download and installation of Microsoft and system updates)

www.microsoft.com/security/default.aspx

(Provides general security information)

<http://onecare.live.com/site/en-us/default.htm>

(Microsoft provides a free PC safety scan if running a Windows operating system)

6 Secure your wireless network

A wireless network provides additional functionality and freedom to network users. Rather than be physically connected to the network by the common twisted pair cable it's possible to wirelessly connect using radio waves (no cables, no plugs). However, from a security prospective this presents further challenges.

Wireless network systems connect to the network using a wireless network adapter (usually embedded in the system) to the wireless access point (WAP). The WAP usually connects physically into the organisation's network enabling access to internal network resources such as email, internet, data files and printers. Therefore, if an intruder gains access to the wireless network, it could be possible to access the organisation's internal network. Home users normally connect directly to the internet via the WAP.

6.1 Recommendations

- Change the default wireless access point (WAP) password.
- Disable automatic IP address allocation. This helps prevent casual threats.
- Reduce the strength of the WAP signal if possible, the stronger the signal the greater the distance the radio waves will travel.
- Avoid WEP (wired equivalent privacy) encryption as this is considered a weak wireless encryption protocol.
- Use the WPA2 encryption protocol (Wi-Fi protected access 2) instead of WPA. The WPA2 protocol utilises the AES (Advanced Encryption Standard) cryptography standard for encryption. WPA uses the TKIP (temporal key integrity protocol) for encryption. WPA and WPA2 can operate in two modes. Personal mode uses a pre-shared key (PSK) or password. The user enters the PSK in their wireless connection. The PSK needs to match the WAP key. This key should be long and random to prevent a guessing attack. The second mode is enterprise mode. In this mode the wireless client presents a user-id and password to an authentication system, no pre-defined key is provided to the wireless users requiring access to the network. Each user presents their unique logon credentials to connect to the wireless network. The enterprise mode is generally used in larger organisations.
- Implement MAC (Media Access Control, the physical network address of network adapters/cards) filtering on the wireless access point. This will help restrict which network devices can access the wireless network. However, device MAC addresses can be spoofed.
- Implement hidden SSIDs (service set identifier) on the wireless access points. This will prevent advertising of the access point. However, it's very easy for an attacker to sniff a wireless network when connections are in use, as the SSID is transmitted as part of the wireless operations. Once captured the attacker enters the SSID into the wireless connection. Hiding the SSID will help prevent casual wireless scanning. It also helps to mitigate wardriving, attempting to locate wireless networks by a person in a moving vehicle using a wireless device.
- Access the wireless network using a VPN (virtual private network) connection. Traditionally, VPNs are used to secure network connections over a public network e.g. the internet. VPNs are considered to offer the highest level of wireless protection from intruders. Of course this depends on the implementation and encryption protocols implemented.
- The implementation of network access control could further help to mitigate wireless attacks. Network access control is also used on wired networks to provide an additional layer of security. Users are permitted wireless access by authenticating to an authentication server, usually a RADIUS (remote authentication dial-in user service) server based on user id and password. The 802.1X is an open standards based protocol for authenticating network clients on a user-ID basis.
- Monitor, log and control wireless access.

6.2 Some useful links

http://www.wi-fi.org/files/kc_25_Five Steps to Creating a Wireless Network.pdf

(Five steps to creating a wireless network)

www.sans.org/reading_room/whitepapers/wireless/elements_of_wireless_security_154

(Element of wireless security)

7 Ensure your clients are aware that your company would never request their personal or sensitive data

Inform clients your organisation would never request personal or sensitive information by email. This should help your clients understand that your organisation appreciates information security requirements, and that you take the security and protection of client information seriously.

8 Educate staff so they are aware of the threats

All staff requiring access to the network and systems should undergo security awareness training. This could include password policies, acceptable use of email and internet, awareness of email scams and opening infected emails and attachments, don't install unapproved software (the network security policy should prevent users installing unauthorised applications). In addition to this, lock your workstation when not at your desk, implement a clear desk policy, do not email sensitive or confidential information (passwords, data of birth etc) and do not transfer sensitive or confidential data to external storage devices. If this is required, purchase an encrypted USB storage device to protect the data if lost. Be aware of the dangers of social networking sites (if allowed) and instant messaging (if also permitted) on the network. Finally, explain the security implications of losing a laptop or the device being stolen when containing company information. Ideally, sensitive or confidential data should be encrypted when stored on the laptop. This is not a complete list however it provides a starting point. Usually the greatest weaknesses in the security of a system are the users.

8.1 Some useful links

www.microsoft.com/protect

(Additional information on protecting users and systems)

www.opsi.gov.uk/acts/acts2006/ukpga_20060048_en_7#pt5-pb2

(The Computer Misuse Act 1990 as amended by the Police and Justice Act 2006)

9 Encrypt your data and control who has access to it

Sensitive or confidential data should be encrypted or at the very least password protected. This type of data should never be transmitted over a public network such as the internet or email, unless it is encrypted. Any confidential or sensitive data transferred onto an external storage device or media should be encrypted. Therefore, if the device or media is lost the data is not accessible. As reported in the press a large amount of data has been lost in this manner. Sensitive data includes political opinions, physical or mental health, religious beliefs to name a few. Please refer to the Data Protection Act 1998 for further details on sensitive data.

9.1 Some useful links

http://en.wikipedia.org/wiki/List_of_UK_government_data_losses

(List of UK government data losses)

[http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/security v1.0_plain_english_website_version1.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/security_v1.0_plain_english_website_version1.pdf)

(Guidance on security of personal information)

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_2#pt1-l1g2

(Description of sensitive personal data)

10 Employ a backup data to guard against data loss

All required data should be backed up. A backup policy document should be created. The backups should ideally be kept off site in a secure location in case of fire at the location of the systems. If the backup media is to be kept onsite it needs to be stored in a secure fireproof safe. It is also possible to use an online backup service. Data is transferred in an encrypted format over the internet to a secure data centre. Therefore, in the event of data loss or failure the data can be retrieved directly from the online provider. No need to worry about tapes, USB drives or any other data backup media failing or going missing.

10.1 Useful link

http://www.sans.org/reading_room/whitepapers/backup/

(Guidance on backup strategies)

Disclaimer

Copyright

All content in this document is NFA copyright unless otherwise stated.

Web links

Web links are provided for information and convenience only. NFA cannot accept responsibility for the content of sites linked to, and any links do not represent an endorsement by NFA. We cannot guarantee that these links will work all of the time and we have no control over the availability of linked pages.

Document accuracy

While NFA takes every care to compile accurate information and to keep it up-to-date, we cannot guarantee its correctness and completeness. We do not accept responsibility for any loss, damage or expense resulting from the use of this information.