



:: A Pretty Kettle of Phish

Something phishy in your email?
What you need to know about phishing fraud

David Harley BA CISSP FBCS CITP

Andrew Lee CISSP



Table of Contents

Introduction	2
The Compleat Angler – A Brief History of Phishing	3
Older email scams	3
Pump and Dump scams	3
The eternal 419	4
Fresher Phish	6
Phishing Attack Components	6
Bait Distribution	7
Phishing Targets	7
Spear Phishing	8
Intent to Deceive	9
Data Collection	9
Phishing Cousins	10
Phish Farms	10
A Cross to Bear	11
The Phishing Economy	11
Solutions	13
Detection Techniques	14
Phish education	15
Phish Recognition and Response for End-Users	16
How do I recognize a phish?	16
What should I do about it?	17
Conclusion	20
References	21
Glossary	23



Introduction

“Phishing” usually refers to the practice of posting a deceptive message¹ as part of an attempt at fraud and/or identity theft. It’s sometimes referred to as “carding”, “hoax mail”, or “spoofing”. In this paper, we will refer exclusively to the practice as phishing, as the use of these other terms can be confusing for the following reasons.

Historically, carding is understood to apply to the fraudulent use of an (often stolen) credit card, resulting in direct loss to the retailer. It doesn’t necessarily carry the same implications of theft of the card owner’s money or identity. Furthermore, the presentation of a stolen card or card data is only part of the full phishing process, and may not be part of a phishing attack at all. The term can also apply to a scammer’s verifying that a stolen card is still valid.

- Spoofing has many meanings in security, relating to a wide range of areas, including DNS/IP spoofing, forgery of goods and/or documents, forged email, and so on. While some of these usages may be used appropriately in the context of a specific phishing attack, the term is best avoided as too general, particularly when used out of context.
- The term spoof mail or hoax mail is often used synonymously with the terms phishing or phishing mail.^{2,3} The term spoof mail is defensible, since the identity of the sender is normally forged. However, the use of the word hoax in this context should be strenuously avoided, in view of the widespread and long-term use of the term “hoax mail” to apply to messages that are deceptive in intent or origin, but not specifically intended to execute a financial fraud or identity theft. This latter use of the term hoax is more closely related to urban legends and chain letters.⁴

Traditionally, the term “phishing” refers to an email or other message that has been manipulated to make it look as if it comes from a legitimate business or agency, when in reality it is from another (criminal) source. It is intended to trick the recipient, using social engineering techniques, into giving sensitive data to the scammer (or phisher). Although there have been phishing attacks focused on industrial espionage, targeted data are often financial (credit card details, for example), or intended to allow the scammer unauthorized access to financial data (password information, for example). The phisher’s intention is usually to plunder the victim’s financial resources, to steal their identity in order to defraud others, to obtain such information for sale to others, or a combination of all of these.

In principle, though, it’s possible for phishing techniques to be used to gain any data for any purpose, and the posting of the deceptive message is only part of the phishing process. So, indeed, is the acquisition of data from fake web sites or using keyloggers and backdoor Trojans: the whole phishing process is explored a little further in the section below on “The Phishing Economy”.



The Compleat Angler – A Brief History of Phishing

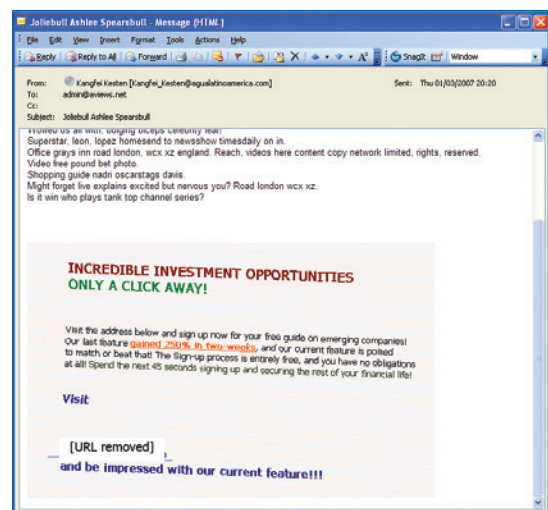
The term phishing has been around since the mid 1990s, but was originally largely limited to angling for AOL account passwords and credit card information (and, to a lesser extent, other providers such as Prodigy). Indeed, a large proportion of non-replicative malware of the time was aimed at stealing such information, as it was relatively expensive to subscribe to an Internet provider. It clearly refers to the practice of “fishing” for victims, using a deceptive message as bait: the use of “ph” instead of “f” is probably influenced by the older term “phreaking” (a portmanteau term for “phone freaking”, applied to techniques for the illicit exploitation of the exploitation of phone systems). The usage has invited a cascade of wordplay around the paired consonants “p” and “h” which we have occasionally phailed to resist ourselves.

Older email scams

AOL scams were often but not necessarily email-borne; nor were they the first scams to circulate in the darker corners of the Internet. Indeed, 419s, pyramid schemes, lottery pyramids, Ponzi schemes, homeworkeer business “opportunities”, mule scams and other job scams, and so forth have been around longer than email, and are still seen, often in more sophisticated forms. These are not discussed here, but Daniel Barrett’s book “Bandits on the Information Superhighway”,⁵ though seriously outdated in terms of the current threatscape, is a useful resource for historical completists.

Pump and Dump scams

Pump and Dump mails are designed to temporarily inflate the value of stock held by the scammer by advertising it to naïve investors.⁶ As the value of the stock rises, the initiators of the scam sell off their stock, which promptly falls in value, resulting in a financial loss to the new investors. These mails are often seen as a minor branch of the spam forest, especially in countries other than the USA where the same trading structures for penny stock trading are not found. However, the rising volume of such scams (involving claims of marketability and innovation strangely reminiscent of the bubble companies⁷ of the 18th Century) plus the significant involvement of organized crime⁸ suggest the tip of a sinister and damaging iceberg.



