

SECURITY REPORT ONLINE IDENTITY THEFT

February 2006

Contents

Overview	3
Identity theft	5
What is online identity theft?	7
How do criminals steal an online identity?	9
What can users do to protect their online identity?	13
Ten point guide to protecting your identity online	14
What are ISPs, banks, retailers and software vendors doing to help consumers?	16
What the future holds – identity theft and protection	18
Going forward	19
Conclusion – it’s not just technology...	22
Where to go for advice or help if your identity is stolen	23
Online security glossary	26

Overview

In the UK there are now more than five million broadband users, and consumers are increasingly using the internet to make life easier by conducting everyday tasks, such as banking and shopping, online.

Around one fifth of people in the UK did the majority of their banking over the internet during 2005¹. However, consumers seem unaware of the risks of both new and emerging threats, and often have a ‘head in the sand’ or ‘it’ll-never-happen-to-me’ attitude, despite cyber crime being a major issue and netting more than drug trafficking in the last year².

Indeed 62 per cent of UK consumers thought that online fraud could not happen to them, and over 40 per cent said that they were not aware whether they had been victims of online fraud or not. Of those questioned, one in ten also indicated that they would have no qualms about giving their credit card details to an unidentified third party³.

Internet crime is not just about credit cards, though. A major new and rapidly growing threat is online identity theft, which means that internet users’ identities are used illegally without the knowledge of the individual victims.

This is one of the fastest growing types of frauds in the UK, with eight per cent of UK PC users falling victim to online fraud and 15 per cent knowing someone who has been targeted by an internet criminal⁴. This represents a serious problem for internet users, unless they are made aware of how they can protect themselves from the cause and possible consequences.

¹ Lloyds TSB, January 2006, from a Tickbox.net survey of 1,000 people during December 2005

² Valerie McNiven, US Treasury advisor, November 2005

³ MasterCard Europe, December 2005

⁴ Yahoo! Security Report, June 2005

Identity theft also poses a risk to the continued adoption of the internet as a channel for companies and customers to interact, and this threat needs to be handled in a way that empowers consumers to join the fight against identity theft. Identity theft is a serious and growing problem and government, industry and consumers must work together to find a solution.

This security report, the first in the series, brings together the skills, experience and research of government, law enforcement agencies and industry, including BT, CPP, Get Safe Online, Lloyds TSB, Metropolitan Police and Yahoo!. It will examine what online identity theft is, the current situation and where we go from here, as users and industry attempt to reduce the risks.



Identity theft

Identity theft (or impersonation fraud), whether on or offline, is the misuse of the identity (such as the name, date of birth, current address or previous addresses) of another person without their knowledge or consent.

Obtaining someone's personal details is not a criminal offence, nor is creating fake utility bills or bank statements that can be used to prove you are that person. An offence is only committed when someone attempts to use the stolen identity to obtain goods or services – identity fraud.

Identity fraud is a lot more common than most people think, with a quarter of UK adults having either been the victim of such fraud or know someone who has⁵ – according to CIFAS⁶, there were 137,000 cases during 2005, a 14 per cent increase over 2004. The Home Office estimates identity fraud to cost £1.7 billion or £35 per adult per year⁷, compared with £1.3 billion in 2002.

There are numerous ways in which identities can be stolen, the most common of which are:

- **Bin raiding** – Unskilled fraudsters retrieve documents such as bank statements, utility bills or even junk mail that you have thrown away. The information obtained can be used to apply for credit in your name
- **Phishing** – Fraudulent e-mails pretending to be from your bank asking for your account details. Once obtained these details are used to operate accounts fraudulently.
- **Skimming** – Cloning of payment cards using devices bolted onto cash machines, or copied by unscrupulous individuals with access to credit/debit card, for example, staff in restaurants or petrol stations
- **Moving house** – Mail still being delivered to your old address can

⁵ Which? Magazine, March 2005

⁶ CIFAS, December 2005

⁷ Home Office, February, 2, 2006

be used to set up finance agreements in your name

- **Social engineering** – Inadvertent revealing personal information through lottery scams or cold calling.

