Leicester
City Council

A Detailed Briefing Paper for Elected Members
Protecting Your e-Identity
V1 6 April 2009

Introduction

1. Traditionally, harassment and stalking has been something that is very direct and physical, whilst that remains true we now also face the same crimes the world of IT and the Internet.

2. Everyone is open to e-Harassment but as a recognisable public figure Elected Members are at heightened risk as they need to be contactable by their electors not just by phone but by email. Thus they are open not just to the SPAM that all email users suffer, but also to abuse through email by those who regard politicians of all levels and persuasions as targets.

3. Politicians were amongst the first to realise and exploit the wider potential of Social networking sites, public web posting sites for video-clips, and Chat and Blog. But these are now being used as platforms targeting personal abuse and attacks of many forms at Members.

The Threat

4. The Threat comes from abusers exploiting the usual list of IT Threats; Spyware, Hacking, SPAM, Phishing. These we see regularly used for identity theft and attacks aimed at stealing our money or our financial credentials such as our credit cards. Now these methods are being exploited by the would be harasser to get up close and personal with the victim in the electronic environment but whilst the victim may understandably fear physical violence the key targets are money and reputation – and for those in the public eye the latter is likely to be foremost.

5. Sometimes we are put at risk by others such as when data about us is not sufficiently protected. Sometimes we leave ourselves open through simply not being aware of how our use of email and the internet can be turned against us.

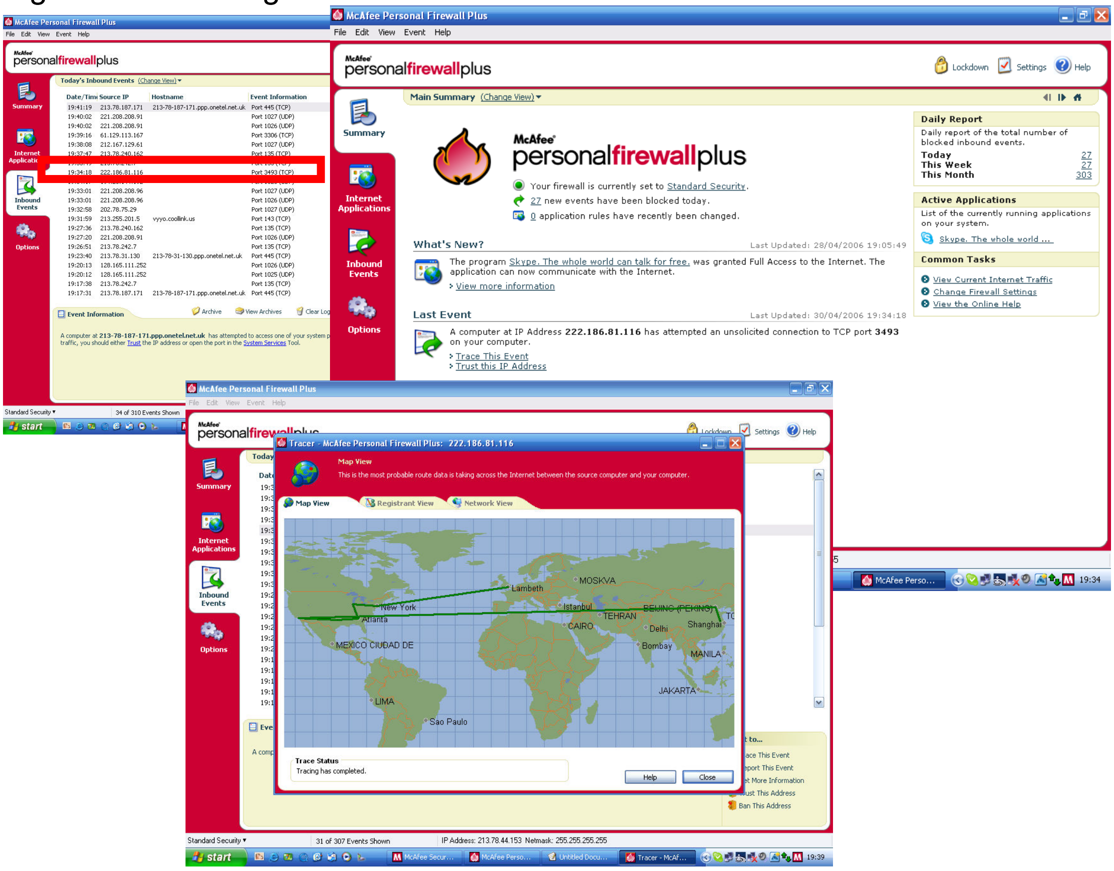
6. But we can fight back and the first steps are to understand the threat and how we can limit our exposure.

Hacking

7. The spectre of the hacker was one of the earliest recognised threats on the Internet, often pictured as the spotty teenager in a back bedroom somewhere. Some of these really existed and whilst some have grown up and moved on to getting socially valuable lives others have moved on to using their skills for criminal gain. As in all walks of life where there is money to be made organised crime is never far away and this is certainly true with the internet organised crime gangs, often eastern European based, that include people who can be very direct in their methods of dealing with those who cross them.

8. Whilst the hacking of an individual computer is possible, the majority of activity that we see at a personal level is the fully automated probing of computers looking for vulnerabilities to be exploited. This activity goes on at an industrial scale relying on us not getting the basics right, ie having a firewall, having antivirus and antispyware programmes that are kept up to date and patching our software programmes.