Pump & Dump image spam: note also the randomized hashbuster text

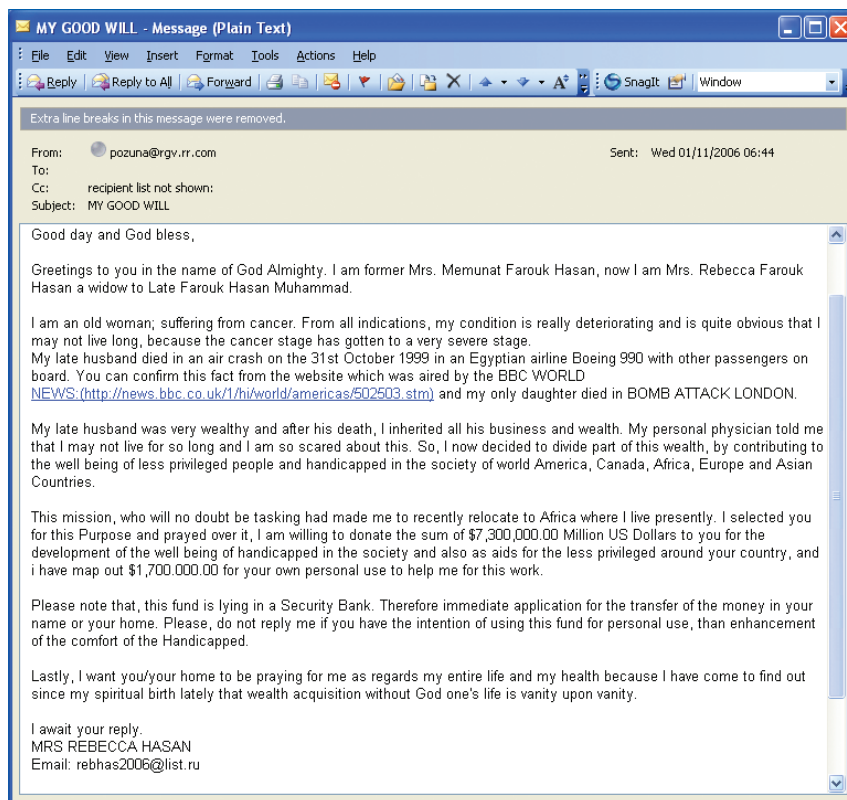


These schemes involve the “hands-off” manipulation of the stock market, rather than the direct plundering of a victim’s funds and identity that characterizes the phishing scam. However, they constitute a much more serious problem than is generally realized at present.

The eternal 419

419s get their name from section 419 of the Nigerian Criminal Code, reflecting the fact that this type of scam very often (but by no means always) overtly originate in Nigeria, the Côte d’Ivoire and thereabouts. They are also known as “Advance Fee Fraud”, because they generally offer large sums of windfall money, but when the victim responds to the bait, they soon find that they have to pay advance fees of various kinds – tax, bank charges, even bribes – before the windfall can finally be delivered. Most security professionals distinguish between 419s and “real” phishing.⁹ However, there are enough similarities between the two activities to contradict the assumption that they are completely separate phenomena. For instance:

- Both are frequently implemented by organized gangs.
- Both include money-laundering as part of the exploitation mechanism.
- Both are opportunistic, taking advantage of personal tragedies, natural disasters and so on as a means of parting a victim from their money.



A classic 419 scam.



- Both are sometimes very stereotyped in the way they present their bait emails
- Both use social engineering techniques to bait the trap, albeit with the 419 offering some sort of financial reward, and phishing often purporting to prevent financial loss.
- Both involve some form of identity theft: that is, they claim to be someone else or to represent an often real and presumed legitimate organization.

Some significant points of difference are that:

419s often, though by no means invariably, have a strong overt African connection, though it isn't practical to distinguish between frauds on a purely national basis. Indeed, there have been an increasing number of such frauds ostensibly originating in conflict territories such as Iraq and Afghanistan.

419s rely on an element, sooner or later in the defrauding process, of personal contact, whereas phishing gangs tend to work at more of a distance and go to lengths to cover their tracks.

419s generally rely more on social engineering (or human gullibility) than on technical attacks such as embedding malware, cross site scripting, DNS spoofing and so on. (Historically phishing was also more reliant on social engineering, but techniques have evolved to combine this with more advanced technological methods)

It's not unknown for a 419 scam to hinge upon a deceptive web site, though it's more common for a 419 to use a legitimate but irrelevant web site as some form of authentication. Similarly, not all phishing attacks employ a deceptive site such as a fake bank site, but most do. However, it's uncommon for a 419 to depend on a fake financial institution site, or forms that seem to be generated by genuine institutions.

The 419 scammer often claims to represent a fake organization or group of individuals, whereas the phisher generally relies on spoofing a genuine organization's mail or web site.

419s tend to work on a more personal level: the scammer often claims to represent an organization such as a bank or a military organization, but will usually be offering a "deal" which would be against the interest of that organization.

Thus, while there are evident points of dissimilarity, it's hard to find absolute differences. There are features of tone and phraseology that are unmistakably "419", and some of the topics are virtually unique to the 419 – bank account proxy (next of kin) scams, lottery scams, some kinds of job scam and so on. However, some others, such as fake charity and disaster relief appeals and mule recruitment solicitations, resemble the output of phishing gangs in topic, if not in tone. Indeed, 419 gangs are now showing an increasing eagerness to pick up on phishing ideas and technology.¹⁰



Phresher Phish

Around 2003-2004, changes in tone, target and technology brought phishing attacks into much greater prominence. Increasingly, the targets were major organizations (and their customers) in the financial sector (notably banks, building societies and credit unions, as well as eBay and PayPal) and the practice had become linked with tricks for passing off the request for data as if it came from a legitimate business, including:

- Web sites constructed to resemble (increasingly realistically) the genuine site.
- Pop-up forms designed to appear when the real site was accessed via a link in the email.
- Deceptive links, disguised in various ways to resemble links to a legitimate site.
- Replication of the entire genuine site, with only the essential login area compromised, in some cases by inserting a malicious script dynamically into the genuine site.

Phishing technologies also included (and continue to include) the planting of malware and spyware such as keyloggers, password stealers, and backdoors. As with older email-borne malware such as mass mailer viruses, either the malware itself or a malicious URL is spammed out to prospective victims, attached to messages passed off as an invitation to view an electronic greetings card from “a friend”, or to contact a prospective romantic partner.