However, while public awareness of the dangers of identity theft increased during 2005, publicity centered mostly on the risks posed by offline fraud, such as throwing identifying documents like utility bills in the bin.

The 90 per cent increase in document shredder sales during 2005 shows how well the ‘shred your documents’ message from the Home Office, police and industry has been promoted. However, stealing documents from people’s rubbish is only one of the ways that criminals can steal your identity. The personal details of most individuals may be more easily stolen using the internet than offline.



What is online identity theft?

Whenever someone uses the internet they use an online identity, usually involving passwords, whether that is an email address, online bank account, online retail account or instant-message alias.

Offline, stealing identities is often a piecemeal affair, as thieves gather small pieces of information and gradually create a persona. Online identity theft is a much bigger and more rapid threat that can be perpetrated by criminals anywhere in the world.

The anonymity of the internet means that a criminal can trick users out of their personal details without knowledge of who they are really dealing with. By gathering information about individuals using the internet, such as their email address, bank account and log-in details, criminal elements can become that person online and no one will know until it's too late.

Criminals can also use technology to work on their behalf, by releasing a virus or sending a phishing e-mail, so they can hit millions of internet users very quickly and it doesn't take a high rate of success for this to be a lucrative way to steal information.

If the details have been taken for a specific bank account or service, for example, criminals can use the information to move money, open new bank or credit card accounts, take out loans or increase lines of credit or obtain mobile-phone service on the internet.

Often, the victim won't realise that someone has stolen their online identity until much later, because the criminals don't use a home address for statements or may have changed the address online. They will also try to ensure that victims don't receive any information relating to their hijacked account for as long as possible.

Online identity fraud has hit the headlines recently, after reports that criminal gangs stole millions from the government through tax credit fraud using stolen identities involving the Department for Work and Pensions and Network Rail. However, individuals are equally at risk and are being targeted by criminals across the globe.



The victims of the incidents involving the Department for Work and Pensions had no idea their details had been stolen and were then being used to apply for benefits fraudulently.

Large-scale frauds, like this case, are the ones that get press attention, but for every big fraud there are many smaller ones that never make it to the newspapers, and everyone is at risk.

Some of the consequences of online identity theft include:

- cost, time and hassle involved in resolving the issue
- a bad credit rating and/or loans refused
- final demands for products and services not purchased
- wrongful accusation of criminal activities
- difficulty getting a mortgage
- unwarranted receipt of summons, court actions and county court judgements
- difficulty opening a utility account.

How do criminals steal an online identity?

1. Phishing emails

As in the offline world, there are many ways an identity or details can be stolen online. The simplest way is using phishing emails, an email that purports to be from a bank or financial institution and asks the recipient to enter personal details, such as logins and passwords.

In 2005 there were a series of high-profile phishing attacks, with emails purporting to be from online retailers and payment sites, along with most UK major banks, diverting people to look-alike websites that asked for personal login information.

Not only does this put users' accounts at risk of financial attack, it also puts their identity at risk of being used to defraud others. If they have an account with an online auction site, disclosing account and login details through responding to phishing emails, allows the fraudster access to the account, from which they can defraud others.

In the US, 2.4 million consumers have reported losing money directly due to phishing; of these, approximately 1.2 million consumers lost \$929 million during the year preceding the survey. Almost 30 per cent of respondents, however, said they feared undetected access to private credit reports and other sensitive financial data than defending against phishing attacks⁸. Worryingly, almost half of women and half of 16-24 year olds in the UK do not know what phishing is⁹.

User identities are also at risk if they respond to emails commonly known as 'advance fee' or '419 frauds'. These emails are sent out as bulk spam often notifying the recipient that they have won a lottery or been left a large sum of money. If they respond to these emails, apart from the fact recipients are often requested to pay a fee up front, for taxes or any other alleged fee, they are also requested to provide full identity details and copies of identity documents. Once these have been provided, the fraudsters can then use the stolen identities in other activities.