Fig. 1 – Firewall log



Today's Inbound Events (Change View)

```
Date/Time  Source IP        Hostname                        Event Information
19:41:19   213.78.187.171   213-78-187-171.ppp.onetel.net.uk Port 445 (TCP)
19:40:02   221.208.208.91                                    Port 1027 (UDP)
19:40:02   221.208.208.91                                    Port 1026 (UDP)
19:39:16   61.129.113.167                                    Port 3306 (TCP)
19:38:08   212.167.129.61                                    Port 1027 (UDP)
19:37:47   213.78.240.162                                    Port 135 (TCP)
19:34:18   222.186.81.116                                    Port 3493 (TCP)
19:33:01   221.208.208.96                                    Port 1027 (UDP)
19:33:01   221.208.208.96                                    Port 1026 (UDP)
19:32:58   202.78.75.29                                      Port 1027 (UDP)
19:31:59   213.255.201.5    vyyo.coollink.us                 Port 143 (TCP)
19:27:36   213.78.240.162                                    Port 135 (TCP)
19:27:20   221.208.208.91                                    Port 1026 (UDP)
19:26:51   213.78.242.7                                      Port 135 (TCP)
19:23:40   213.78.31.130    213-78-31-130.ppp.onetel.net.uk  Port 445 (TCP)
19:20:13   128.165.111.252                                   Port 1026 (UDP)
19:20:12   128.165.111.252                                   Port 1025 (UDP)
19:17:38   213.78.242.7                                      Port 135 (TCP)
19:17:31   213.78.187.171   213-78-187-171.ppp.onetel.net.uk Port 445 (TCP)
```

Event Information

A computer at **213-78-187-171.ppp.onetel.net.uk** has attempted to access one of your system p traffic, you should either Trust the IP address or open the port in the System Services Tool.

34 of 310 Events Shown

Main Summary (Change View)

Your firewall is currently set to Standard Security.

27 new events have been blocked today.

0 application rules have recently been changed.

What's New? Last Updated: 28/04/2006 19:05:49

The program Skype. The whole world can talk for free. was granted Full Access to the Internet. The application can now communicate with the Internet.

› View more information

Last Event Last Updated: 30/04/2006 19:34:18

A computer at IP Address **222.186.81.116** has attempted an unsolicited connection to TCP port **3493** on your computer.

› Trace This Event
› Trust this IP Address

Daily Report

Daily report of the total number of blocked inbound events.

Today	27
This Week	27
This Month	303

Active Applications

List of the currently running applications on your system.

Skype. The whole world ...

Common Tasks

- View Current Internet Traffic
- Change Firewall Settings
- View the Online Help

Tracer - McAfee Personal Firewall Plus: 222.186.81.116

Map View

This is the most probable route data is taking across the Internet between the source computer and your computer.

Trace Status

Tracing has completed.

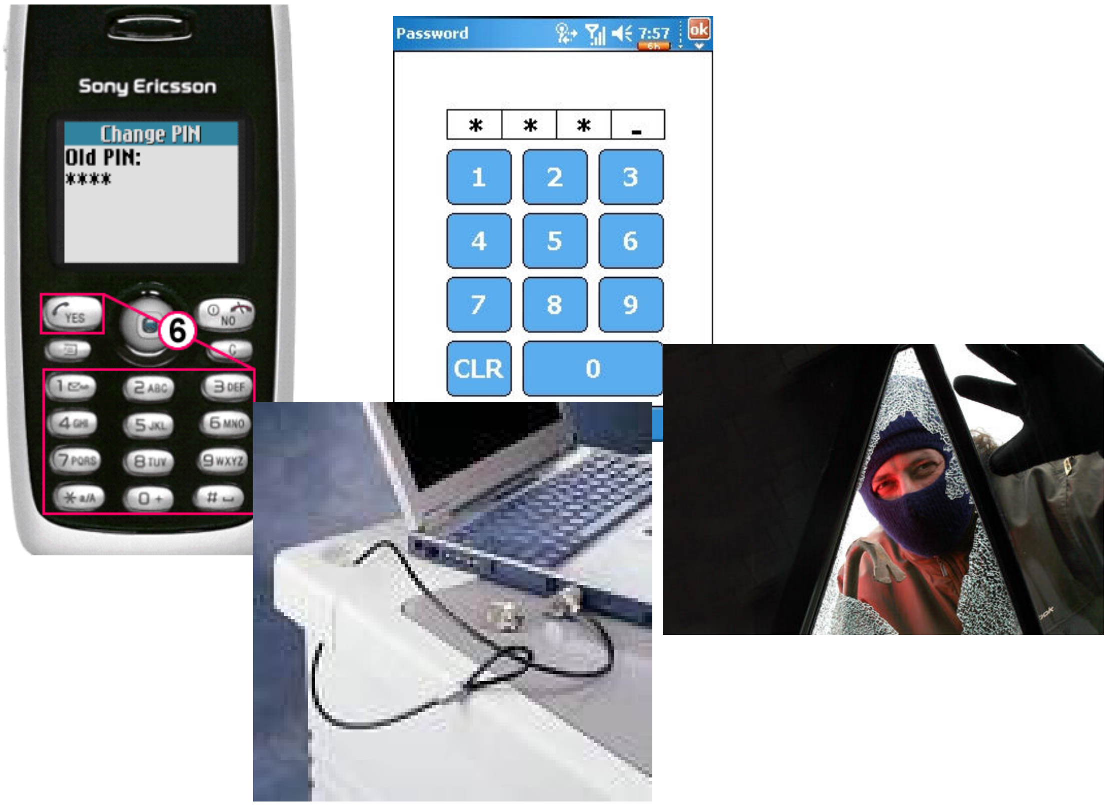
31 of 307 Events Shown IP Address: 213.78.44.153 Netmask: 255.255.255.255

9. Fig. 1 shows the log from the firewall of a home PC, reporting an automated probe from somewhere in China. This happens continuously to all of us who use the Internet which is why the basic best security practices are so important.

Safeguard Your IT Equipment

10. Use the simple ready to hand tools to protect your self, lock equipment down, with mobile devices be they phones, PDAs, laptops or whatever, use passwords and PINS to prevent their use by others. Never leave equipment on show in a car and if you are a laptop user get a security cable to secure it when in use out of your own environment.