Phishing Attack Components

A phishing attack can be regarded as having three parts, as described by Mustaca.¹¹ However, Mustaca's definitions of this tripartite structure are focused on a narrower range of attacks than we deal with here, so the following definitions expand on those:

- Bait distribution through email, instant messaging, or, increasingly, other channels. Typical phish email messages are examined later, but although most current literature assumes that the bait is cast via email (still the most usual channel), other channels are already used. Vishing, for example, uses VoIP (Voice over IP) technology to extend phish-like scams to telephone services.
- Data collection through a fake web site (or a direct response to email, or an intermediate form of misauthenticated response, or through the planting of some form of spyware onto the victim's system). Again, it's often assumed that fake web sites are an essential component of phishing attacks, but they are actually a special case of data collection through misdirection, albeit the most common at this time.
- The use of the misappropriated information for purposes of fraud and (to a lesser extent) identity theft.
- These definitions are purely functional: a phishing crew may comprise a far wider range of roles (bot-herder, mule-driver, programmer and so on), and we consider these lower level considerations in the section below on the phishing economy.



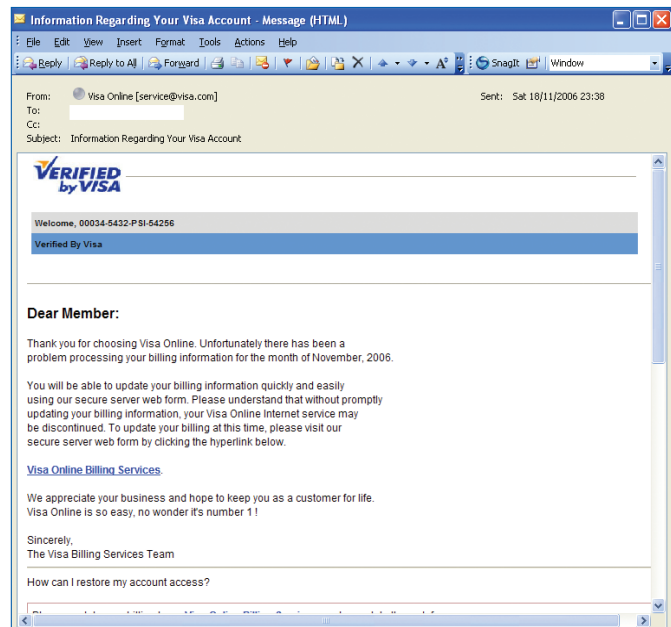
Bait Distribution

Classic phishing emails include many forms of message, from crude, badly-spelled plain-text to sophisticated, well-conceived, graphic-rich messages virtually indistinguishable from the real thing. They tend to be distributed via networks (botnets) of systems compromised or infected by specialized malicious software called bots, which enable a criminal to control compromised systems remotely, often by IRC (and often rented from a bot-herder for the purpose). Such botnets are also used for other criminal purposes such as the distribution of other types of fraud and spam (pump and dump scams, for instance), or for the orchestration of Distributed Denial of Service (DDoS) attacks.

Phishing Targets

Of course, the target of a phishing attack is in one sense the recipient of the bait mail (or other form of message), but the term “phishing target” is also (indeed, more often) applied to the organization whose “brand” or identity is stolen by the scammer. The following are some of the organizations most targeted by phishers as a source of potential victims among the victim’s customers.

Historically, ISPs like AOL were the main target for phishing when the term and the activity first came into vogue. In a paper published in 1998¹² a number of phishing messages are quoted that use very similar social engineering techniques to modern phishing messages, to very similar ends— the theft of ISP account passwords and credit card numbers – over similar channels: that is, email and IRC. They even presage more recent concerns¹³ about the targeting of minors to steal sensitive information. At the same time, there were already AOL-targeting password stealers and Trojans mailing account information, credit card data and so on, to an anonymous drop box. ISPs remain a major target, though many reports¹⁴ suggest they are targeted primarily to steal credit card information rather than ISP account information.



Visa Online Phish: note the threat of account discontinuation.



In recent years, while many of the basic techniques remain in use (although displaying increasing refinement and sophistication), the targets have diversified. Recent figures from Phishtank¹⁵ confirm a longstanding trend: the most frequently phished sites are PayPal and eBay (other auction, e-commerce and money transfer services are also hit, but the number of hits these sites get reflects their leading position in the market place). Other “Top 10” targets tend to be top banks such as Barclays, Citibank and Bank of America. However, even small banks, building societies, credit unions and so on may be targeted – phishing aimed at small institutions is sometimes referred to as “puddle phishing”.

Financial institutions are far from being the only targets, though. Retail operations like Sears are also targeted, either because they are themselves providers of financial services such as credit and store cards or because they offer a means for the phisher to steal information related to cards issued by other providers. Essentially, any organization that provides a for-fee product or service is a potential target, if the use of their “brand” is a possible route to eliciting sensitive personal information, financial or otherwise. Even a non-commercial entity such as national or local government, some healthcare and educational organizations, and so on, may routinely allow or solicit the use of financial information to pay for services. Even if they don’t, phishers may be able to use social engineering to persuade the victim to part with sensitive information to an entity they believe to be, for example, the IRS (Internal Revenue Service),¹⁶ the Social Security Administration¹⁷ or a law enforcement agency.

Natural disasters inspire many public-spirited aid initiatives, both official and unofficial, but also generate a rash of 419s and phishing attacks, sometimes complete with spoofed web sites.¹⁸ These take advantage of the natural sympathies of their victims, and rather than directing the funds to the victims of disaster, the collectors pocket the proceeds and walk away.

Note that the target of the phished email is not necessarily the target of the phished web site. One particularly bizarre phish report¹⁹ concerns an email that appears to come from the “Netcraft Anti-Phishing Team” offering a “small prize.” However, the fake web site represents itself as eBay, so eBay is the primary phishing target, not Netcraft.

Spear Phishing

Phishes aim to hook the users of specific services by pretending to come from a service provider, but the bait is usually distributed more or less randomly: after all, a phishing gang isn’t usually able to tell whether the recipient of the message is a customer of that service. Sometimes, though, deceptive mails can be highly targeted. Where there is a much higher than normal probability that the potential victim is a member of a targeted group, the term “spear phishing” is often used. Closely related to this problem is the one highlighted by NISCC²⁰ and many other CERTs²¹ since 2005. Information-gathering Trojans are sent to targeted individuals: the mail is spoofed to make it appear that it comes from the target’s employing organization or a recreational or other group they belong to, to make it likelier that they’ll open attached or linked documents or files – malicious programs are frequently embedded into data files. The aim in these cases tends to be closer to industrial espionage



than classic phishing fraud: the malware is used to steal passwords to privileged accounts, upload system information and sensitive documents, the downloading of additional malware, and relayed attacks against other systems.

