ANTI-PHISHING AS A WEB-BASED USER SERVICE[1]

Christopher Cranston
Department of Computer and Information Sciences
University of Strathclyde, Glasgow G1 1XH
UK
ccranston@cis.strath.ac.uk

George R S Weir
Department of Computer and Information Sciences
University of Strathclyde, Glasgow G1 1XH
UK
george.weir@cis.strath.ac.uk

ABSTRACT

This paper describes the recent phenomenon of phishing, in which email messages are sent to unwitting recipients in order to elicit personal information and perpetrate identity theft and financial fraud. A variety of existing techniques for addressing this problem are detailed and a novel approach to the provision of phishing advice is introduced. This takes the form of a Web-based user-service to which users may forward suspect email messages for inspection. The Anti-Phishing Web Service rates the suspect email and provides a Web-based report that the submitter may view. This approach promises benefits in the form of added security for the end-user and insight on the factors that are most revealing of phishing attacks.

KEYWORDS

Phishing, spam, email scams.

1. INTRODUCTION

Phishing scams are an increasingly common method of identity theft. They begin with an email message that appears to originate with an established legitimate organization. The email usually asks the recipient to submit personal information on a website. However, the email is fraudulent and has actually been sent with criminal intent. Unfortunately, many email users are unsophisticated in the ways of email and being unable to spot phishing attempts, they innocently follow the instructions contained therein. A consequence of this innocence may be significant financial loss.

This paper describes the nature of phishing scams and the associated problems email users face in identifying phishing emails. In addition, we describe a software solution (the Anti-Phishing Web Service) that aims to assist with the phishing problem.

1.1 Email, spam and scams

The term ‘spam’ commonly refers to unsolicited bulk email. Unsolicited email includes sales and job enquiries specifically addressed to a particular recipient without their prior knowledge or request. Bulk email includes mailing lists and newsletters to which the recipient has subscribed. Spam is the intersection of these email varieties – it is both unsolicited and bulk.

The majority of spam emails advertise products such as computer software or drugs. With negligible cost and effort required to send spam, it now accounts for around 76% of all email messages (Gaudin, 2004).

[1] Presented at the IADIS e-Commerce 2006 conference, Barcelona, Spain, 9-11 December 2006.

Many infrequent email users now find it difficult to locate legitimate email in their mailbox. As a result, the effectiveness of email as a communication medium has been severely reduced.

To combat this growing problem, most Internet Service Providers (ISPs) prohibit the sending of spam from their networks. Some spammers use multiple free ISP accounts to send spam, whereby, if one of these free accounts is terminated, another can be quickly created. Another popular method of despatching spam is through virus infested PCs, usually belonging to unsuspecting home broadband users (Leyden, 2004a). Despite attempts to reduce the problem, the incidence of spam continues to increase.

Many countries, including the UK and the US, have introduced laws to prevent the sending of spam (BBC News, 2003). However, these laws have had little effect, since most spam originates from outside the legislating country. There are also loopholes and inadequacies in these laws. For example, the US Can Spam Act requires individuals to opt-out of spam, rather than opt-in. EU anti-spam laws also have problems, because business email addresses are exempt from the legislation.

Since most legal attempts to address spam have met with limited success, many ISPs and email users now rely heavily on email filters to remove spam. Spam filters perform a series of tests on each incoming email and combine the results to determine whether the message is spam or legitimate. Spam filtering takes place at the mail transfer agent (MTA) or mail user agent (MUA). Popular MTA spam filters include SpamAssassin and Brightmail. Many MUA, such as Eudora and Mozilla Mail, now provide integrated spam filters. Without spam filters and related spam blacklists many users might otherwise simply abandon the use of email.

While the majority of spam emails are advertisements for products, some messages aim to entice the recipient into scams. Common email scams include pyramid schemes that promise very high returns on an initial investment (Wikipedia, 2006a). Unfortunately, such ‘investors’ have no chance of receiving any return on their initial outlay. Perhaps the most popular email scam is the Nigerian money transfer (Wikipedia, 2006b). This scam asks the recipient for help with the transfer of money from a Nigerian bank account, promising a large payment in return. Once entered, the investor is asked for sums of money to help with the fictitious transfer process. Of course, no money transfer is ever received by the unwitting subjects of this criminal operation.