Fig 2 – Basic precautions



11. For LCC equipment you can order a security cable through IT Procurement and similar products are available through IT retailers for use with your personal equipment.

12. Your LCC equipment sits within an envelope of corporate protection measures, including; system and application patching for vulnerabilities, firewalls, antivirus (including anti-spyware), SPAM filtering etc etc. As a public figure it is doubly important that you apply the same measures to our own personal equipment. Do the commonsense basics:

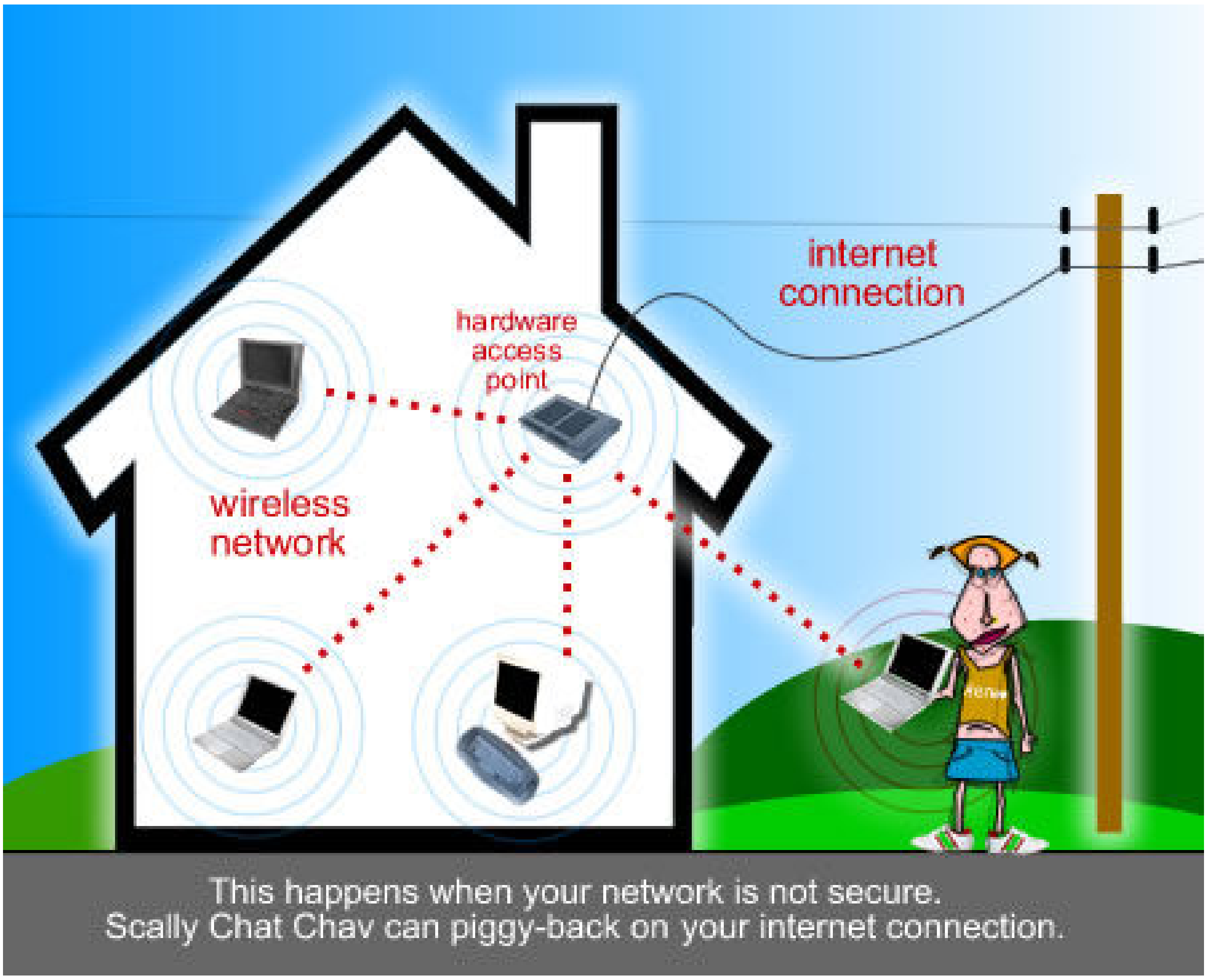
- Get a Firewall
- Get regularly updated AntiVirus
- Get antispyware
- Use a reliable email service that has antiSPAM.

13. None of this need involve major expense, many really good products are freely available - see the note “A guide to Protecting Your Home PC” on Insite.

WiFi Piggyback

14. Many people use WiFi connections at home to connect multiple pcs to a single internet connection or simply to allow flexibility in the home. WiFi is incredibly useful but it’s very easy to get wrong - commercial statistics show that 1 in 6 wireless users leave their wireless router unprotected and one in nine admit to piggybacking ie connecting to someone else’s router to use the internet for free. Leaving your wireless connection open means others can potentially steal your passwords, bank details and identity information. Additionally if your wireless access is used to access illegal sites such as paedophilia then you, as well as the real offender, could be liable for prosecution.

Fig 3 – WiFi Piggyback


internet connection
hardware access point
wireless network
This happens when your network is not secure.
Scally Chat Chav can piggy-back on your internet connection.

15. Protect your wireless internet connection with:

- a strong password
- change the administrative password

- check you use WPAv2 encryption as a minimum and not the older and weaker WPA or even worse WEP

16. WiFi access points provided by the Council will meet these standards.

Spyware

17. Spyware represents an insidious threat to privacy and can result in financial fraud. It is also a huge pain to live with. In simple terms it's a type of virus that can be installed on your computer without your knowledge. It is capable of logging your activity on the keyboard thereby capturing your passwords and other personal information. Infection usually occurs when it is installed alongside another program such as a peer to peer file sharing application. It's increasingly, blending with viruses making it harder to eradicate and harder to avoid.