⁸ Gartner, May 2005

⁹ APACS, November 2005

2. Trojans

There are more technical ways to gather information about an individual in order to steal their online identity, for example, spyware, keyloggers or Trojans. Like the horse from Greek mythology, this malicious software sits dormant within a computer until it is needed.

Once activated, the software can collect information about what is being typed into the computer, such as web-site addresses and personal details, including logins and passwords. It does this by exploiting security weaknesses on operating systems and security software to send the information back to the creator, who can then use it to recreate the stolen identity.

Trojans can be downloaded in a number of ways, but the most common routes are along with content from compromised web sites or as email attachments.

3. Botnets and compromised PCs

Criminals are now creating code that turns infected computers into a tool they can use to launch attacks, which means that unless users are protecting their PC properly it may not just be personal details that are at risk.

The machine might be one part of a large network of computers being used to perpetrate phishing, virus or denial of service attacks, and are termed “bots”.

The ramifications of a computer being involved in this kind of activity can range from the internet connection being closed by the ISP, through to potentially being part of a fraud investigation.

Botnet facts and figures

- Norwegian ISP Telenor disbanded a 10,000 node botnet in September 2005 and Dutch police found and dismantled a 100,000 node botnet in October 2005
- 172,009 new bot-infected computers are identified each day¹⁰
- A botnet of 30,000 zombies is enough to bring down any web site
- There are around one million bot-infected computers worldwide¹¹
- 25.2 per cent of identified bots worldwide are located in the UK, followed by US with 24.6 per cent¹²

4. Man-in-the-middle attacks

A man-in-the-middle (MITM) attack is where an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

The typical scenario is an email is sent from a bank with a bogus link to the web site. When the recipient clicks the link in the email, it takes them to a site that acts as a relay to the bank, so log-on is as normal through the site but the site in the middle can manipulate the content of the transactions.

¹⁰ CipherTrust, May 2005

¹¹ HoneyNet Project and Research Alliance

¹² Symantec Internet Security Threat Report, March 2005

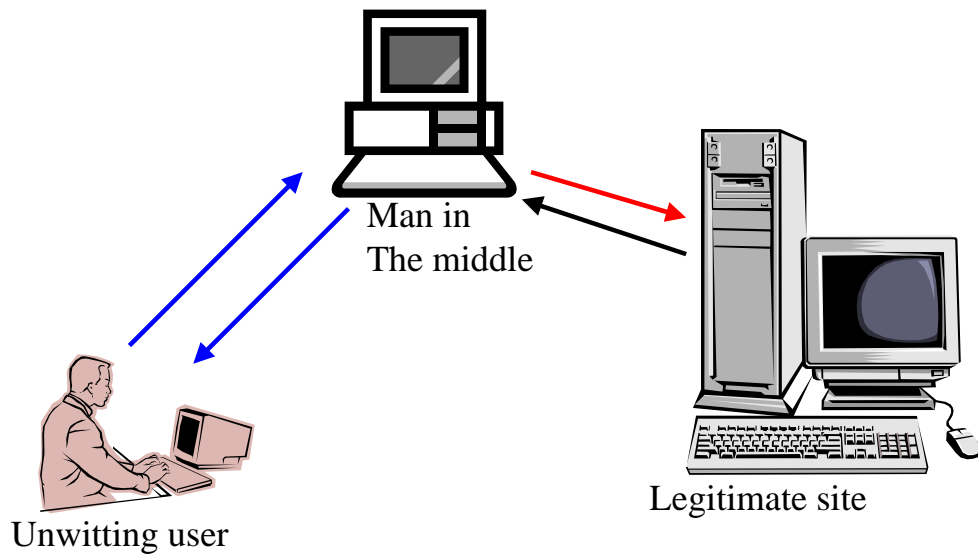


Figure: Man-in-the-middle attack

5. Simple passwords

Other security weaknesses that criminals exploit are:

- consumers using over-simple passwords, including the word “password” itself. A strong password should include letters, numbers and special symbols, for example c3Rt1£Fy8
- users choice of publicly obtainable data, such as a mother’s maiden name or place of birth, as their password
- the failure to change passwords regularly.

