The Fraud
Advisory
Panel

the fraud
advisory
panel

Have you been scammed? Identifying Internet and Email Scams

HAVE YOU BEEN SCAMMED?

Identifying Internet and Email Scams

1. Introduction

The enormous growth of the Internet has resulted in a rising number of website domain name registrations by businesses and organisations hoping to profit by expanding into e-commerce. This rise has been coupled with increasing levels of Internet fraud and misuse.

One particular problem for businesses is that of copycat and ambiguous domain names and websites. Web pages may be copied in order to dupe customers into dealing with less reputable businesses or to direct/divert consumers to illicit sites that might otherwise have been overlooked or avoided. Alternatively, fake websites may be created in order to defraud consumers or other businesses. The practice of creating a fake website in order to dupe consumers is known as "spoofing". There are a variety of different scams involving spoofing.

This paper is designed to give businesses and individuals a brief guide to identifying Internet and email scams, including:

- Phishing
- Cybersquatting and other forms of spoof websites
- Hoax emails

2. Phishing

2.1 What is "phishing"?

Phishing is a relatively new term used to describe attempts to trick people into disclosing personal, financial or security information to replica websites operated by fraudsters. This is an example of a "social engineering" attack where a trusted organisation's identity is used to add credibility to the scam in order to persuade people to carry out actions which they would not have done, had they known the true identity of the perpetrators. In this way, the attack is directed at customers of a particular organisation, rather than at the organisation itself. Numerous companies operating on the Internet have been "targeted" by phishing attacks, including banks, Internet retailers, auction websites and government departments.

"Phishing" is a play on the word "fishing" (ie. fishing for information) and originates from 1996 when people set up replica AOL websites to gather screen names and passwords to get free online access. Such access details were known as "phish" by the community. Phishing typically relies on mass distribution of spam emails at random, with the aim of reaching as many live email addresses as possible belonging to customers of the organisation being targeted. Email addresses are obtained by a variety of means including commercially available address lists, harvesting them from websites and news groups and semi-random generation.

Phishing scams normally involve the fraudster sending bulk email messages purportedly from a bank or other well-known company operating on the Internet. The email will typically use an excuse to request that recipients confirm account and security information and redirect the recipient to a bogus but realistic website via a link contained in the email message. Excuses can include a security breach or some other urgent event at the company, although some messages have themselves purported to be scam warnings or marketing offers, so customers have to be wary of any unsolicited email requesting that they click on a link to go to a website. Security details entered into the bogus website can then be used by the fraudster to access the victim's account. Often, the fraudster will transfer money to accounts under their control in a laundering process, so that they may benefit from the proceeds of their fraud.

In some cases the internet browser programs allow the true source of the bogus website to be disguised from the user and the victim is therefore unaware of the deception until sometime later when funds have been transferred out of the account. For example a link which appears to read **www.abcbank.co.uk/securitycheck** may redirect the victim to a completely different part of the Internet that has nothing to do with ABC Bank.

A search on Ebay will reveal that lists of millions of email addresses are for sale for a few pounds. At the time of writing, several sellers on Ebay are offering *"100,000,000 Email addresses for all your marketing needs"* for £9.99. With very large email lists readily available, the fraudster is able to cast the net very widely and very cheaply and it only needs a small percentage of people to be taken in by the scam to make it very profitable for the fraudster.

Phishing is unique in that it combines the economies of scale of spam and the shortcomings of some Internet browsers to work a simple but serious deception. Phishing can also be very difficult to prosecute as the fraudster may be located in any country and the local legal system may not be sufficiently developed to enable the crime to be prosecuted. The majority of phishing emails are sent through open email proxies, or compromised home computers controlled by spammers, making it extremely difficult to trace the true originators. As a result phishing can be very appealing to a potential fraudster.

Many Internet Service Providers ("ISPs") block such spam emails, however there are certain ISPs in lesser-developed countries which choose to turn a blind eye to the process. In certain cases the fraudster and ISP may have common ownership as a part of a larger criminal enterprise.