18. There are different types of Spyware including adware which is designed to get you to visit commercial websites. Typically Adware Spyware will:

- Pop up unwanted adverts, including offensive material.
- Download adverts from the internet, taking up your bandwidth.
- Hijack your browser so that new menus appear or your default home page or search page is changed.
- Put new icons on your desktop.
- Block access to certain websites.
- Try to get you to shut down anti-virus and antispyware or block updates.
- Track your online activities in an effort to send you more adverts.

19. Surveillance spyware is the most extreme version. In common with some viruses it can:

- Scan your hard disc for private data such as credit card numbers.
- Log the keys you type scanning for passwords or credit card numbers.
- Take screen shots of the sites you visit to capture personal information.
- Upload this information to criminals over the internet.

20. Sometimes spyware will advertise so-called spyware removal programs. This is a kind of extortion and you should stick to trusted anti-spyware applications

Preventing Spyware

21. The basic protection is to get antivirus and antispyware programmes and keep them up to date. In addition to that, download material from the internet with caution – some spyware installs alongside advertising-funded programs downloaded from the internet. So:

- Wherever possible, buy reputable software from reputable companies.

- If you download free software from the internet, exercise caution and only use trusted websites that operate a no-spyware policy, such as download.com.
- Be especially wary of programs that appear to be pirated or distributed from P2P file sharing networks.
- Be wary of 'free' programs that might be paid for by advertising.
- Be wary of 'free' programs that offer to install additional programs during the install process.
- Read the small print on licences for programs you download from the internet to make sure that you aren't giving permission for adware to be installed on your computer.
- Be careful about the websites you visit. Avoid dubious sites because these can also install spyware.

SPAM

22. Everyone suffers from unwanted emails or SPAM, but email may also be used very specifically as a means of personal harassment. The Council gives you an LCC Groupwise mail account to use as an Elected Member but additionally we recommend that you have separate mail accounts for your party political and private lives.

23. Never:

- Give out the email address for the service that you use for your private life to any one other than family and your most trusted friends.
- Autoforward from your LCC mail account to a private one – you are putting at risk Council information and potentially information protected under the DPA.
- Use your LCC Groupwise email account as your primary account for your Party Political work.

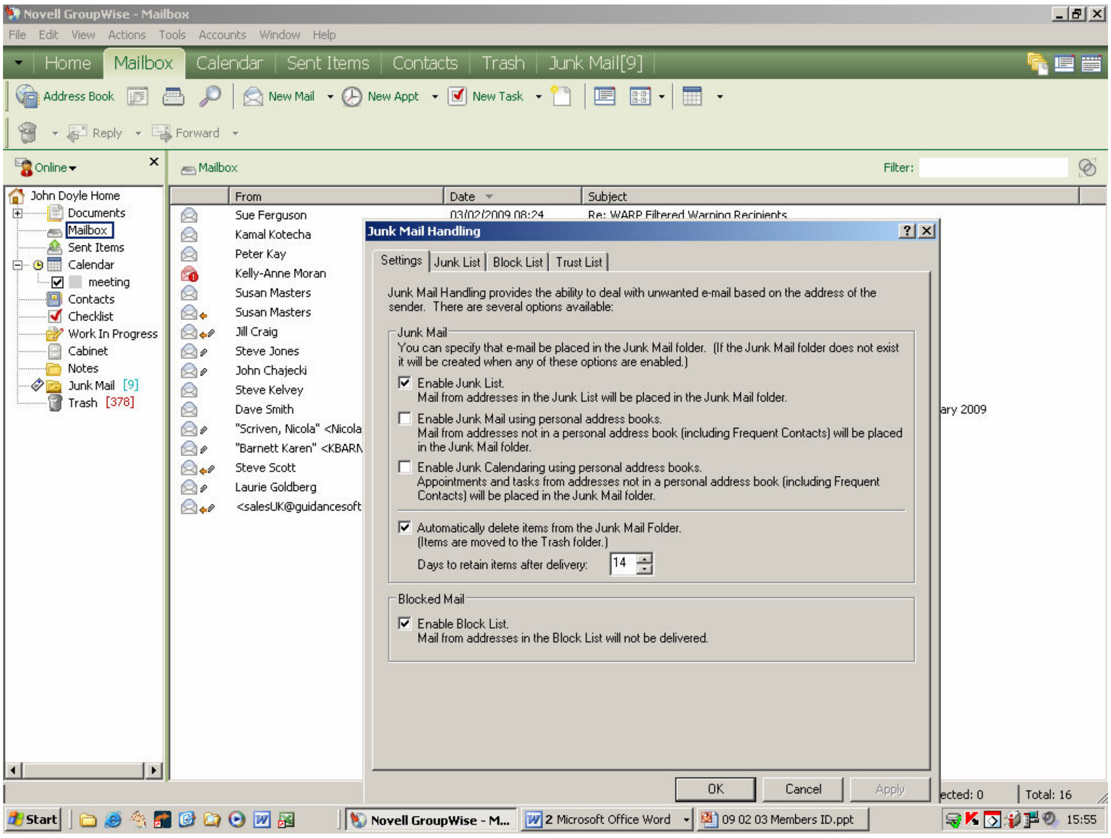
24. For the Council we already block the majority of SPAM (approximately 20% of all incoming mail to the Council) that comes into our mail service from the Internet but a percentage will always get through. What we are not able to block is abusive mail that comes from individuals as this mail will not be recognised as SPAM, additionally we could be accused of limiting access to you which clearly we do not want to do!