Another weakness that can leave people open to attack is the use of the same password to securely access a number of online banks and other web sites. 61 per cent¹³ of computer owners use one main password wherever possible, but this inevitably means that, once a criminal has gained access to one site, they can also access others.

¹³ Yahoo! Security Report, June 2005

What can users do to protect their online identity?

The most important thing is for users to be aware of what they're doing online and the threats on the internet. By treating their online experience as they would an offline experience, like walking down a street they didn't know, users will naturally take the necessary precautions.

Users should ask why banks, financial institutions or any web site are asking for personal details. Banks in particular will never email and ask customers to log in to their site to change details through a link in the email. If users do receive an email claiming to be from their bank or financial institution, they should log into the site by typing the web site address (www.webaddress.com), rather than clicking on the link in an email. This can be made easier by users saving their bank's web site address in their 'favourites' folder.

From an IT perspective, keeping all security software (including anti-virus, anti-spam, anti-spyware, adware defences and firewalls), as well as the operating system, up-to-date will minimise the risks.

How do users monitor financial transactions?

Internet users should ensure they regularly check bank and credit card statements for unauthorised transactions.

In addition, they can carry out occasional personal credit checks with a recognised credit agency to see if there has been any unauthorised use of their name and personal details to obtain credit through any financial institution.

If users discover any financial misuse they should inform the financial institution immediately and confirm this in writing. They can also register the fact that their identity has been compromised with CIFAS or one of the recognised credit agencies to prevent further unauthorised use of their personal details.



TEN-POINT GUIDE TO PROTECTING YOUR IDENTITY ONLINE

1. **Keep your wits about you at all times**

Understand the risks and operate on the internet in the same way as you do in the offline world, with caution and appropriate scepticism. But do not be frightened; with simple precautions it is safe to use online banking and traders.

2. **Question why a Web site is asking for information about you?**

Think about whether it is somewhere or someone you want to give your details to. Only use secure web sites and also use common sense when it comes to phishing emails and web sites

3. **Never give any online security details to anyone unless it is completely necessary**

Be particularly cautious if you share your accommodation with other people. Consider passwording your computer to avoid unnecessary access.

4. **Look after your password**

Change your passwords regularly and avoid standard passwords like family members' names or dictionary words. When creating a password use a combination of letters, numbers and even special characters, like an exclamation mark when possible. This will make your password 'strong'. Do not use the same password for every secure site you are registered with.

5. **Never click on links in emails**

Always type the web site (www) address for banks, financial institutions and retail sites into the browser address line or store them using the browser's favourites function.

6. **Keep up-to-date**

Keep your security software (anti-virus, anti-spam, anti-spyware and firewall), operating system and applications such as Microsoft Office up-to-date at all times.

7. Remove the spies

Check all files on every computer that is connected to the internet at least once a week using anti-spyware and adware applications.

8. Keep your connection secure

Make sure everyone who uses the computer understands the precautions they need to take when online. Do not leave your broadband connection switched on if you are not using it and if you use a wireless modem ensure you set it to use at least 128-bit encryption if you are registered for online banking.

9. If it seems too good to be true, it probably is

Don't open emails or go to sites that claim you have won a prize, unless you've entered a specific competition. If an email looks suspicious and is unsolicited delete it and don't open it.

10. Know where to go for help should you be a victim of online identity theft

There are wide range of organisations and groups that people can turn to for advice should they be the victim of online identity theft. These are outlined below, but include the police, industry bodies and suppliers of online services.



What are ISPs, banks, retailers and software vendors doing to help consumers?

All parties that have an interest in online security, from a range of areas of industry, government and law enforcement, are increasingly working together on initiatives to both educate and protect people when they're online and catch criminals that are using the internet as a tool to make money.

The recent Get Safe Online initiative has brought together Government and law enforcement with companies like BT, eBay, HSBC, Lloyds TSB, Microsoft, securetrading and Message Labs to provide easy-to understand expert advice about online threats and how consumers can protect themselves.