The quality of phishing emails is variable. Some are very convincing and are almost indistinguishable from a bona fide email from the company being impersonated. Others suffer from poor English grammar or spelling which may indicate that the scam is being operated from outside the UK. However, as the fraudsters become more experienced at their craft, this leads to increasingly convincing and sophisticated phishing schemes.

Many phishing scams are thought to be operated by organised criminals located in Eastern Europe. The proceeds of phishing may be used to fund further crimes such as people and drug trafficking, prostitution and perhaps terrorism.

In the event that the phishers have managed to obtain Internet banking security details, they need a method of obtaining the money, as it is not possible to transfer the money directly overseas. To help with this process, fraudsters recruit people to receive funds into their own bank account and send them on via a wire transfer service in return for a small commission (normally 7–10%). These “money transfer agents” or “mules” are recruited via fake job offers sent by spam email, adverts on genuine recruitment websites, ICQ (instant messaging), as well as adverts appearing in broadsheet newspapers. Positions on offer include sales representatives, finance managers, mail forwarders and numerous other “work from home” opportunities. These mules are also used to forward goods purchased from e-commerce websites using stolen credit cards as well as funds obtained through bonus auctions.

As the money received in commission payments is the proceed of fraud, it will be confiscated by the bank. Individuals who provide personal information in support of a fake job offer put themselves at risk of identity fraud, as well as having their accounts closed by the bank and becoming embroiled in a police investigation.

2.2 What is Being Done About It?

The major banks, credit card companies, Internet companies and law enforcement agencies are acutely aware of the problem and are working with ISPs to combat the problem. As soon as an ISP becomes aware of a phishing scam it will notify the company concerned so that it can take appropriate action. This may involve sending an email warning to all its customers. Action will also be taken to disable the bogus website. However, this may take some time if the website is hosted in a lesser well-developed country.

The UK has a dedicated law enforcement agency, the National High Tech Crime Unit (“NHTCU”) tasked with policing serious and organised computer crime and other uses of the internet for criminal purposes.

2.3 What Can You Do?

i. Individuals

There are a number of steps that individuals can take to minimise the risk of becoming a victim of a phishing scam:

(a) **NEVER** divulge your security information to anyone requesting it by email or phone.

If you do receive an email which you suspect to be a phishing scam, do not reply to it or click on the link to view the website. If you are concerned about the message, inform the company by calling a publicly listed telephone number, or by forwarding the email (preferably as an attachment including header information) to the dedicated address given on their website. Remember, the safest way to access the company's website (where there may be a warming about this particular scam) is to type the address yourself into your web-browser rather than clicking on the link.

(b) Use **DIFFERENT** passwords for different accounts.

Be very protective over all your passwords and use different passwords for different banking or credit accounts and email services.

Once a fraudster has your password he or she may then try to hack into your email account using that password to find out more information about you. Your email account contains much information about you and the fraudster could use this information to impersonate you. For example, the fraudster may apply for credit online or use your identity to open new accounts in your name.

If your "Inbox" or "Sent Items" contains emails to or from banks then expect the fraudster to try to gain access to these accounts. This "snowball" effect can be the result of divulging one password to the fraudster.

(c) Use **IMAGINATIVE** passwords containing numbers and other characters wherever possible.

One recent survey[1] has found that as a result of having too many passwords to remember, many internet users tend to use one easy to remember password such as the name of a spouse, children, favourite football team and/or pet for all their accounts.

To make a password more difficult for a fraudster to crack insert random numbers and characters. For example, the password "johnsmith" at an account with ABC Bank could be made more difficult to crack by inserting "abc" at the beginning of the password and using numbers and other characters with a password of "abcj0hn$m1th". To make the password harder to guess, additional characters should be substituted and added e.g. substituting "!" for "j" and adding an asterisk at the beginning and end giving a password of "*abc!0hn$m1th*".

If a fraudster is unable to access your account within a reasonable period of time it is possible that he or she will move on to a different victim.

(d) Use up-to-date **ANTI-VIRUS** software and a personal firewall.