Intent to Deceive

Phishing emails use a number of technical wrinkles to evade standard detection technologies.²² Many of these are used by other forms of spam, for instance:

- Hash busters – random text or graphical elements introduced into a message to forestall detection based on a hash or checksum.
- Spam-flagging words are split using HTML comments, pairs of zero width tags, bogus tags, and so on, so that they look like normal words when displayed on screen, but are more difficult for filters to detect as complete words.
- Using white characters on white background (or a variation on this theme) to hide neutral text intended to confuse filters, but which might look suspicious to the recipient if it was visible.

Image spam is a term applied to spam in which the core of the message is presented as a graphical image, not as pure text or HTML text, so that it isn't susceptible to filtering on textual content.²³ Since purely graphical content can be used as a spam indicator, this kind of spam is often accompanied by text which may be random or from a source of neutral text such as a novel or a news item. Image spam is now most commonly associated with the Pump & Dump stock scam phenomenon, but has a long and ignominious history in phishing.

Data Collection

There are, however, other techniques that are more characteristic of phish mails than other types of spam and scam, most of them associated with the hiding or obfuscation of the real target URL, using such techniques as URL encoding, specially constructed INPUT tags, or misusing a <map> tag to disguise a malicious URL.²² A detailed explanation of these techniques would require a short book in its own right: what matters here is that the phisher is attempting to disguise a suspicious link in such a way that it looks like a legitimate URL. Since the resulting link looks convincing to the victim, misdirection to a well-constructed but spoofed site is practically guaranteed, if the victim does actually have a business relationship with that provider.

These techniques are, along with various forms of social engineering, intended to lure the recipient of the bait into the next phase, whereby sensitive (often financial) data are gathered by the phisher. Deceptive web sites are not the only means by which data may be collected: alternatives include

- Forms embedded into a bait message (email, instant messaging, and so on).
- Malicious software attached to or referenced by the message.
- Telephone numbers referenced in the message.

Nor are bait messages the only approach to reeling in a victim, though they may be used in tandem with the following methods.



Phishing Cousins

There are a number of ways of decoying a victim away from the legitimate web site they think they're accessing, usually in conjunction with bait emails. Cousin domains are domains registered with names that incorporate the names of targeted institutions or a close variant with the intention of setting up a phishing web site. Domains with names like "UpdateMyFirstBankofHicksvilleAccount.com" can be pretty effective, since legitimate institutions often use similarly constructed domains or sub-domains. Variations on this cybersquatting theme include using slightly misspelt names like "Barclaays.com" which not only look authentic to a careless observer, but may also catch a careless typist looking for the real site (this is sometimes referred to as typosquatting). There are also innumerable ways of disguising a web link within email in order to pass it off as link to a legitimate site. Patches for widely exploited vulnerabilities in browsers (especially Internet Explorer) are available, and may have been incorporated into current versions, but there are other techniques available for misdirecting victims to spoofed sites.

Phish Pharms

DNS spoofing is a term applied to the malicious, covert redirection¹ of a web browser from a legitimate site to a different, illegitimate IP address. The term pharming is sometimes used where the redirection is to a web site controlled by a phisher. Instead of the legitimate web site that the victim thinks he is accessing, for the specific purpose of identity theft by the stealing of online credentials.⁹ A specific technique for this misdirection is DNS cache poisoning, where a flaw in the DNS (Domain Name Server) software is exploited, with the result that the server accepts false information. The DNS responses are not correctly validated, and the false data are therefore cached locally and returned to other systems making the same queries.²⁴ More commonly, some malware contains code to add information to the 'hosts' file on the system, which is normally queried by default before DNS, to resolve a given name (e.g. <http://www.ebay.com>) to a different IP address. This simple technique is effective, because it works even when the user directly enters the correct URL into a browser.

A Cross to Bear

Once the victim is decoyed to a deceptive site, a number of attacks may be used for data harvesting, including:

- Pure social engineering (inviting the victim to enter information onto a form, or to install spyware, for instance.)
- As a variation on the invitation to fill in a web form, a form that pops up over a legitimate web site with which it has no connection. In more sophisticated attacks, the credentials entered may be passed through to the legitimate site, and used to log the user in. To the user it seems as if the transaction was entirely normal. In other cases the form may simply redirect the user to the genuine site, where the correct login form is present: in most cases the user will just assume that the details were incorrectly entered the first time.



- exploits to do so automatically, rather than by social engineering.
- Some variation on Cross-Site Scripting, also known as XSS or CSS, though the use of the latter acronym is best avoided, since it invites confusion with Cascading Style Sheets. XSS is a common partial misnomer for an attack where a client-side or server-side vulnerability is used to facilitate an attack against a client application. (It's a misnomer because the attacks don't have to be cross-site, or even to use scripting.)²⁵

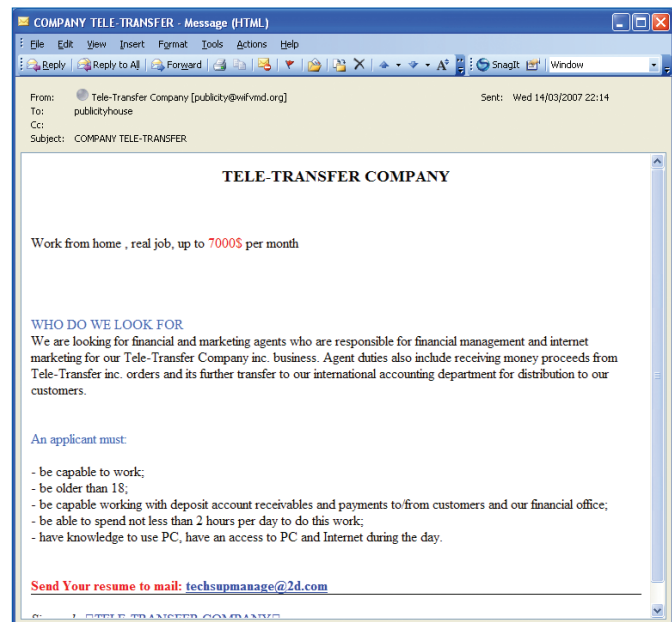
The kind of techniques sometimes attributed or related to XSS include injecting an arbitrary malicious script into a web transaction, injection of malicious data specially formatted to force the server to misinterpret the input, and even forcing⁹ insecure redirect mechanisms.