25. You have the facility to start to filter out mail from abusive sources simply by placing any mail you chose in the Groupwise JunkMail Folder then any subsequent mail from that address will then automatically be sent to JunkMail. Periodically, you should move items from the Junk Mail folder into Trash. You can automate this very easily as follows:

- Right-click on the Junk Mail folder
- Select Junk Mail Handling
- Tick the Automatic Delete box, and set the number of days to 7 or 14, depending on the volume of junk mail you are receiving.

Once the emails are in Trash, they are included in your usual procedure for deleting items, whether you do this manually or via a GroupWise Rule.

Fig 4 – Groupwise Junk Mail Handling



Junk Mail Handling

Settings | Junk List | Block List | Trust List

Junk Mail Handling provides the ability to deal with unwanted e-mail based on the address of the sender. There are several options available:

Junk Mail

You can specify that e-mail be placed in the Junk Mail folder. (If the Junk Mail folder does not exist it will be created when any of these options are enabled.)

☑ Enable Junk List.
Mail from addresses in the Junk List will be placed in the Junk Mail folder.

□ Enable Junk Mail using personal address books.
Mail from addresses not in a personal address book (including Frequent Contacts) will be placed in the Junk Mail folder.

□ Enable Junk Calendaring using personal address books.
Appointments and tasks from addresses not in a personal address book (including Frequent Contacts) will be placed in the Junk Mail folder.

☑ Automatically delete items from the Junk Mail Folder.
(Items are moved to the Trash folder.)

Days to retain items after delivery: 14

Blocked Mail

☑ Enable Block List.
Mail from addresses in the Block List will not be delivered.

OK Cancel Apply

26. The majority of Internet email Service Providers are aware of their public responsibility to try and prevent their service as a means of abuse and will take action to block senders of such mails where they can. Free to use email services such as Googlemail and HOTMAIL operate SPAM filtering and have clear terms and conditions for use and Privacy Policies. Make sure you understand how to use the SPAM filtering available and any other service that may help you cut down unwanted mail.

27. Remember if you're the victim of on-line abuse that you have recourse to the Police who can deal with criminal activity and you may wish to seek independent legal advice or contact the Council's Solicitor, Peter Nicholls.

28. Be Suspicious of Unsolicited Emails - You are in the public arena and your email address is constantly being "farmed" and then reused.

On-Line Shopping and Banking

29. In the UK over 40 per cent of the adult population, nearly 20.6 million people which represents 55 per cent of internet users, now bank

online. More and people are using their online accounts more regularly with one in five of us accessing our accounts daily compared to one in thirteen just four years ago.

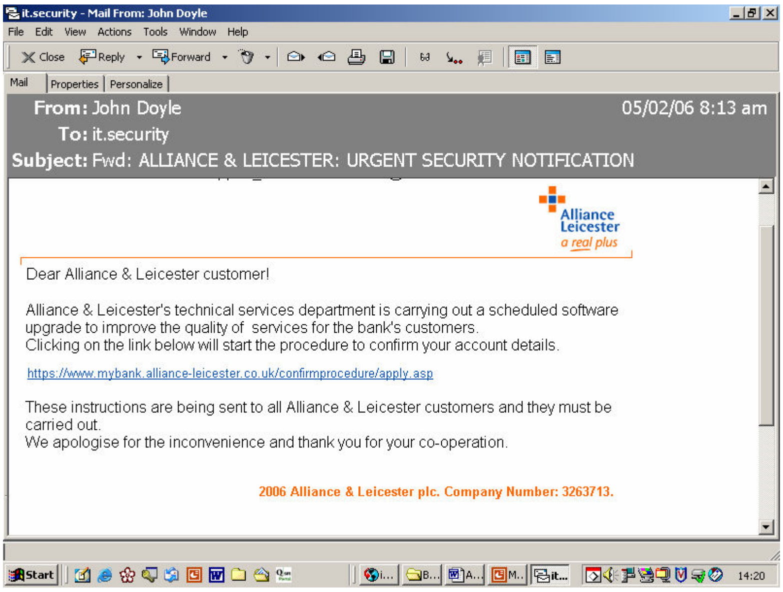
30. All that activity represents an attractive target to criminals but because the banks' own systems have proved difficult to attack, criminals have turned their attention to getting information directly from online banking customers themselves. As with banking many of us now shop on line and that area too is being targeted.

31. Most fraud on online bank accounts involves a customer being tricked into giving away their user passwords and security information by a phishing scam, or by their computer being infected with spyware designed to steal the information.

Phishing

32. Criminals are constantly attempting to gain identities and financial details which is termed "Phishing". This is done in a variety of ways, most commonly the spoofed email claiming to come from a bank or building society asking you to check your account details and password. Remember no financial institution will contact you by email and ask for password or other sensitive info or ask you to enter same into an on-line form or website. Note particularly the embedded link in the email at Fig 5, these are often used to install spyware on your computer. Never follow such links or cut and paste, always type in the address that you want to visit or use your "Favourites" list.

Fig 5 – Phishing - Spoofed Financial email



From: John Doyle 05/02/06 8:13 am
To: it.security
Subject: Fwd: ALLIANCE & LEICESTER: URGENT SECURITY NOTIFICATION

Dear Alliance & Leicester customer!

Alliance & Leicester's technical services department is carrying out a scheduled software upgrade to improve the quality of services for the bank's customers.
Clicking on the link below will start the procedure to confirm your account details.

https://www.mybank.alliance-leicester.co.uk/confirmprocedure/apply.asp

These instructions are being sent to all Alliance & Leicester customers and they must be carried out.
We apologise for the inconvenience and thank you for your co-operation.