If you are using Windows XP, activate the Internet connection firewall which is

[1] BBC News Online (20 April 2004) *Passwords Revealed by Sweet Deal*. Retrieved on 4 June 2004 from http://www.telehealth.net/subscribe/newslettr4a.html1. The survey was undertaken for the Infosecurity Europe Trade Show held during April 2004 in London.

included in the operating system. Be cautious of any unsolicited emails from unknown senders and do not download unexpected or suspicious attachments.

Victims of phishing scams may also have their computers infected with a virus which downloads a program called a "Trojan" (as in Trojan Horse) which can log their internet activity and monitor keystrokes. The Trojan will then send an activity report to the fraudster and this information will be used to access online accounts and defraud the victim.

(e) **NEVER** follow a link to your Internet bank from an email or unreliable 3rd party source.

Links can often take victims to bogus websites. If you want to access your bank's website then type the bank's website address directly into your browser.

Top Tips for Banking Online[2]

Know who you are dealing with. Always access Internet accounts by typing the address into your web browser. Never go to a website from a link in an email and enter personal details. If in doubt, contact the company separately on an advertised number.

Keep passwords and PINS safe. Always be wary of unsolicited emails or calls asking you to disclose any personal details or card numbers. Keep this information secret. Be wary of disclosing any personal information to someone you don't know. Your bank and the police would never contact you to ask you to disclose PINs or all your password information

Keep hold of your cash! Don't be conned by convincing emails offering you the chance to make some easy money. If it looks too good to be true, it probably is! Be especially wary of unsolicited emails from outside the UK – it will be much harder to prove they are who they say they are.

Keep your PC secure. Use up-to-date anti-virus software and a personal firewall and, if your computer uses the Microsoft Windows operating system, keep it updating from the Microsoft website. Be extra careful if using Internet cafes or any PC which is not your own and over which you have no control.

Check your bank's website. If in doubt, a good place to get help and guidance on how to stay safe online is your bank's website. Check regularly for specific information and guidance on protecting your PC and yourself online.

Check your statement. If you notice anything irregular on your account contact your bank immediately.

Additional protective measures

- Always remember your password and other security information and destroy the notice as soon as you receive it

[2] Top tips are a joint initiative by the Association of Payment Clearing Systems (APACS), National Hi-Tech Crime Unit (NHTCU) and the British Bankers' Association (BBA).

- Never write down or record your password or other security information. Make sure that you always read your Terms and Conditions
- Always take reasonable steps to keep your password and other security information secret at all times
- If you change your password, choose one which cannot be easily guessed
- Never give your account details or security information to anyone. If phoning a company, be aware that they will probably not ask for your password in full
- Ensure that there is a locked padlock or unbroken key in the bottom right of your browser window before entering any information. The website address will change from “http” to “https” when a secure connection is made
- Never leave your computer unattended when logged in to Internet Banking
- Ensure that you log-out properly when you have finished banking online

ii. Businesses

There are a number of steps that businesses offering online services can take to minimise the risk of their customers becoming victims of phishing scams:

(a) Adopt policies which do not require their customers to provide security information in response to email communication.

Businesses should also make their customers aware of phishing by placing notices in the “login” section of their websites. The notice should make the company’s email customer communication policy clear and stress that customers must never give security information to any party no matter how bona fide it appears. Businesses should consider setting up hotlines to enable customers to report suspected phishing.

(b) Be vigilant of domain name registrations that are set up to impersonate your business. For example the domain name **www.abcsecurity.com** may purport to be the security section of ABC Bank and could be used as part of a phishing or other scam to defraud ABC’s customers. Specialist Internet search agencies exist which can inform businesses of domain names that have been registered and are similar to their own.

(c) Review your password policy and allow customers to use as many different characters as possible.

(d) Encourage the use of imaginative passwords by customers. This could be highlighted during the customer registration process.

(e) Remind customers to use up to date anti-virus and firewall software at every opportunity.

3. Cybersquatting and Other Types of Spoof Websites

3.1 What is "Cybersquatting"?

One of the most common types of spoofing is cybersquatting. Cybersquatting is the use of copycat and ambiguous domain names similar to a well-known brand to attract customers to a website or to commit fraud. Cybersquatters also carry out the practice of registering a domain name in order to enable them to charge a genuine business an inordinate sum to buy it back.