So-called Cross-Site Scripting techniques have a number of applications in phishing, especially when reinforced with social engineering: for instance, the execution or installation of malicious code by exploiting weak client-side scripting, or increasing the client's exposure to a spoofed site in conjunction with legitimate pages, thus enhancing the credibility of the spoofed site.

The Phishing Economy

The range of targeted information, and the fraudulent use made of it, has widened. While there are still attacks aimed at stealing accounts for adolescent mischief rather than profit, they seem to have moved away from AOL towards venues such as MySpace.²⁶ Fraudulent activity is not always restricted to opportunistic, short term exploitation of credit cards: instead, it may be the jumping-off point for full-scale identity theft, involving such scams as the acquisition of large loans in the name of the unsuspecting victim.

While the media has certainly homed in on the idea that identity theft is the biggest problem with phishing, it still remains true that the 'one hit wonder' is by far the most frequent form of phishing. It is comparatively more difficult, and indeed risky, to assume the identity of a phished victim. It's more simple to just use the details once, and then either sell them, or otherwise launder them. A common way of laundering the money gained is to buy real goods with stolen creditcards, and then sell those goods at a huge discount via spammed emails.



Or would you rather be a (money) mule?

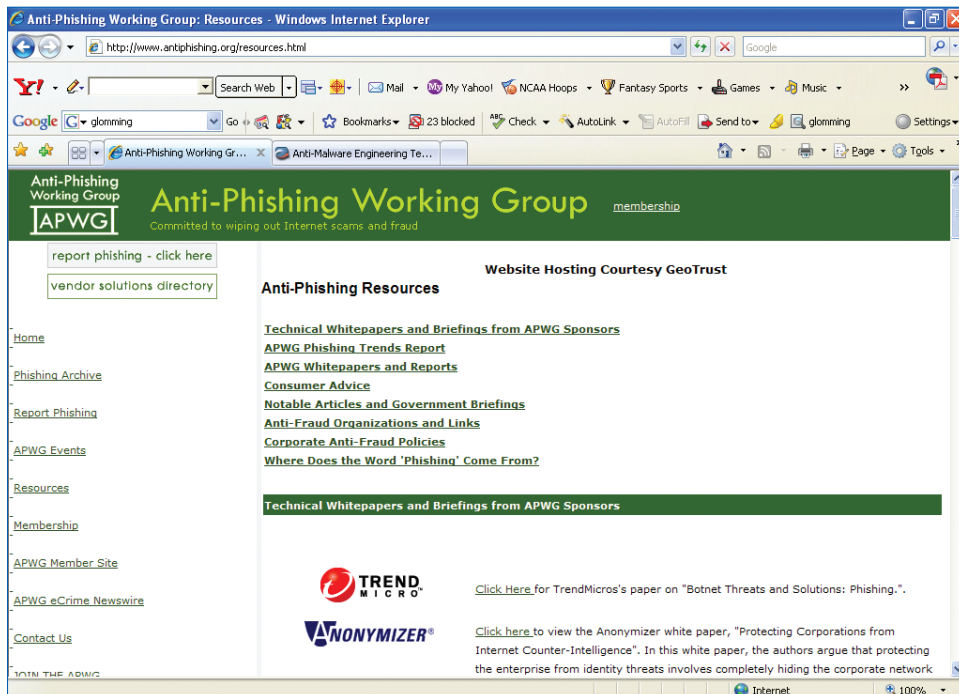


Phishing gangs now operate within a complex network infrastructure that closely resembles any other supply-and-demand economy.²⁷ Their members may take on a wide variety of roles and functions, taking in:

- Gathering of information such as target email addresses.
- Acquisition of tools for setting up phish sites (often using widely available phishing kits).
- Acquisition of spamming tools and hosts for bait distribution – this is a very common use for botnets.
- Acquisition of access to compromised hosts for scam pages.
- Setting up a process for retrieving stolen credentials e.g. from an anonymous mailbox (drop box) or via an eggdrop bot (a scriptable bot that connects to a chat room for control and data transfer).
- Supplying victim's credentials to a cashier for "cashing out" (conversion to cash).
- Use of stolen credentials to buy goods subsequently sold on to the black market.

A common manifestation of these money laundering activities is the mule solicitation email, offering "financial management" jobs that involve receiving money and passing it further up the chain after taking a percentage as commission.

Solutions



The Anti-Phishing Working Group site holds reports, resources, and a phish repository.

A number of collaborative groups, some more formal than others, are now working in this space. The Anti-Phishing Working Group (APWG) – <http://www.antiphishing.org/> - describes itself as a “global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types”. Its members include banks and other financial institutions, ISPs, anti-phishing solutions providers, and law enforcement. It runs a number of services such as a reporting service, phishing archive, and meetings and events: it also runs a number of working groups, dealing with such areas as Best Practices, Education, Solution Evaluation, and Working with Law Enforcement.

There is no single solution to the phishing problem: as so often in security, it pays to distribute your eggs between as many baskets as you can afford – more formally, this approach is often referred to as “defense in depth” – and at a number of levels:

- Technological solutions such as:
 - Web filtering
 - Browser security plug-ins



- Multi-level malware management solutions
- DNS blacklisting and more sophisticated reputation services
- Mail authentication measures such as SPF
- Direct cooperation with law enforcement (and ISP's) to track gangs and close down phishing resources.
- Safer banking practices such as 2/3-factor authentication, mutual authentication between the client and the banking system, and better practice in customer communications and notifications.
- Educational practices, from policy and governance to phishing quizzes and training strategies.

MAAWG (Messaging Anti-Abuse Working Group) – <http://www.maawg.org> – aims for a holistic approach to working collaboratively within the messaging industry, and has collaborated with other groups such as APWG within the anti-phishing space.

Reporting phish and other frauds such as 419s can be a frustrating experience, in that there's often no feedback or means of gauging whether your reports have any impact, especially they're reported to over-worked, under-resourced law enforcement agencies. PIRT (Phishing Incident Reporting and Termination Squad) is a public, community-oriented initiative devoted to taking down phishing sites as quickly as possible, originating in a collaboration between CastleCops and Sunbelt Software. PIRT actively encourages public participation, and has had a noticeable impact on the phishing problem by allowing the rapid dissemination of quality data to trusted anti-phishing resources.