2006 Alliance & Leicester plc. Company Number: 3263713.

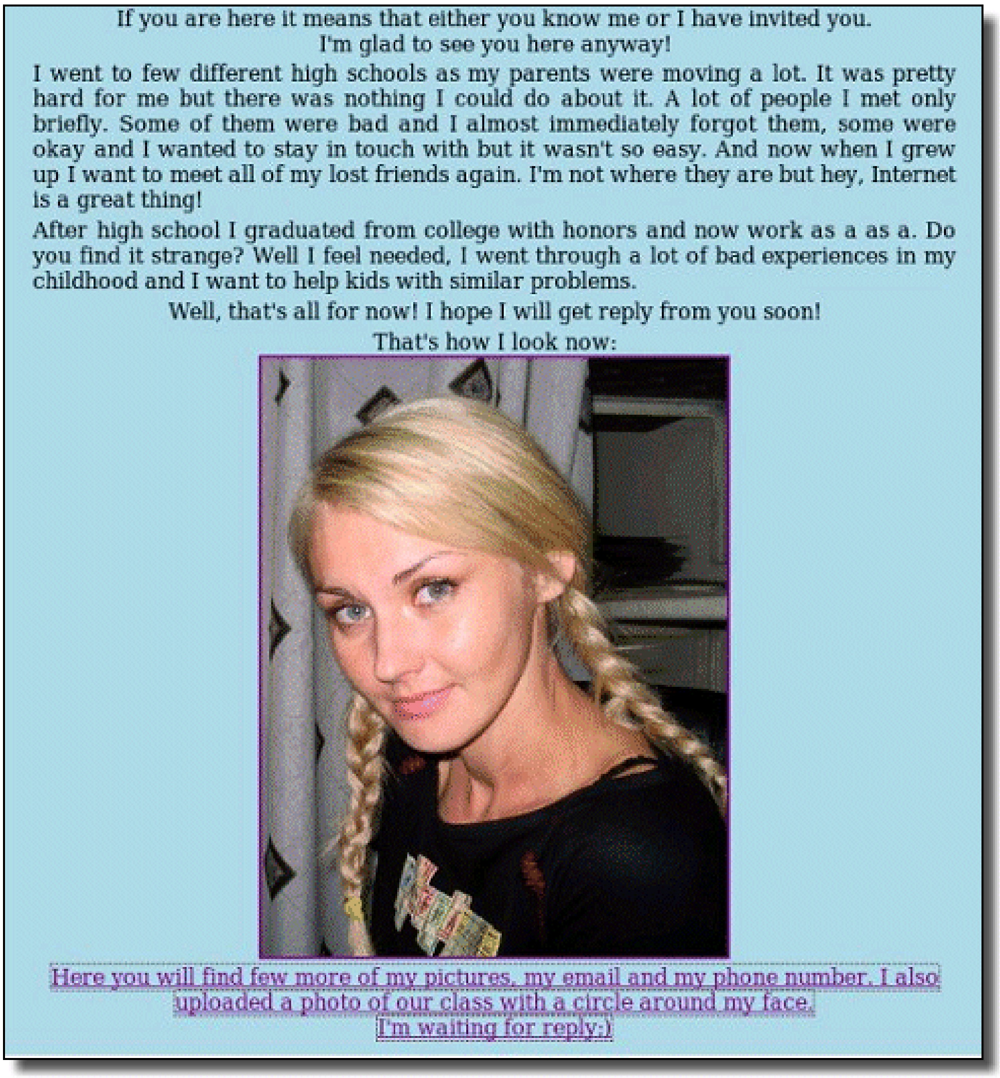
33. Other forms of attack involve some type of attempted social engineering such as the request to help move a large sum of money from a war torn country for which you will get a percentage but you

need to send the details of your bank account first!. Some of these latter attempts are very clumsy and quite obvious but despite that people still get taken in and lose money.

34. More invidious for the public figure is the rather more subtle attempt at entrapment where no money is mentioned – at least at first. Of note here are the emails supposedly coming from individuals who claim to have been let down in arrangements to enter the UK and are seeking assistance. Here the risk to your reputation in addition to your money.

35. We also see similar methods used to download spyware to a victim's computer. This starts with an email invitation to visit a social networking site or a personal website. Once on the site spyware and viruses are automatically downloaded to our computer.

Fig 7 – Social Engineering – Website loaded spyware



If you are here it means that either you know me or I have invited you.
I'm glad to see you here anyway!

I went to few different high schools as my parents were moving a lot. It was pretty hard for me but there was nothing I could do about it. A lot of people I met only briefly. Some of them were bad and I almost immediately forgot them, some were okay and I wanted to stay in touch with but it wasn't so easy. And now when I grew up I want to meet all of my lost friends again. I'm not where they are but hey, Internet is a great thing!

After high school I graduated from college with honors and now work as a as a. Do you find it strange? Well I feel needed, I went through a lot of bad experiences in my childhood and I want to help kids with similar problems.

Well, that's all for now! I hope I will get reply from you soon!
That's how I look now:

Here you will find few more of my pictures, my email and my phone number. I also uploaded a photo of our class with a circle around my face.
I'm waiting for reply:)

36. Always ensure you have up-to-date anti-virus and anti-spyware software installed. If your Council supplied equipment starts to act