One famous example of cybersquatting is the website www.whitehouse.com. The staff of the White House maintain a US government information website with links to government services and programs at a site called **www.whitehouse.gov**. However there is also a **www.whitehouse.com**, which is an adult entertainment site that declares "our candidates are better looking and probably know more about the economy too!"

In another case, a fake website was created on the basis of the official World Trade Organisation website which was graphically the same but with different content. For example, the home page announced that the Opening Ceremony of the Third WTO Ministerial Conference had been "suddenly cancelled". The cybersquatters even placed an alert message lower on the page about a "fake WTO website misleading public", with a hyperlink to the original WTO website. The URL, **http://www.gatt.org**, was carefully chosen with obvious reference to the previous name of the WTO (the official website address is **http://www.wto.org**).

However, not all cybersquatting is so harmless. Indeed many cybersquatting websites are used to commit fraud. For example, in 2003, a site called **www.barclaysprivate.com** was shut down having been used as part of a wide-ranging fraud, as was **www.eurocitibank.com** which had nothing to do with Citibank. The sites were used to show the intended victims that the promised millions had been deposited in an account that appeared to be held at a legitimate bank. In many cases, the victims were asked to fill in an online application form with their personal details, including the numbers of their real bank accounts and credit cards.

Another cybersquatting practice involves people registering domain names similar to famous brands in the hope that they can then sell the domain name to the real business for a large profit. In the PC World case, a company called PC World Direct Limited registered the domain name "pcworlddirect.co.uk". However, the company was nothing to do with the Dixons Group which owns the well-known chain of computer shops. Dixons wrote a letter to PC World Direct Limited asking them to transfer the domain name. PC World Direct Limited responded with an offer to sell the name for £300,000. Dixons rejected the offer and had to start legal proceedings to recover the name.

3.2 What is the Difference Between Phishing and Cybersquatting?

Phishing and cybersquatting are closely related but there are key differences. Phishers use a fake website and a spam email to entice customers to a website to give sensitive personal data. It is always fraudulent. Cybersquatters use a website with a very similar domain name to attract customers using the goodwill of another business. Customers are not necessarily requested to provide sensitive personal information and the practice is not necessarily fraudulent.

3.3 Other Examples of Spoof Websites

Another method of spoofing is where a person or business pretends to be someone else for the purposes of making money out of the Internet. It is not just the impersonation of a well-known brand's website or domain name. Examples of spoofing include using a website to market a fake business or to encourage victims to invest in a business that does not exist. A bogus Internet banking site can be set up offshore, attract funds and be dismantled overnight.

In one case of spoofing, a website was used to mislead investors into believing they could join the same group of capitalists who provided the original capital for Microsoft and Intel. The investors were invited to buy unregistered securities in companies formed to purchase and operate franchises that would sell and support software for operating commercial websites. It is unknown how many investors were tricked before the fraud was closed down.

In another case, a website was established asking people to invest in a high-tech start up company which was a scam. However, it attracted nearly 100,000 people to its website. Although only 3,000 of these people subsequently sent emails requesting further details, 150 of them were sufficiently convinced to send in money netting the fraudsters $190,000.

3.4 What Can You Do?

i. Individuals

Cybersquatting

Do:

- Use a search engine if you are unsure about the exact address of a website. If several similar addresses appear, take extra care
- Contact a business and ask for their website address if you are unsure about its website address
- Regularly check the websites that you use to see if there has been any change of format. It may also tell you if there are any spoof websites attacking its customers.
- Check your bank statements and other records immediately. This will allow you find out quickly if any fraud has been committed
- Contact the real business immediately if you find a fake website

Do not:

- Assume that because a website has a similar name, it belongs to the real business
- Assume that because a website looks similar to the real website, it belongs to the real business
- Submit sensitive personal information to a website unless you are certain that it is legitimate
- Use the same password for all sites

Spoofing

Do:

- Thoroughly check the identity of any business on the web
- Contact Trading Standards or the FSA to see if there have been any complaints if the company appears to be making unrealistic promises
- Seek immediate legal help if you think you have been defrauded