The anti-phishing community is a mosaic of many groups, some more visible than others, from vulnerable providers, to security vendors, to law enforcement agencies, to volunteer activist groups. The best chance of mitigating the problem lies in improving cooperation between these groups, but what can the non-specialists do to help themselves?

Detection Technologies

The "safe" technological solution to managing most phishing attacks is to prevent potential victims from accessing sites known to be dangerous. Comparisons²⁸ between various types of filter can only be a snapshot of current capabilities. Phishing sites tend to come and go very quickly: this is not, unfortunately, just an indication of how quickly phishing sites are taken down. It's just as likely to denote ranges of bot-compromised systems being switched in and out by the bot controller (botherder). Anti-Phishing toolbars constitute a potentially useful supplement to other detection and management techniques.²⁹ However, like any solution based on blacklisting (see below) they rely on information about known bad objects (sites, messages, attachments, links and so on), so users are susceptible to harm by unknown bad objects.

However, the main delivery channel for phishing bait continues to be email and closely allied technologies like Internet Messaging, so anti-virus and anti-spam technologies continue to pay a major role in intercepting bait messages before the victim can act upon



them. Anti-spam heuristic software can pick up a high percentage of phish mails, which use many of the same techniques as other forms of spam. Leading edge anti-virus scanners are very practiced at detecting known malware (including such relevant malware as banking Trojans) and, heuristically, unknown malware, but can also detect features characteristic of phishing messages. Such measures as good software patching practice and the use of personal (and, where appropriate, corporate) firewalls are also recommended. However, technological security solutions are most effective when supported by sound knowledge of the subject at all levels of an organization.

Phish Education

An increasingly popular approach to end-user education is the phishing quiz. These can be multi-choice questions aimed to raise consciousness about phishing issues, or recognition tests where the participant assesses whether sample messages are genuine. These are, however, of highly variable quality. Often, the site's analysis of what is "suspicious" is inadequate or misleading.

Sometimes there isn't enough information given. A useful – though by no means infallible – phish detection heuristic is a link that appears to be to a genuine site but on examination turns out to resolve to a very different URL. A static screenshot that doesn't illustrate such a discrepancy can be seriously misleading. Sometimes a genuine service provider uses poor message composition and formatting that closely resembles that of phishing messages: if such a message is used as an example of a genuine mail, it may be assessed as a fake. When this happens, the participant is "penalized" for being suspicious of a mail that illustrates bad practice.

The continued use of such poor practices as phish-like text and unnecessary URL redirects into a very different domain is sometimes⁹ referred to as "consumer mis-education", since it primes potential victims to accept bad practice as "legitimate". It's particularly depressing when mis-education is reinforced by a phish quiz.

However, a paper³⁰ from CyLab not only illustrates one interesting alternative approach, but examines a whole range of training strategies. MySecurityPlan have a number of identity theft quiz resources that may be very useful.

- <http://www.mysecurityplan.net/score/>
- <http://www.mysecurityplan.com/litescore/>
- <http://www.mysecurityplan.com/quiz/>
- <http://www.mysecurityplan.com/safetyscore/>

Note: A paper examining the role of such phish education will be presented by the authors at the Virus Bulletin 2007 conference, and will be made available at <http://www.eset.com/download/whitepapers.php>³¹



Phish Recognition and Response for End-Users

What are phishers looking for? That depends on the exact scam, and which organization they're pretending to be. But in general, the sort of information they want is credit card numbers, Social Security Numbers, and any supporting information that will allow them to make purchases in your name,³² withdraw cash from your accounts, or use you as a channel for secondary exploitation, such as applying for loans in your name.

How do I Recognize a Phish?

There is no absolute, infallible test for discriminating between phishing mails and legitimate mails, either by eye or using automated software. Indeed, part of the problem is that occasionally, bad practice on the part of targeted organizations makes it easy for the scammer to generate mails that look very similar to the real thing. There are, however, a number of useful indicators.

- Email from a bank or other institution concerning an account with them that you don't actually have is obviously suspicious. It's almost certainly been sent to a number of email addresses the scammer got hold of, in the hope that in some cases, they'd strike lucky and someone with an account at that institution would get the message.
- There is, or should be, an obligation for any institution sending email relating to sensitive data to personalize it in some appropriate way so that you can be reasonably sure it comes from where it says it comes from.

If you get mail that you are reasonably sure comes from your bank (or similar), but doesn't conform to good practice, complain!

Email sent to an address that you do not use in when you contact that particular bank or service will always be suspicious. If possible, create a separate email address (most ISP's will allow this, but you could also use a service such as gmail), with a unique name, e.g. (mybanking.email@yourdomain.com), and use that address exclusively for that activity, never publishing it anywhere or using it to send email. This will provide an easy way of checking that it was sent to you at a correct address.

If you do have an account with the institution, but the message isn't addressed to you using your own name or a specific identifier such as a verifiable account number, regard it as highly suspicious. Greetings like "Dear Lloyds Bank Customer" or "Dear eBay User" suggest that the sender is trying to catch anyone who happens to receive the mail, and they have no idea who you are or whether you have an account or business relationship with the organization. If the identifier is one of your email addresses (e.g. "Dear henry056@hotmail.com"), that is still suspicious. It's trivial to insert the email address into the message. Assume that it is not genuine.

- If it does include your real name, that isn't a guarantee that it's genuine. There are



many ways of obtaining that information. In fact, sometimes it can be harvested from your full email identifier, without any need to find it out from other sources.