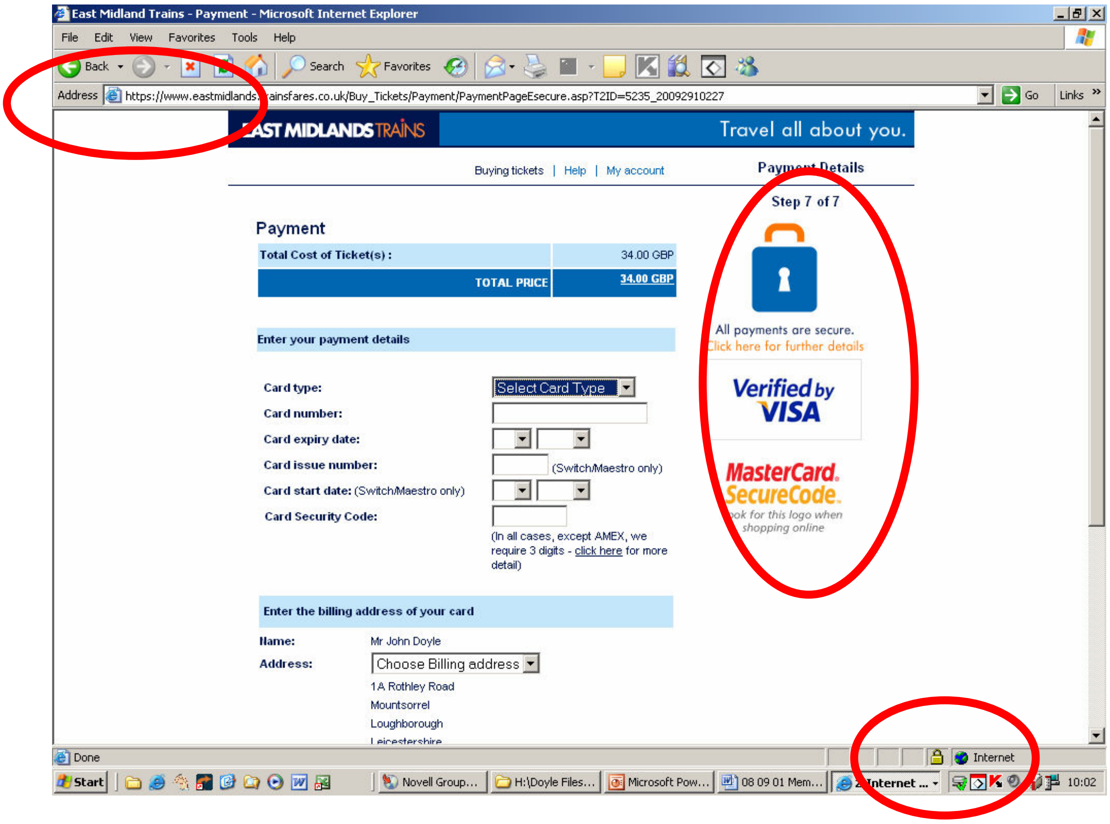
oddly report it to ict.support.centre@leicester.gov.uk or Tel: 0116 252 88888.

Preventing On-Line Fraud

37. Be aware that your card details are as valuable as cash in the wrong hands so store your cards securely at all times and try not to let them out of your sight. Only shop at secure web sites and before submitting card details ensure that the locked padlock or unbroken key symbol is showing and the retailer's internet address has changed from 'http' to 'https. By sticking to these simple rules you minimise the chances of your details being obtained by fraudsters.

38. Sign up to *Verified by Visa* or *MasterCard SecureCode* whenever you are given the option whilst shopping online. This involves you registering a password with your card company. By signing up, your card will have an additional level of security that will help prevent you from being a victim of online fraud.

Fig 8 Secured on – line Shopping Site



East Midland Trains - Payment - Microsoft Internet Explorer

Address https://www.eastmidlandstrainsfares.co.uk/Buy_Tickets/Payment/PaymentPageEsecure.asp?T2ID=5235_20092910227

EAST MIDLANDS TRAINS Travel all about you.

Buying tickets | Help | My account   Payment Details

Step 7 of 7

Payment

Total Cost of Ticket(s) :	34.00 GBP
TOTAL PRICE	34.00 GBP

Enter your payment details

Card type: Select Card Type
Card number:
Card expiry date:
Card issue number: (Switch/Maestro only)
Card start date: (Switch/Maestro only)
Card Security Code:
(In all cases, except AMEX, we require 3 digits - click here for more detail)

All payments are secure.
Click here for further details

Verified by VISA

MasterCard. SecureCode. Look for this logo when shopping online

Enter the billing address of your card

Name: Mr John Doyle
Address: Choose Billing address
1A Rothley Road
Mountsorrel
Loughborough
Leicestershire

39. Other points to note are:

- Always be suspicious of emails which are supposedly from your bank.
- Never give your login details in full by email or over the phone – your bank will never request these in this way.
- Never disclose your card PIN to anyone and never send it over the internet.

- Print out your order and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number).
- Consider using a separate credit card specifically for online transactions.
- Shred paperwork – both LCC related and personal
- Inform your Bank, Building Society and the DVLA when you change address, use Royal mail redirect to ensure your mail is redirected
- Report all phishing emails to reports@banksafeonline.org.uk .

Check Your Credit Report

40. A good indicator that something is amiss is unusual activity being shown up on your personal Credit Rating and you should monitor this through one of the Credit Rating companies. Contact Equifax, Experian, or CallerCredit for a personal report, these cost approximately £2. Consider registering with CIFAS for protective registration so that any credit requests in your name are automatically double checked

Social Networking and Personal Video Sites

41. Social networking and personal video sites is the most difficult area to do anything about when things go wrong and they are being used to mount abusive attacks upon you. There so many different sites, many not hosted here in the UK that could be used. Many are unreceptive to complaints, whilst others may find it difficult to judge where "free speech" becomes abuse. Dependable advice on the whole arena of Social Networking can be found on the Get Safe On Line website at http://www.getsafeonline.org/nqcontent.cfm?a_id=1459

42. Most, such as the widely used site for video clips, YouTube, do have clear guidance in their Terms of Use and Community Guidelines but getting action still may not be easy.

43. Your primary defence in preventing abuse through the use of sites such as YouTube is by limiting exploitable information about you being published on the Internet.

44. Many individuals use Social Networking sites, such as FaceBook, Bebo or Myspace, with great success, but there is always a risk, the golden rule is "*Think before you publish*". All these sites try to be responsible in their delivery of services and offer advice on how to use their sites safely. Do follow that advice.