Do not:

- Sign up for any scheme which appears to offer massive returns. If it looks too good to be true it probably is.
- Assume that a website is legitimate because it has ".com" or ".co.uk"
- Delay seeking help in the hope that it will all work out

ii. Businesses

Businesses who are victims of cybersquatters have the following options:

- Refer the matter to the criminal authorities
- start an arbitration to recover the domain name
- bring a civil action against the cybersquatters for damages

(a) Arbitration

If the dispute relates to a top level domain name (including ".com" and ".net"), Domain-name owners and trademark holders can file a complaint through the Uniform Dispute Resolution Policy (UDRP) adopted by the Internet Corporation for Assigned Names and Numbers (ICANN), This is a quick (30-60 days), cheap (under $1,000) arbitration proceeding where three elements need to be established:

- that the domain name is identical or confusingly similar to a trademark or service mark
- that the registrant has no rights or legitimate interest in the domain names
- that the domain name has been registered and is being used in bad faith

The UDRP is effective for all ICANN-accredited registrars of Internet domain names. Money damages are not available through UDRP, only a transfer of name, and the defendant must be actually using the name. Importantly, UDRP is not suitable for cases where injunctions are required. Therefore the procedure is of limited use where fraud is being committed.

Uniform Dispute Resolution Policy

In the case of Thomas Cook Holdings Limited v Vacation Travel (WIPO D2000-1716), the WIPO panel decided that the domain name "jmcflights.com" was confusingly similar to the JMC trademark and had been registered in bad faith for commercial gain.

Vacation Travel was a travel agent which opened a website under the jmcflights.com domain name to offer flights and holidays, identifying themselves as retail agents for JMC and with connectors to Flight Search and ABTA flights facilities to enable them to check JMC flights and others. The respondent also registered the domain name abtaflights.com and abtaflights.co.uk and opened the former as a website to invite visitors to book their flights. The home page of that site featured logos of a number of well-known holiday travel organisations including JMC.

In the United Kingdom the domain name registry, Nominet, provides a dispute resolution service whereby the disputing parties are encouraged to achieve a mediated resolution. If an agreement is reached it will create a contract enforceable in law. If no agreement is reached, the parties can submit to arbitration under the Nominet UK Dispute Resolution Service (DRS) or seek recourse through the courts.

To succeed in DRS arbitration, two elements need to be established:

- the domain name is similar to the claimant's brand or trade mark or other intellectual property rights
- the domain name was registered or is being used in bad faith

Nominet UK Dispute Resolution Service

In the Froogle case, a United Kingdom web-hosting company registered "Froogle.co.uk" days after Google launched a product search service under the same name. Google contacted the web hosting company and offered £1,500 for the domain name but this was refused. Google then started DRS arbitration.

The DRS panel held that Google did have sufficient intellectual property rights in the word "Froogle" to force the name to be transferred. The panel noted that it was not necessary for Google to have enough intellectual property rights to start an action for passing-off or breach of copyright. It was not even necessary for the intellectual property rights to be in the United Kingdom. The panel therefore ordered the transfer of the name.

(b) Litigation

As yet there is no specific "anti-cybersquatting" legislation in the United Kingdom. However, there is the tort of "passing off". This tort is used to stop one person exploiting another's business reputation and has been applied by the English courts in a number of domain name cases. To establish liability under the tort of passing off the following elements must be present:

- A reputation or goodwill acquired by a claimant in his goods, name, mark etc
- A misrepresentation by the defendant leading to confusion or deception
- Damage to the claimant

Although trademark owners and companies are protected by the courts up to a point, litigation can take months and sometimes years to resolve and can cost thousands. However, injunctions can be sought and this makes it more useful where fraud is involved.

Litigation

In Britannia Building Society v Prangley & Ors, the defendant had registered the domain name "britanniabuildingsociety.com". The court held that there was no doubt that Prangley & Ors registered the domain name whilst having regard to the fact that it represented Britannia Building Society and was a commercially viable instrument. It was plain that any use of the domain name in this country would lead to a serious risk of confusion that the registered owner of it was connected to Britannia and that the domain name was to be used for fraudulent gains.