- If you do have an identifier, especially a numeric or alphanumeric identifier, it should be checked. For instance, it's common for eBay phishing emails to include tags like "Your registered name is included to show that this message came from eBay," but not actually to show the registered name, or even to use a made-up identifier.
- In principle, the same goes for digitally signed messages: it's very easy to counterfeit a PGP signature, for instance, so you can't tell whether it's genuine unless you actually try to verify it using PGP. Unfortunately, the propensity for some email clients to mess with incoming email causes even legitimately signed messages to occasionally have bad signatures.
- Reading message headers is a dark art requiring years of study at Hogwarts (<http://en.wikipedia.org/wiki/Hogwarts>). Well, not really. But many people are intimidated by it. However, here are a couple of things to watch out for that don't require you to read the full headers.
 - If the mail doesn't seem to be addressed to anyone, it was blind copied to you and, probably, any number of other people. Don't trust it.
 - It may seem to be addressed to someone else, including the apparent sender of the mail, or to a generic name such as "customer" or "clientlist." This is sometimes appropriate for mail sent to many people, especially if the blind copy field is used to preserve their privacy. However, where the message concerns sensitive information such as banking data, it suggests an inappropriate lack of personalization.
- If you receive email apparently from your bank or another institution with which you have a business relationship (say eBay, or a tax office, or eBay), that obviously doesn't mean that you should accept it unquestioningly. It does mean that if you already have electronic messages from that source, you have something to compare it with – but we have seen very convincing forgeries (messages as well as web sites). If it's likely to lead to your being required to authenticate yourself to a web site and it's not mail you'd expect to get from them, it's suspicious. This includes security warnings: email advising you that your account has been compromised is a common phishing type. A telephone notification can also be malicious, but it may be easier to ascertain whether it's genuine: at any rate, it can't be purely random, and there are ways of verifying such as calling back a known valid number (for instance, one off an account statement).
- Even if you are reasonably sure that the mail is genuine, do not click on an embedded URL directing you to a login page. If you have a pre-existing relationship with the organization, for instance if you already do e-banking with them, you should already have a standard login procedure: use that. If you need to contact them by phone, avoid using phone numbers included in the message. Just as web sites can be spoofed, so can telephone numbers: use the telephone directory!
- A particularly common trick (but also a clear indication of mischief if you spot it) is an embedded URL which looks legitimate but has been modified to hide the real target. URLs can be obscured in many ways, including the following, though some of the variations will not be accepted by many up-to-date browsers. However, if inspecting the source code for HTML mail or even passing the cursor over the URL shows a mismatch between the apparent site name and the target URL the browser actually sees, this is very suspicious.
 - Deceptive text inserted between `http://` and an "@" symbol: this may include



the apparent target name, but will be ignored by the browser, which will only interpret the text that follows the @ as the domain name.

- The domain name may be expressed as an IP address in one of several formats (dotted-decimal, dword, hexadecimal or octal). The characters forming the URL may also be expressed as hex: there are some examples at <http://www.pc-help.org/obscure.htm>.
- The URL may be made so long that it can not be completely displayed in the status bar.

In this snippet of HTML code from a Wells Fargo phishing message, the link looks like a convincing URL for online.wellsfargo.com using https, which sounds reassuringly secure: however, the real target (in double quotes) is very different.

```
<a href="http://g-lec.com/data/cont/news/sicherung/einfach_millionaer/wells/">  
https://online.wellsfargo.com/signon?LOB=CONS </a><br>
```

- For many phishers, their first language is not English, and this may show in the spelling and grammar. Major institutions and their marketing departments are aware that poor presentation makes a bad impression, and are usually careful to avoid it. However, it's always possible for a typographic or other error to slip through in a legitimate communication. Conversely, the fact that the presentation is impeccable isn't proof that a message is legitimate.
- The kind of crude, text-only phish we saw a few years ago is far rarer today, but the increasing sophistication of spam filter avoidance techniques sometimes brings gains in terms of detection: many phishing messages are classic image spam, or include hashbusting graphics or text, and so on. These are intended to get the message past automated filtering measures, but can be quite noticeable to the human eye.
- One of the weapons in the phisher's armoury is to present the problem that requires you to log in as requiring urgent resolution ("You must log in within 24 hours or your account will be terminated for security reasons.") This variation on a well-known sales technique ("Offer only lasts till the end of today!") is intended to panic you into responding. Apart from increasing the pressure on the victim, it also works to the advantage of the phisher, who often needs an urgent response before law enforcement and other countermeasures are put into place. There is no reason which either of us could think of which would require you to take such action. Indeed, in cases of doubt, your bank may well telephone you, rather than using email, to check the details. Be aware though, that some phishing frauds have been elaborate enough to incorporate a telephone call to the victim, to 'take them through security' as part of the phish. This is a rare, but nonetheless real social engineering attack.



What should I do about it?

Any mail that includes a link to a web site at which you're expected to enter your credentials is potentially a phishing attack, as already indicated. If you have any doubts as to the genuineness of what appears to be a targeted attack, your first move is to find a known valid phone number or email address to check with the provider and let them know that they're a target, as well as alerting specialist groups like PIRT and APWG. If you do get as far as accessing a site login, though, it's essential to be aware of what sort of authentication is reasonable. Some phishing attempts are outstandingly greedy: the phisher asks for credit card details, PIN, social security numbers, account numbers, pretty much everything that defines your financial/social identity. That should ring a carillon of alarm bells – after all, most people are suspicious of being asked for so much information (especially their PIN, which should never be asked for) - but it's also possible for an attacker to try to aggregate smaller lumps of data into a larger chunk.

And if you do get caught out, here's some good advice from the Federal Trade Commission in the US (<http://www.ftc.gov/bcp/edu/microsites/idtheft/>).

The screenshot shows a Windows Internet Explorer browser window displaying the FTC's Identity Theft site. The address bar shows the URL <http://www.ftc.gov/bcp/edu/microsites/idtheft/>. The page features a dark header with the text "FIGHTING BACK AGAINST IDENTITY THEFT" and "FEDERAL TRADE COMMISSION". Below this are three icons labeled "DETER", "DETECT", and "DEFEND". A red navigation bar contains links for "CONSUMERS", "BUSINESSES", "LAW ENFORCEMENT", "MILITARY", "MEDIA", "REFERENCE DESK", and "EN ESPAÑOL". The main content area is titled "WELCOME TO THE FTC'S IDENTITY THEFT SITE" and includes a section for "DETER-DETECT-DEFEND AVOID THEFT" with a brief description of the site's purpose. Below this, a section titled "IF YOU THINK YOUR IDENTITY HAS BEEN STOLEN, HERE'S WHAT TO DO:" lists two numbered steps: 1. Contacting fraud departments to place a fraud alert, and 2. Closing accounts that have been tampered with or opened fraudulently. A "Hot Links" sidebar on the right contains links for "Become a Partner", "Watch the video", "The President's Identity Theft Task Force", "Deter, Detect, Defend Brochure (PDF 207KB)", and "Take Charge: Fighting Back Against Identity Theft".