The Home Office has produced information about how to protect your identity and how to spot if someone is using it fraudulently, and law enforcement agencies like the Metropolitan Police have fraud initiatives that allow people to email for advice. They are getting around 400 emails per day about fraud, with many of the alleged attacks being online.

Banks and financial services organisations are also looking at ways to prevent customers falling foul of malicious emails and hacking, including trials of a two-part security system by Lloyds TSB. This is where a key ring-sized security device that generates a six-digit code every 30 seconds is used in tandem with the standard username and password.

Coupled with this is work that the Financial Services Authority (FSA) has been doing around online security. It revealed that more than 50 per cent of people were extremely concerned about the risk of online fraud, yet less than almost a quarter did not know when they last updated their security software.

The industry as a whole is also working together to promote the message that shredding alone will not protect consumers and organisations like CPP are also investigating ways in which criminals steal identities and use them to commit fraud.



Internet Service Providers (ISPs) have a range of initiatives already in place to help customers with online security. Many provide software to protect against viruses and spyware, as well as filter emails for spam and viruses before they reach the users to minimise the risk of Trojans and malicious code being installed on machines. BT, in conjunction with Yahoo!, filters its customers' mailboxes and prevents over 95 per cent of spam reaching their inboxes.

ISPs have developed education initiatives around the risks and precautions users should take when operating online, as many are not aware of the threats, such as phishing and hacking.

Mail providers like Yahoo! Mail, are also developing technologies, such as DomainKeys, to help combat online threats. DomainKeys, developed by Yahoo! offer a cryptography-based solution to solve the problems of phishing and email forgery, as they validate the origin of email messages. It has also recently joined forces with Cisco Systems to create a combined technology solution known as DomainKeys Identified Mail (DKIM), which has been submitted to the Internet Engineering Task Force (IETF) for consideration as an industry standard.

Lastly, ISPs, software providers and government bodies have come together into technical bodies, such as the Messaging Anti-Abuse Working Group to ensure that internet users have the safest possible online experience.



What the future holds – identity theft and protection?

As with the offline world, criminal elements are always looking for ways to make money, so no matter how sophisticated technology becomes, there will always be criminals intent on disruption, fraud or theft. As a result, the threats are constantly evolving and as one door is locked, another new door is opened.

All of the groups involved with the internet, including ISPs, government, law enforcement agencies, banks and vendors are working together to make the internet a safer place for users. BT, for example, has an extensive research department constantly developing and investigating new technologies to help protect its customers online. BT research teams are part of a global community of scientists and technologists that is piecing together a consensus on the future electronic identity infrastructure.

The root of the problem

Today, at the heart of the current problem is the absence of a clear understanding of what an ‘electronic identity’ really means. After all, we cannot protect what we cannot define.

In the offline world, everyone understands what their identity is and how to recognise each other. However, to be used by IT systems, the notion needs to be formalised, and this is surprisingly difficult. A single person may legitimately have multiple digital identities used for different purposes – fifteen to twenty is not uncommon.

A digital identity is not just about getting access to on-line services. It is the means by which the digital world perceives someone, and the owner of an identity often plays an active role in shaping it. Some will create web pages telling the world about their families, hobbies and business. Others jealously guard all personal information, revealing only the bare minimum necessary to take advantage of basic electronic services. Fictitious personae are not just used to perpetrate fraud, but also for harmless recreational purposes, such as role-playing games, or to protect privacy.



Going forward

The threat of online identity theft isn't going to go away. In fact, such crime is set to increase over the next few years, as more criminals go down the online route. But consumers can protect themselves against the threat. Security technologies are advancing all of the time, and keeping apace with what criminals are doing with the internet. With commerce on the internet, there is often the need to identify participants with confidence to ensure that customers, banks and retailers can exchange goods and services legitimately.

A range of internet identity systems have emerged, from those maintained by merchants to support customers' transactions to those established within enterprises for employees. These identity systems are generally not interoperable; identity information held in one system is not generally consumable by another.

Federated identity management addresses this interoperability issue and enables organisations to share trusted identities across the boundaries that separate them. This allows people to use the same user name, password or other personal identification to sign in to more than one organisation and make transactions, simplifying the online experience.