4. Hoax Emails[3]

4.1 What are Hoax Emails?

Anyone who has an email account will be only too aware of the email that arrives giving dire warnings of some software weakness or virus which, if action is not taken at once, will destroy computer files or infect computer programmes. Although some of these emails are genuine, others, and increasingly the majority, are hoaxes designed to scare the computer user or encourage them to circulate the warning to all of their friends and family thus perpetrating the hoax to an even wider audience.

Such hoaxes do not restrict themselves to computer issues. They may include warnings of children at risk, offers of free holidays, money, and the good old chain letter which if sent on gives the sender good luck and fortune for the rest of their lives!

Chain letters and most hoax messages follow a similar pattern and have three recognisable parts:

[3] This section has been prepared with assistance from Lawrence Livermore National Laboratory sponsors of http://hoaxbusters.ciac.org/

- A Hook
- A Threat
- A Request

(a) The Hook

First, there is a hook, to catch your interest and get you to read the rest of the letter. Hooks used to be *"Make Money Fast"* or *"Get Rich"* or similar statements related to making money for little or no work. Electronic chain letters also use the "free money" type of hooks, but have added hooks like *"Danger!"* and *"Virus Alert"* or *"A Little Girl Is Dying"*. These tie into our fear for the survival of our computers or into our sympathy for some poor unfortunate person.

(b) The Threat

When you are hooked, you read on to the threat. Most threats used to warn you about the terrible things that will happen if you do not maintain the chain. However, others play on greed or sympathy to get you to pass the letter on. The threat often contains official or technical sounding language to get you to believe it is real.

(c) The Request

Finally the request, some older chain letters ask you to mail a sum of money to the top ten names on the letter and then pass it on. The electronic ones simply admonish you to *"Distribute this letter to as many people as possible"*. They never mention clogging the Internet or the fact that the message is a fake, they only want you to pass it on to others.

4.2 Why People Send Chain Letters and Hoax Messages

The only person who knows the real reason for sending a chain letter or hoax email is the original author. However some possible reasons are:

- To see how far a letter will go
- To harass another person (include an email address and ask everyone to send mail, e.g. Jessica Mydek)
- To extract money out of people using a pyramid scheme
- To kill some other chain letter (e.g. Make Money Fast)
- To damage a person's or organisation's reputation

4.3 What Can You Do?

Because there is such a wide variance of these types of emails sorting the good from the bad might at first appear difficult if not impossible. However, this is not the case and there are a number of actions that recipients of such emails can take to ensure that they do not become part of the hoax or scam.

The first thing you should do if you receive such an email is not to panic. Look at the email and its contents and ask yourself *"why it has come to my email box?"* If the email is from someone you don't know then there is every chance it falls in the hoax or scam category. If it is from someone you do know it does not make it automatically true. You need to apply some basic analysis to the content first.

i. Hoax Emails

(a) Check whether the email contains a request to *"send this to everyone you know"* or a variant of this statement. This should raise a red flag that the warning is probably a hoax. No real warning message from a credible source will tell you to onsend it to everyone you know.

(b) Look at what makes a successful hoax. There are two known factors that make a successful hoax:

- Technical sounding language
- Credibility by association

Most people, including technologically savvy individuals, tend to believe warnings that use proper technical jargon. For example, the Good Times hoax says that *"...if the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop which can severely damage the processor...".* The first time you read this it sounds like it might be something real. However with a little research you find that there is no such thing as an nth-complexity infinite binary loop and that processors are designed to run loops for weeks at a time without damage.

Credibility by association refers to the person who sent the warning to you. Even though the person sending the warning may not know what he is talking about the prestige of the company backs the warning and makes it appear real.

For example, if the janitor at a large technological company sent a warning to someone outside of that company, it is likely that the recipient would tend to believe the warning because the company should know about those things. If a manager at the company sends the warning the message is doubly backed by the company's and the manager's reputations.