1.2 Phishing

Phishing is a dangerous variety of email scam that is often harder to spot than ‘traditional’ email-based scams. Typically, phishing emails try to trick users into divulging personal information such as bank account details and PIN numbers. Despite being sent by fraudsters, phishing emails appear to originate from an established legitimate enterprise, usually an on-line bank or e-commerce site. The email usually asks the user to proceed to the organization’s website to confirm their personal details, often citing security or maintenance reasons for the request. Invariably, the user is sent to a bogus or spoofed website that is almost indistinguishable from the real website. If the user submits their personal details, the information is then in the hands of organized criminals and this usually results in the defrauding of the user.

This practice is called ‘phishing’ from the analogy between fisherman fishing and fraudsters attempting to snare unsuspecting users (APWG, 2006). It is termed ‘phishing’ rather than ‘fishing’ in the hacker tradition of replacing the letters ‘f’ with ‘ph’. (This echoes the use of ‘phreaking’ to describe the act of bypassing a telephone network's security systems (Telephone Tribute, 2000).

According to the Anti-Phishing Working Group (APWG), there were 1422 unique phishing attacks in June 2004 alone (APWG, 2004). This is up from 116 unique attacks in December 2003, representing an average monthly increase of 52%. Of the 1422 unique attacks in June 2004, 77% were against financial services organizations, 20% were against retailers and 2% were against ISPs. Overall, the most popular targets were US based: Citibank with 492 attacks, eBay with 285 attacks and US Bank with 251 attacks. Each unique phishing attack requires hundreds of thousands of emails to be sent, a fact corroborated when MessageLabs intercepted 125,000 copies of a new phishing attack within 5 hours (Leyden, 2004b). It is clear that phishing attacks are now a prevalent method of Internet fraud.

The amount of money lost to phishing attacks is certainly huge. A recent Gartner report stated that US Banks and credit card issuers lost $1.2 billion in 2003 to this problem (Litan, 2004). This figure was based on 1.78 million Americans (3% of those polled) who admitted providing personal information to a phishing email or web site. Furthermore, Gartner estimate that at least a million more people have unknowingly been defrauded by such schemes. This seems plausible, given a recent study by MailFrontier Inc. that asked 1,000

users to classify emails as phishing attempts or legitimate mail (MailFrontier, 2004). The experiment found that phishing attempts were incorrectly classified as legitimate mail 28% of the time. One particularly effective phishing attempt targeting PayPal was classified as legitimate by 31% of participants. A significant percentage of participants even classified authentic mail as phishing attempts.

1.3 The Phishing Process

Most phishing attacks take four distinct steps toward defrauding unwary recipients: (1) the scam operators set up the phishing website. This website usually imitates an established, legitimate site; (2) using guessed or copied email addresses, the scammers send out emails purporting to come from the legitimate site; (3) the recipient downloads their email and receives the phishing message. The email asks the user to click on a hyperlink and enter personal details on the resulting website. If the user clicks on the hyperlink the phishing site will be displayed. If duped, the user may then enter the requested personal information; (4) the recipient's personal details are now held by the scam operators. The scammers may now assume the identity of the recipient and gain illicit access to funds. These steps are elaborated below.

Step 1: Construct the Phishing Website

The first task is to establish a phishing website. These are simple to set up, requiring little more than an Internet-connected computer serving web pages. The Web pages are usually altered copies of pages belonging to the targeted organisation. Sometimes, the phishing site appears as a pop-up window over the legitimate site. Generally, phishing sites are contrived to appear authentic.

Most phishing sites do not have a domain name and Web links to the site in the phishing email usually take the form of IP addresses, e.g. http://61.71.120.10/citi/index.php. Sometimes phishing sites do use domain names, often cleverly crafted to mimic established sites, e.g. http://www.usbank-secure.biz/. However, registering a domain name entails some financial cost and provides additional information that may be used to track the perpetrators.

Recent analysis by the Anti-Phishing Working Group (APWG) found that most (27%) of phishing sites were hosted in the US (op. cit.). This was closely followed by South Korea with 20% and China with 16%. For comparison, the UK hosted only 1% of phishing sites. The report also estimated that 25% of phishing sites were hosted on hacked computers, without their owners' knowledge. Finally, the report states that on average phishing sites are only live for 2.25 days - the longest noted was a site serving content for 15 days. Sites with a longer lifespan tend to operate from countries where there may be difficulties in closing down sites, where there are different or no Internet crime laws.

Step 2: Write and Send Phishing Emails

Once the phishing site is set-up, the next step is for large numbers of phishing emails to be sent out. For this to be possible the scam operators must collate a large number of email addresses. These are acquired using address harvesting techniques perfected by spammers. Like other spammers, phishing scam operators must accumulate as many email addresses as possible in order to maximize the response rate.