The details and complexity of the identity systems of each are hidden from the other through standards for XML messaging.

A closely related topic is authentication – the process of proving that a person or other entity is really who he she or it claims to be.

Over the next five years we will see personal authentication moving away from the traditional password or PIN to more biometric options, such as voice prints, fingerprints and retina scans, 'one-time passwords' generated by hardware tokens, like those being trialled by Lloyds TSB, and use of other personal devices, cards and 'dongles' as proof of identity.

'Two factor authentication', in which two-by-two independent means are required to prove identity will become the norm. We will also see an increased use of two-way authentication, where web-site owners such as



banks will have to prove their identity to customers, as well as the other way around.

Cryptography, digital certificates and related techniques will be used more extensively to protect the confidentiality and integrity of information and to provide reliable audit trails.

They will also be used to allow computers to distinguish between authentic and dubious software and hence reduce the threat from 'malware'. Proliferation of tamper-proof trusted hardware modules embedded in computers and other devices will also help here.

Improved methods and tools used by software developers will reduce the number of 'bugs' and other vulnerabilities in operating systems and application programmes, though this will be a gradual process. Vulnerabilities will never be eliminated entirely, but techniques for detecting and reacting to attacks and other problems will become more automated and effective. One line of research inspired by imitation of nature aims to make IT self-defending and self-repairing.

Conclusion – It's not just technology...

While technological developments will always increase the safety of the internet, individual users can do much more to protect themselves and their computers. In doing so, they will also help to make the internet more secure for others.

Technology and service providers are striving to make the internet a safer place, but security is not purely a technological issue. The internet is an amazing tool, but without the proper precautions it exposes consumers' lives and identities to risks in the same way as not locking your front door.



Where to go online for advice or help if your identity is stolen

- **APACS** – is the UK payments association is the trade association for institutions delivering payments services to end customers. It is also the main industry voice on issues such as electronic payments, electronic banking and e-banking fraud. APACS maintains banksafeonline.org.uk
www.apacs.org.uk
- **The British Bankers' Association (BBA)** – is the leading trade association in the banking and financial services industry representing banks and other financial services firms operating in the UK
www.bba.org.uk
- **BT** – provides a range of advice and services as part of its broadband packages to help customers protect themselves and the things that are important to them
www.bt.com
- **Card Watch** – is the UK banking industry's body that works with police, retailers and organisations including Crimestoppers to fight plastic card fraud
www.cardwatch.org.uk
- **CIFAS** – is the UK's fraud-prevention service with over 240 member organisations spread across banking, credit cards, asset finance, retail credit, mail order, insurance, investment management, telecommunications, factoring, and share dealing. It provides a facility for people who think their identity has been stolen, who have lost identity documents to register a warning with their members for a small fee
www.cifas.org.uk
- **Code Fish Spam Watch** – is a web site dedicated to following and exposing spam scams
www.code.org



- **CPP** – is an industry expert on identity fraud prevention, and provides a range of advice, assistance products and services
www.cpp.co.uk
- **Fraud Alert** – is the Metropolitan Police Economic and Serious Crime Directorates web site maintained by its ST£LING Prevention and Partnership Unit
www.met.police.uk/fraudalert
- **Get Safe Online** – is an initiative sponsored by government and leading businesses, Get Safe Online. It provides expert advice to protect everyone against internet threats
www.getsafeonline.com
- **Home Office Identity Fraud Steering Committee** – is a collaboration between UK financial bodies, government and the police to combat the threat of identity theft
www.identity-theft.org.uk
- **Interactive Media in Retail Group (IMRG)** – is the industry body for global e-retailing
www.imrg.org
- **Lloyds TSB** – is a UK bank that is working closely with industry and government to help protect customers’ financial transactions online
www.lloydstsb.com
- **Miller Smiles** – is the internet's biggest archive of spoof email and phishing scams, where people can go to check whether emails they have received are part of a “scam”
www.millersmiles.co.uk
- **Spamfo** – provides spam information and is a resource with information relating to spam, news, reviews, FAQ and useful links
www.spamfo.co.uk



- **Yahoo!** – Yahoo!’s Security Centre provides the latest virus and spam news, information and tools on how to keep yourself as safe as possible online.

www.yahoo.co.uk/securitycentre



Online security glossary

Address spoofing – A type of attack in which the attacker impersonates a legitimate system by stealing its web site address.