Technical sounding language and credibility by association make it very difficult to claim a warning is a hoax. This means that you must do your homework to see if the claims are real, and if the person sending out the warning is a real and is someone who would know what they are talking about.

(c) Check the person's website or their company's website to see if the hoax has been responded to there.

It is important to exercise a little caution when verifying the source of a possible hoax email. The apparent author may be a real person who has nothing at all to do with the hoax. If thousands of people start sending them emails asking if the message is real, it will essentially constitute an unintentional denial of service attack on that person – this may have been the author's reason for sending the hoax to begin with.

ii. Chain Letters

When you receive a warning:

(a) Examine its Pretty Good Privacy (PCP)[4] signature to see that it is from a real response team or antivirus organization.

To do this you will need a copy of the PGP software and the public signature of the team that sent the message. The CIAC signature is available at the CIAC home page: **http://ciac.llnl.gov/** You can find the addresses of other response teams by connecting to the FIRST web page at: **http://www.first.org**.

Chain letters usually do not have the name and contact information of the original sender so it is impossible to check on its authenticity. Legitimate warnings and solicitations will always have complete contact information from the person sending the message and will often be signed with a cryptographic signature, such as PGP to assure its authenticity.

(b) Check anti-hoax websites such as http://hoaxbusters.ciac.org/ to see if the warning has already been declared a hoax. Even if there is no warning listed it may just mean that they have not yet seen this particular hoax.

(c) See if the email warning includes the name of the person submitting the original warning.

Many of the newer chain letters contain a person's name and contact information, but that person either does not really exist or does exist but does not have anything to do with the hoax message. If the person does exist do not send them an email message. It is likely that they have nothing to do with this hoax. Instead, check their personal or company website. Often if a person has been the victim of a hoax that hoax message will be debunked on the person's or their company's website.

(d) If you still cannot determine if a message is real or a hoax send it to your computer security manager, your ISP, or your incident response team and let them validate it for you.

When in Doubt, Don't Send It Out

[4] PGP is a public key encryption programme. Originally written by Phil Zimmermann in 1991, later PGP versions have been developed and distributed by MIT, ViaCrypt, PGP Inc., and now Network Associates Inc (NAI). PGP is the de-facto standard for email encryption today with millions of users worldwide.

Example of a Chain Email

The **PENPAL GREETINGS!** hoax shown below appears to be an attempt to kill an email chain letter.

This chain letter is a hoax because it does not execute a virus or any attachments; therefore the Trojan horse must be self-starting. Aside from the fact that a program cannot start itself, the Trojan horse would have to know about every different kind of email program to be able to forward copies of itself to other people.

We have had to modify this statement slightly for the newer html mail readers. If a mail message is formatted with html and contains scripts, those scripts will run when the email message is read. **Active scripting should always be turned off for a mail reader** so that malicious code like the KAK worm cannot automatically run.

Notice the three parts of a chain letter, which are easy to identify in this example.

The Hook

FYI!

Subject: Virus Alert

Importance: High

If anyone receives mail entitled: PENPAL GREETINGS! please delete it WITHOUT reading it. Below is a little explanation of the message, and what it would do to your PC if you were to read the message. If you have any questions or concerns please contact SAF-IA Info Office on 697-5059.

The Threat

This is a warning for all Internet users – there is a dangerous virus propagating across the Internet through an email message entitled

**"PENPAL GREETINGS!" DO NOT
DOWNLOAD ANY MESSAGE ENTITLED "PENPAL GREETINGS!"**

This message appears to be a friendly letter asking you if you are interested in a penpal, but by the time you read this letter, it is too late. The "trojan horse" virus will have already infected the boot sector of your hard drive, destroying all of the data present. It is a self-replicating virus, and once the message is read, it will AUTOMATICALLY forward itself to anyone whose email address is present in YOUR mailbox! This virus will DESTROY your hard drive, and holds the potential to DESTROY the hard drive of anyone whose mail is in your inbox, and who's mail is in their inbox, and so on. If this virus remains unchecked, it has the potential to do a great deal of DAMAGE to computer networks worldwide!!!! Please, delete the message entitled "PENPAL GREETINGS!" as soon as you see it!