Address harvesting techniques vary, but one popular methods is to use programs that search the web for published email addresses. These programs target Usenet posts, web forums, mailing lists and guest books, since these resources are likely to contain email addresses (Hird, 2002). Another technique is dictionary-based address generation. Finally, rather than collect addresses themselves, phishing scammers may simply purchase a list of addresses from an unscrupulous third party. Regardless of the selected technique, large numbers of addresses are acquired by the scammers. Although many of these addresses will be malformed, duplicates or out-of-date, and many of the valid addresses will belong to individuals who are not customers of the organization being impersonated (and so cannot be defrauded by the scam), this will not deter the scammers, since sending email is of negligible cost. The scammers' concern is simply to maximize the quantity of phishing emails sent.

The content of a phishing email is often carefully crafted. A typical email attempts to alarm the recipient by describing security or maintenance issues at an established legitimate organization. The message will ask the recipient to resolve these issues by confirming personal information on a web page. An embedded hyperlink in the email often provides easy access to the web page. This hyperlink is often disguised to resemble a link to the legitimate website, although it points to the phishing site.

Some emails contain embedded forms for users to enter their personal details. This removes the need for a separate phishing web site. Other phishing emails do not ask for personal details at all, but urge the user to install an attached piece of software. Software offered in this way is usually malicious and may be a virus, worm, Trojan horse or spyware program. Spyware programs are particularly dangerous, as they can intercept and transmit sensitive personal information, without the user's knowledge.

Regardless of whether the goal is to have recipients visit a web page, enter details in a form or install a program, the user must be convinced that the email is authentic. To accomplish this, phishing emails often contain images, slogans or disclaimers taken from the organization being impersonated. Fortunately not all phishing emails look authentic. Many have poor spelling or grammar and may also bear little resemblance to legitimate emails from the genuine organization. Such clues may alert users to the email's true purpose.

When phishing emails are sent out, it is common to spoof the sender's address. Spoofing the sender's address is possible since the current email Simple Mail Transfer Protocol (SMTP) does not validate the purported 'From' address. This loophole allows scammers to send phishing emails that appear to come from legitimate organizations. A recent Anti-Phishing Working Group Report indicates that in June 2004, 92% of phishing emails were sent with a spoofed sender's address. This technique is prevalent as it convinces many recipients that the email is authentic.

Once phishing emails have been written, disguised and addressed, the final step is to send them. This step employs standard spamming techniques, e.g., sending the phishing emails using someone else's mail server. In the past this was easily done through open relays and open proxies. Although these vulnerabilities are now rare, they are still occasionally used to send spam and phishing emails. Todays phishing emails are commonly sent from mail servers or proxies running on virus infected machines. Viruses such as Sobig contain built-in SMTP servers, turning infected machines into unwitting spam senders (Sophos, 2006). This permits the perpetrators to remain hidden, while an estimated 60% of all spam is sent using virus infected machines (Spamhaus, 2003).

Step 3: Deceive the Recipient

This step determines whether the phishing attack succeeds or fails. If the recipient is not a customer or associate of the spoofed organization, the attack will fail. Thereby, any recipient who is not a US Bank customer cannot be defrauded by email asking all US Bank customers to confirm their personal details on a web page. If the recipient is a bank customer, or a member of the organization referred to in the email, they may more easily be convinced to follow the instructions if they are unacquainted with the phishing problem. For this reason, many on-line banking or e-commerce organizations now warn their customers about phishing scams, even to the extent of having phishing tutorials and examples on their websites. Although user education seems to be the best defence against phishing, large amounts of money are still being lost.

The most successful phishing attacks use emails and websites that appear almost identical to their legitimate counterparts. On the other hand, many phishing attacks contain poor spelling and/or grammar, and look dissimilar to email and websites belonging to the legitimate organization.

Step 4: Defraud the Recipient

Once the recipient has submitted personal information on the phishing website, they are easily defrauded. The scam operators can use the identity of the duped users for access to on-line banking or e-commerce accounts.

2. ANTI-PHISHING SOLUTIONS

Of the following solutions, the first two are 'corporate' while the following two are 'end-user' in nature.

1. Digitally Signed Email

Digitally signed emails allow the recipient to verify that the sender information is genuine. This also lets the recipient know that the message has not been modified in transit. These guarantees are extremely useful in the context of phishing, as they prevent individuals from impersonating established organizations in phishing emails. Popular digital signature standards include OpenPGP and S/MIME, although they are incompatible with each other. These facilities can be used with mail clients such as Outlook, Navigator and Eudora.