Adware – Software incorporated in the advertising that's included in, or linked to, a web page. It can be innocuous, but can also gather data from the user or the user's computer and feed it back to the advertiser.

Authentication – The act of making sure that a person or other system that is trying to access a system is correctly authorised to do so.

Biometrics – The use of measurable biological characteristics, such as fingerprint recognition, voice recognition, retina and iris scans to provide authentication to computer systems.

Cracker – Someone who breaks into computers, usually for fun or political motives and occasionally (but rarely) for financial gain. Cracking is the act of breaking into computers.

Cryptography – The process of converting information into a secret code, called cipher text, by an encryption algorithm. Cryptographic services can provide confidentiality, integrity, authentication and non-repudiation.

Cybercrime – A collective term used to describe the range of attacks it is possible to make against an organisation by electronic means.

Denial of service – The process by which legitimate users, customers, clients or other computers are prevented from accessing resources on a computer by an unauthorised party. This is usually accomplished by overwhelming a computer with bogus requests, or by tampering with legitimate requests.

Encryption – The process of scrambling information to prevent unauthorised disclosure or modification using mathematical techniques. Techniques normally use an encryption algorithm with a key to ensure that only the intended recipient can read the information.



Firewall – A system with both hardware and software components that manages information flow between an organisation's internal private network (intranet) and the internet. They can be used to filter out certain types of traffic, to block access to unauthorised internet users while permitting access to certain trusted users and systems.

Hacker – Originally used to describe someone with a deep and thorough understanding of computers and considerable skills and ability to program them. Misuse in the media has led to the term becoming synonymous with 'cracker', much to the dissatisfaction of the small genuine hacker community.

Identify theft – Using spyware or other mechanisms, fraudsters can acquire sufficient details about a person to impersonate them or undertake business or financial transactions on their behalf.

Malicious code – A term for a virus, hostile applet or code fragment downloaded from a web server or sent directly from one system to another.

Pharming – Pharming describes the situation in which a hacker exploits weaknesses in domain name server (DNS) software to acquire the domain name for a site and redirect traffic to it to his or her fake site.

Phishing – This is a form of identity theft. People receive emails that look like they come from a legitimate company asking them to update their records and to verify their username and password. Alternatively, the mail may ask the recipient to carry out some sort of transaction. Users who reply with the requested information or go to a linked fake web site and give their personal or financial information to the fraudster have a security certificate.

Spam – Spam is unsolicited email. The term can include both marketing emails from bona-fide companies, less tasteful mails from people promoting pornographic web sites, mails designed to tempt the recipient to complete a financial transaction with a fraudster, phishing attempts and mails carrying viruses or worms.

Spoofing – Pretending to be someone or something else.



Spyware – Software that monitors how a computer is used and sends reports to another computer via the internet. Spyware programs have been created that log credit card numbers or username and password entries, for example, enabling identity theft. Another example is rogue dialler software that causes a user's PC to call a premium rate phone line instead of their ISP's standard number. Spyware has also been used to initiate Distributed Denial of Service (DDOS) attacks, causing large numbers of infected computers to launch a coordinated attack on a specific web site.

Trojan – A form of virus. Once on a computer, Trojan programs run in the background deleting files or scrambling their contents. Alternatively, they can allow the computer to be controlled remotely, giving someone else access to files and applications.

Virus – A piece of malicious code which may erase data, use up system resources and use a system to propagate copies of itself to other systems. Viruses are frequently loaded by accident or without the knowledge of the system owner. Users can protect themselves against viruses by installing anti-virus software.

Worm – Worms are network-savvy viruses. They are designed to discover and exploit weaknesses in a network prior to propagating themselves from computer to computer.