45. In a similar vein some individuals use on-line dating services such as Match.com and DatingDirect.com. Again most operate responsibly and set out clear guidance for users to protect themselves. As with using Social Networking sites do follow the advice.

Basics for the safe use of Social Networking Sites

46. Remember that despite the Terms of Use for any social networking site the effectiveness of access controls and password strengths on several sites is questionable and several sites used by “personalities” have been hacked and defaced. Some basic guidelines that will help minimise your risk are:

- Fully understand the Terms of Use for the site
- Always use a strong (8 upper and lower case characters including numbers and punctuation marks)
- Set the privacy settings
- Think through what you are going to publish.
- Limit the detail and the amount of personal information – dates of birth, addresses, phone numbers, email addresses, bank details.
- Set up a separate email account that does not use your real name and use it to register and receive mail from the site (avoid any service that requires too much personal information for registration)
- Be very selective in accepting “friends” on the site
- Beware of revealing your personal schedule such as when you are away on holiday
- Be wary of 3rd Party applications available through social network sites – many of these contain viruses and spyware.
- Be wary of geographical networks – even if you have set your privacy settings to ensure that only “friends” can view your profile joining a network permits access to everyone else in that network and you will need to reset your privacy settings.

Personal Protection

47. If things really start going wrong remember contact the Police and follow their advice but there are some simple first steps though:

- When out and about - Take a mobile telephone with you
- Carry a personal attack alarm and learn how to use it
- Do not carry anything that is meant for use as a weapon.
- Try to alter your daily routines, ask friends to go with you whenever possible,
- Always try to let someone know what your plans are.

Help the Police to Help You

48. If you are subject to abuse or you suspect stalking:

- Keep a record of what happened, where, when every time you were followed, phoned, received post or e-mail. The more details you have the better, how the offender looked or sounded, what they were wearing, the make, and number plate or colour of their car.
- Keep letters, and parcels as evidence: even if they contain frightening or upsetting messages, do not throw them away and handle them as little as possible.

- Keep copies of e-mails on disk and print out hard copies, do not delete the original.
- Making notes in a diary is a good idea. Write the information down as soon as possible, when events are still fresh in your mind.
- If you recognise the handwriting, you can keep letters or parcels as evidence without having to open them.
- Make sure you keep any stored messages (including text messages) or telephone numbers that you have received on your mobile phone and caller ID units.
- Tell your friends, neighbours and work colleagues about what is happening.
- Try to get photographic or video evidence of your stalker (especially if they are someone already warned by the police not to come near you).

49. Avoiding Unwanted Telephone Calls

- Answer the phone by saying 'hello', not your name or number.
- Try to keep calm and not show emotion, many callers will give up if they don't think they're making an impression on you or your feelings.
- Use an answer machine to screen out calls and only talk to people you want to.
- If the caller rings again, put the handset down on a table for a few minutes - the caller will think you're listening. After a few minutes replace the handset, you do not have to listen to what the caller has to say.
- Register for the Telephone Preference Service (TPS), this will screen out at least the unwanted sales related calls both for landline and mobile phones. There is also a FAX preference Service for those who use FAX. A recent development is the SilentGuard service to limit as far as possible automated silent calls.

50. If you know or find out who is stalking you

- Do not confront your stalker or even engage them in conversation.
- Do not, under any circumstances, agree to a meeting to talk about how you feel about them constantly bothering you.
- Do not respond in any way to calls, letters, or conversations. If you ignore the phone nine times and pick it up on the tenth, you will send the message that persistence pays. Once they have your attention, they will be encouraged to carry on.

Further Information

www.bankingcode.org.uk – a body that ensures that banks and building societies comply with the standards detailed in *The Banking Code* and *The Business Banking Code*.

www.banksafeonline.org.uk – assistance for internet users to help them protect themselves from online scams and threats such as phishing.

www.callcredit.co.uk – a credit reference agency with a range of information services for businesses and individuals. (Tel: 0870 060 1414).

www.cardwatch.org.uk – information about how card fraud takes place in the UK, what is being done to prevent it and how you can help prevent yourself from becoming a victim.

www.chipandpin.co.uk – archive information, guidance and downloadable materials about chip and PIN.

www.cifas.org.uk – the UK's fraud prevention service, which enables its members to share information on fraudulent activity to help identify and prevent fraud taking place, including on card accounts.

www.consumerdirect.gov.uk – clear and practical help and advice for consumers in Great Britain.

www.equifax.co.uk – a credit reference agency that provides information to businesses, consumers and the public sector. (Tel: 0870 010 0583).

www.experian.co.uk **–** a credit reference agency that helps consumers, businesses and the public sector manage their credit information. (Tel: 0870 241 6212).

www.financial-ombudsman.org.uk – an independent service for resolving disputes between consumers and financial firms.

www.getsafeonline.org – a Government and leading business-sponsored site that provides advice on how to protect your computer and use the internet with safety.

www.identitytheft.org.uk – how to help protect yourself from identity theft, what to do if it happens to you and suggestions on where to get further help.

http://www.leics.police.uk/advice/3_crime_reduction/ **-** Leicestershire Constabulary advice on a whole series of crime reduction topics

www.mastercard.com/uk/personal/en/cardholderservices/index.html – details of how to sign up and benefit from extra protection when shopping online with a MasterCard.

www.oft.gov.uk – provides information and advice for consumers about your rights when shopping, scams to avoid and where to go for help and assistance.

www.shopsafeonline.org.uk – information for businesses and cardholders about *Mastercard SecureCode* and *Verified by Visa*; what they are and how they work.

www.visaeurope.com/personal/onlineshopping/main.jsp – details of how to sign up and benefit from extra protection when shopping online with a Visa card.

http://www.tpsonline.org.uk/tps/ - the telephone and fax preference services, registration will limit unwanted telemarketing calls.