At first glance, digitally signed emails appear well suited to combating the phishing problem. However, to date very few organizations with on-line banking or e-commerce facilities use this technology. Companies frequently targeted by phishing attacks such as Citibank, eBay and US Bank do not use digital signatures at all. This has been attributed to the difficulty end-users have in using digital signature technology (Tally, G., et al, 2004).

2. Online Brand Monitoring

Companies such as Cyveillance, NameProtect and Netcraft offer on-line brand monitoring services. This entails monitoring domain name registrations, web pages, spam emails and other on-line content for illegal use of clients' brand names. If illegal use of a client's brand name is detected, for example on a phishing web site, then the client is notified and can take remedial to close the website.

In the context of phishing attacks, some components of this service are more useful than others. The monitoring of domain name registrations is perhaps the most useful component, as organizations can be alerted in advance to possible phishing websites. For example, the organization with the domain bank.com could be informed that bank-security.com was recently registered by another party. The organization controlling bank.com may then conclude that this newly registered domain is likely to be used for phishing attacks, so could give prior warning to customers.

The web page and spam email monitoring components are less useful. These features may alert organizations to new phishing attacks, but they still have to go through the appropriate channels to close down the phishing website. Closing down phishing websites can take as long as 15 days. During this period end-users are still vulnerable to the phishing attack.

3. Spam Filters

Phishing emails are transmitted using normal spam mechanisms and often contain similar characteristics to commercial spam emails. Consequently, current spam filters can be used to defend end-users against phishing attacks.

Spam filters classify incoming mail as either spam or non-spam. Where the classification takes place depends on the type of spam filter employed. Gateway spam filtering is normally used by large organizations and ISPs. This type of filter adjudges email messages arriving at the mail gateway. Desktop spam filters are also available and may be integrated or run in combination with a user's mail program. Filters of this type judge email once it has been download from the mail server.

Spam emails are often removed by filters, and no spam may be present when the end-user views or downloads their mail. Alternatively, spam filters may simply mark suspect emails as spam. Some systems have the ability to quarantine spam emails, and permit users to browse spam emails that have been removed.

Current spam filters aim to catch as much spam as possible whilst minimizing the degree of false-positives. To achieve this, most spam filters use Bayesian filtering techniques. Bayesian filtering allows the filter to ‘learn’ and adapt over time, taking into account the latest spam emails and the user's personal preferences. Most of today's popular email filters employ Bayesian filtering capabilities

Although spam filters are often very effective, they are not infallible. Even the best filtering technology still lets some spam through (Graham, 2003). Consequently, end-users cannot fully rely on spam filters to remove all phishing emails from their mailbox. In addition, for a variety of reasons, many users do not use spam filters at all. They may not currently receive enough spam to warrant the use of a spam filter. Some users may not have the technical ability to install or configure a spam filter, or may believe that they are prohibitively expensive. Many users may not even be aware that spam filters exist. For such reasons, spam filters cannot be considered a complete solution to phishing emails.

4. Web browser extensions

Since phishing relies largely on deceptive Web sites, Web browsers are a natural focus for anti-phishng measures. An early means of adding anti-phishing capabilities to Internet Explorer was the Earthlink Toolbar. Whenever the user browses to a known phishing web site, the tool alerts them to this fact and the user is redirected to a warning page hosted by Earthlink (Earthlink, 2006). Similar strategies for user alerting are now appearing within mainstream Web browsers. Mozilla Firefox has a facility enabled by default that also works by checking visited Web sites against a list of known phishing sites. In this case, the phishing site list is automatically downloaded and regularly updated within Firefox. Since new phishing attacks may arise at any time, an additional option allows users to check sites against an online service for more up-to-date protection. Users may also report ‘Web Forgery’ in cases where a suspect site is not detected by the anti-

phishing system. In similar vein, Microsoft have added comparable anti-phishing features to version 7 of Internet Explorer.

Such anti-phishing extensions to Web browsers help by alerting users to known phishing sites. This relies on a current database of phishing website information. A system designed in this way cannot protect against all phishing attacks, since there will always be a delay between a phishing attack going live and the database being updated. During this delay users are not protected from the new phishing attack.

3. THE ANTI-PHISHING WEB SERVICE

Although there are existing anti-spam and anti-phishing solutions for end-users, none of them are widely deployed or fully effective. Rising financial losses and a growing numbers of phishing attacks have led to anti-phishing extensions to existing Web browsers, but there is little product attention on helping end-users determine whether a received email is a phishing attempt. This often leaves users relying on their own judgment when assessing the authenticity of an email.