The Request

And pass this message along to all of your friends and relatives, and the other readers of the newsgroups and mailing lists which you are on, so that they are not hurt by this dangerous virus!!!!

Hoax Categories[5]

Malicious Code (Virus and Trojan) Warnings
Warnings about Trojans, viruses, and other malicious code that has no basis in fact. The Good Times and other similar warnings are here.

Urban Myths
Warnings and stories about bad things happening to people and animals that never really happened. These are the poodle in the microwave and needles in movie theatre seats variety.

Give-aways
Stories about give-aways by large companies. If you only send this on, some big company will send you a lot of money, clothes, a free vacation, etc., etc. Expect to wait a long time for any of these to pay off.

Inconsequential Warnings
Out of date warnings and warnings about real things that are not really much of a problem.

Sympathy Letters and Requests to Help Someone
Requests for help or sympathy for someone who has had a problem or accident.

Traditional Chain Letters
Traditional chain letters that threaten bad luck if you do not send them on or that request you to send money to the top *nth* people on the list before sending it on.

Threat Chains
Mail that threatens to hurt you, your computer, or someone else if you do not pass on the message.

Scam Chains
Mail messages that appear to be from a legitimate company but that are scams and cons.

Scare Chains
Mail messages that warn you about terrible things that happen to people (especially women).

Jokes
Warning messages that it's hard to imagine that anyone would believe.

True Legends
Real stories and messages that are not hoaxes but are still making the rounds of the Internet.

Hacked History
Real stories where the facts have been adjusted to fit someone's political agenda.

Unknown Origins
Stories that just don't ring true, but cannot be proved.

[5] Computer Incident Advisory Capability Hoaxbusters website (http://hoaxbusters.ciac.org/)

Acknowledgements: The Fraud Advisory Panel would like to thank Steven Philippsohn, Chairman of the Fraud Advisory Panel Cybercrime Working Group and the Fraud Litigation Team at Philippsohn Crawfords Berwald together with Harvey Dyson, June Hale, Alice Rigby, Tom Salmond and Jack Wraith for their assistance in the preparation of this publication.

The information contained in section four (Hoax Emails) of this guide has been reproduced with kind permission from http://hoaxbusters.ciac.org/.

Disclaimer: Whilst every effort has been made in the construction of this Guide, compliance with it does not guarantee that you and/or your business will not be a victim of a hoax, virus or fraud.

The Fraud Advisory Panel and the contributors of this Guide accept no responsibility for any action taken by parties as a result of reading this Guide. Readers should obtain the appropriate professional advice on the issues raised.

Useful Links

Fraud Advisory Panel
www.fraudadvisorypanel.org

Anti-Phishing Working Group (APWG)
www.anti-phishing.org

Association for Payment Clearing Services (APACS)
www.apacs.org.uk

British Bankers' Association
www.bba.org.uk

Card Watch
www.cardwatch.org.uk

CIFAS – the UK'S Fraud Prevention Service
www.cifas.org.uk

City of London Police
www.cityoflondon.police.uk

Crimestoppers
www.crimestoppers.co.uk

Department of Trade & Industry
www.dti.gov.uk

Financial Services Authority
www.fsa.gov.uk

Hoax Busters
http://hoaxbusters.ciac.org

Home Office
www.homeoffice.gov.uk

HM Treasury
www.hm-treasury.gov.uk

Metropolitan Police
www.met.police.uk

MillerSmiles.co.uk
www.millersmiles.co.uk

Microsoft
www.microsoft.com/security/protect

National Criminal Intelligence Service (NCIS)
www.ncis.gov.uk

National Hi-Tech Crime Unit
www.nhtcu.org

National Working Group on Fraud
www.uk-fraud.info

Office of Fair Trading
www.oft.gov.uk

Philippsohn Crawfords Berwald
www.pcblitigation.com

Stay Safe Online
www.staysafeonline.info

The Fraud Advisory Panel
Chartered Accountants' Hall PO Box 433 Moorgate Place London EC2P 2BJ www.fraudadvisorypanel.org

OTHDIG3224 07/04