In this context, we have prototyped an Anti-Phishing Web Service (APWS). This facility analyses users' emails and advises if they are likely phishing attempts. The APWS operates in a three step process: (1) Users forward any suspect email to the APWS for analysis; (2) The APWS performs a series of tests on the email, each resulting in a score. An overall score is derived which indicates a likelihood that the email is a phishing attempt; (3) The APWS generates an online report for the user.

The APWS has several advantages over existing end-user anti-spam and anti-phishing solutions. Firstly, the APWS helps the end-user decide if an email is a phishing attempt by applying sophisticated analysis techniques. Without assistance, users would otherwise have to judge whether an email is genuine using whatever limited knowledge they may have. Secondly, the APWS may be combined with a spam filter. The spam filter can attempt to catch all spam and phishing emails. Any emails which pass through can still be sent to the APWS for analysis. Thirdly, the APWS has no reliance on a database of phishing attempts. This means that new, un-encountered phishing attempts may be caught. Fourthly, the APWS operates as a network service and requires no software installation on the user's machine.

The goal of the APWS is to determine whether or not an email is a phishing attempt. To achieve this, it relies on a collection of real phishing emails that were analysed as a basis for test design. Once the tests have been applied, a report is generated on the results. The system's report function writes out the following email headers to the html report file: From, To, Date Sent and Subject and adds the total score and corresponding phishing risk rating for the email in question. The total score of an email begins at 0. Every test that returns true adds 1 to the total score (this could be altered to weight some tests more than others). A phishing risk rating is assigned according to the total score for the email (Table 1).

Table 1: Phishing risk rating

Total Score	Risk Rating
3 or more	Very High
2	High
1	Moderate
0	Low

The content of test emails is parsed by the APWS in order to check all links, anchor tags and form tags. Evaluating the credibility of a submitted email is largely heuristic, with a series of seventeen tests applied to the email message in order to derive its final score. An outline of these tests is given below.

Phishing emails often contain URLs with encoded characters in an attempt to disguise the true link target. We apply a test on every embedded Web link which returns true if the authority part of the URI contains encoded characters. Similarly, a test checks each Web link and returns true if the user-info part contains encoded characters. If the path part, the query part or the fragment part of Web link contains encoded characters, each of these contributes a positive score to the message result.

A further common ploy in phishing emails is the use of URLs in which the host part is a dotted quad IP address as an attempt to disguise the true URL. We check each URL for this feature and increment the positive score if the result is true. Similarly, a positive value is added for any URLs in which the host part is an IP address expressed as a single decimal number, and for URLs in which the host part is a dotted quad IP address, with each quad expressed either in octal or hexadecimal.

Emails containing URLs with user-information in the authority part of the URL are often attempting to obscure the true target, and make it appear as if the link points elsewhere. We test every embedded URL and return true if the authority part contains user-information. Another tactic used to disguise the true destination of a Web link, is to use URLs with user-information in the authority part of the URL, and in addition the user-information itself resembles a URL. We test every URL for this feature and return true if the authority part has user-information that resembles a URL. Embedded URLs that specify non-standard Web ports are a further hint of irregularity. For any URL in which the port is not 80, we return an additional positive increment.

The presence of a URL in which the organization domain contains the purported sender's organization domain as a substring, is a futher positive score since this is considered an attempt to disguise the link's true target. Similarly, URLs in which a subdomain matches the purported sender's organization domain returns a positive increment. If a URL has an organization domain that closely matches the purported sender's organisation domain, we also increment the positive score. This test is performed on every URL and returns true if the Levenshtein Distance (LD) between the organization domain and the purported sender's organization domain is less than half the length of the purported sender's organization domain. We do not return true if the LD in this calculation is zero (i.e. the domains being compared are equal).

Phishing emails often contain anchor tags wherein the text the anchor text resembles a URL, but that URL points to a different location than the tag's ‘href’ attribute. We returns a positive increment for URLs with such a feature. Finally, we check for attachments with malicious content. This test is performed on every attachment object and returns a positive increment if the attached file name extension matches one of the following: ade, adp, bas, bat, chm, cmd, com, cpl, crt, exe, hlp, hta, inf, ins, isp, js, jse, lnk, mdb, mde, msc, msi, msp, mst, pcd, pif, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf and wsh.

4. TESTING

The prototype APWS facility was tested with sets of phishing and non-phishing emails. Twenty phishing emails, representing a broad cross-section of current phishing emails, were collected over a period of 3 months. The average final APWS score for an email in this collection was 2.0, corresponding to a phishing risk rating of high. Thirty non-phishing emails containing both legitimate mail and non-phishing spam were also employed. The final scores for these emails were all 0 apart from four messages. The average final score for emails in this collection was 0.37, corresponding to a low phishing risk rating. The 4 anomalous emails had final scores of 1 or more, which should not occur for non-phishing emails. This equates to a false-positive rate of 13%, which is slightly higher than most current spam filters.

While the APWS successfully identified 19 out of 20 emails in the phishing collection, 4 out of 30 emails in the non-phishing collection were false positives. These results are considered reasonable for a proof of concept system, but indicate that the APWS has scope for improvement. The weakness in the current version of the APWS is its pattern-recognition approach to detection of phishing emails. As a consequence, there may always be a small number of emails incorrectly classified as phishing attempts. This approach is also unable to identify new phishing components since all of the current tests were based upon patterns identified in known phishing emails. The deficiencies inherent in the pattern-recognition approach may be addressed by the later addition of text-categorization (based on Bayesian statistics) to the APWS.

5. CONCLUSIONS

Phishing is a growing problem. While active measures are now appearing in mainstream Web browsers, few software solutions aim to protect email users against this scam. Spam filters help somewhat in this regard, but email users are still vulnerable to phishing emails that pass through undetected. Currently, users have to rely

on their own judgment when faced with such messages and often incorrectly identify phishing emails as legitimate. Our prototype Anti-Phishing Web Service (APWS) goes some way toward addressing this difficulty. The reports currently generated by the APWS provide a Web page that contains the results of each test conducted on any submitted email, including the overall score and corresponding phishing risk rating. Our goal is not merely to indicate whether an email is legitimate or a phishing attempt, but also to advise the user on how any decision was reached. This reflects our belief in the need for user education as a means of protection. Further development is underway to enhance the detection and advisory capabilities of our prototype service.

REFERENCES

APWG 2004. *Phishing Attack Trends Report.* http://www.antiphishing.org/APWG_Phishing_Attack_Report-Jun2004.pdf

APWG, 2006. *Origins of the Word 'Phishing'.* http://www.antiphishing.org/word_phish.htm

BBC News, 2003. *Crackdown on spam.* http://news.bbc.co.uk/2/hi/programmes/working_lunch/3310053.stm

Earthlink, 2006. *Internet Scams and ScamBlocker.* http://www.earthlink.net/software/free/toolbar/

Gaudin, S., 2004. *Nine out of 10 U.S. Emails Now Spam.* http://www.esecurityplanet.com/trends/article.php/3365341

Graham, P., 2003. *So Far, So Good.* http://www.paulgraham.com/sofar.html

Hird, S., 2002. Technical Solutions for Controlling Spam. *Proceedings of AUUG2002*, Melbourne, Australia. http://www.lasr.cs.ucla.edu/classes/239_2.spring04/papers/technical_spam.pdf

Leyden, J., 2004a. *Zombie PCs spew out 80% of spam.* http://www.theregister.co.uk/2004/06/04/trojan_spam_study/

Leyden, J., 2004b. *Phishermen attack on a viral scale.* http://www.theregister.co.uk/2004/08/10/phishing_vs_viruses/

Litan, A., 2004. http://www4.gartner.com/DisplayDocument?id=431660

MailFrontier. 2004. *28% of U.S. Adults Continue to Inaccurately Identify Phishing Email Scams.* http://www.mailfrontier.com/press/press_phishtest.html

Sophos, 2006. *Virus information W32/Sobig-A.* http://www.sophos.com/virusinfo/analyses/w32sobiga.html

Spamhaus, 2003. *Virus and dDoS Attacks on Spamhaus* http://www.spamhaus.org/cyberattacks/index.html

Tally, G., et al, 2004. *McAfee Research Anti-Phishing: Best Practices for Institutions and Consumers.* http://www.networkassociates.com/us/_tier2/products/_media/mcafee/wp_antiphishing.pdf

Telephone Tribute, 2000. *Phone Phreaking*. http://www.telephonetribute.com/phonephreaking.html

Wikipedia, 2006a. *Pyramid scheme.* http://en.wikipedia.org/wiki/Pyramid_scheme

Wikipedia, 2006b. *Advance fee fraud.*: http://en.wikipedia.org/wiki/Advance_fee_fraud