Conclusion

Why does phishing work? The technical skills of the criminal are far from being the only relevant factor. Skilful social engineering (offering rewards for information, or scare tactics like “your account has been compromised by a hacker – to re-authenticate, click here”) are also very relevant. However, the phisher’s most potent weapon is the victim’s confusion about the nature of the problem.

Too often in security, we see a problem exacerbated by well-meant but ill-founded advice from a wide range of resources, including some that the everyday user has some right to assume to be authoritative: for example, some of the financial institutions targeted by phishing gangs and law-enforcement agencies. There is still confusion in abundance about the nature of the phishing problem, though more people have become aware of the problem, and the range of technical solutions for dealing with it has increased.

However, it’s important that the legitimate institutions targeted by phishing groups take responsibility for enabling their users to avoid becoming victims:

- By not using bad practice in their communications with their customers that make it easier for phishing gangs to pitch their messages so that they look genuine.
- Never use email to ask for personal identification information such as passwords, usernames, PIN numbers and the like: even if legitimate, it adds to confusion. Not only that, but the insecure nature of standard email makes it unsuitable for transmitting sensitive data.
- By making it easier for customers to get reliable advice and information from customer support facilities and service desks, enabling them to distinguish between genuine and fake communications and sites.

We welcome growing recognition of need for ISPs and other providers to take responsibility for the traffic they carry, and would encourage them to supply or provide pointers to reliable information on phishing issues, as part of their duty of care to customers. Employers may not regard themselves as having the same “duty of care”. Some, however, especially those large enough to provide network services to their employees resembling or analogous to those services supplied by an ISP, may consider it appropriate to offer educational resources as well as technical protection to their staff, if only to avoid the complications that can ensue when an employee is defrauded.

There is no better defense against a threat founded on social engineering and psychological manipulation than the dispelling of ignorance.

David Harley, Andrew Lee

July 2007.



References

1. Robert Slade, "Dictionary of Information Security" (Syngress, 2006)
2. <http://pages.ebay.co.uk/education/spoof/tutorial/>
3. <http://www.millersmiles.co.uk/identitytheft/gonephishing.htm>
4. David Harley: "E-Mail Abuse Internet Chain Letters, Hoaxes, and Spam." <http://www.eicar.org/download/hoax.htm>
5. Daniel Barrett: "Bandits on the Information Superhighway" (O'Reilly, 1996)
6. http://en.wikipedia.org/wiki/Pump_and_dump
7. Charles Mackay, "Extraordinary Popular Delusions and the Madness of Crowds" (Wordsworth Reference, 1995): http://en.wikipedia.org/wiki/South_Sea_Bubble
8. Gary Weiss, "The Mob on Wall Street": <http://www.businessweek.com/1996/51/b35061.htm>
9. Lance James, "Phishing Exposed" (Syngress, 2005)
10. Michael Peel: "Nigeria-Related Financial Crime and its Links with Britain" <http://www.chathamhouse.org.uk/pdf/research/africa/Nigeria1106.pdf>
11. Sorin Mustaca VB Sept 2006
12. Sarah Gordon & David Chess: "Where There's Smoke, There's Mirrors: The Truth about Trojan Horses on the Internet", Virus Bulletin International Conference Proceedings, 1998. <http://www.research.ibm.com/antivirus/SciPapers/Smoke/smoke.html>
13. David Harley, Eddy Willems, Judith Harley: "Teach Your Children Well – ICT Security and the Younger Generation". Proceedings of the 15th Virus Bulletin International Conference, 2005.
14. <http://millersmiles.co.uk/scams.php>
15. <http://www.phishtank.com/stats/2006/10/>
16. Andrew Lee: "Eset warns about IRS Phishing Scam" http://88.208.205.84/joomla/index.php?option=com_content&task=view&id=1341&Itemid=5 (2006)
17. Frank Washkuch Jr: "Phishing scam uses Social Security ploy", <http://www.scmagazine.com/uk/news/article/604182/phishing-scam-uses-social-security-ploy/> (2006)
18. http://english.ohmynews.com/ArticleView/article_view.asp?no=204507&rel_no=1; <http://news.bbc.co.uk/1/hi/technology/4232111.stm>; <http://www.fbi.gov/katrina.htm#vgn-hurricane-katrina-fraud-task-force-vgn>
19. <http://www.millersmiles.co.uk/report/369>
20. National Infrastructure Security Co-ordination Centre: "Targeted Trojan Email Attacks", <http://www.niscc.gov.uk/niscc/docs/ttea.pdf>
21. US-CERT National Cyber Alert System: TA05-189A-Targeted Trojan Email Accounts; <http://www.us-cert.gov/cas/techalerts/TA05-189Apr.html>
22. John Graham-Cumming: The Spammers' Compendium, <http://www.jgc.org/tsc/>
23. John Graham-Cumming: "The Rise and Rise of Image-Based Spam" Virus Bulletin November 2006
24. http://en.wikipedia.org/wiki/DNS_cache_poisoning; <http://isc.sans.org/presentations/>



- dnspoisoning.php; <http://isc.sans.org/diary.php?date=2005-04-07>
25. http://mail-archives.apache.org/mod_mbox/httpd-cvs/200002mbox/%3C20000202180253.12587.qmail@hyperreal.org%3E
 26. http://news.netcraft.com/archives/2006/10/27/myspace_accounts_compromised_by_phishers.html
 27. Christopher Abad: "The Economy of Phishing: a Survey of the Operations of the Phishing Market", http://firstmonday.org/issues/issue10_9/abad
 28. Peter Kruse: CSIS. (<http://www.csis.dk/Media/test-aptools.pdf>); Mozilla: "Firefox 2 Phishing Protection Effectiveness Testing", <http://www.mozilla.org/security/phishing-test>
 29. Cranor, Egelman, Hong & Shang: "Phinding Phish: An Evaluation of Anti-Phishing Toolbars", CyLab, Carnegie Mellon University
 30. Ponnurangam Kumaraguru, Yong Woo Rhee, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Elizabeth Nunge: "Protecting People from Phishing: the Design and Evaluation of an Embedded Training Email System", CyLab, Carnegie Mellon University, November 9 2006.
 31. David Harley & Andrew Lee: "Phishing Phodder: Is User Education Helping or Hindering?" in "VB2007 Conference Proceedings" (Virus Bulletin, 2007)
 32. David Harley et al: "AVIEN Malware Defense Guide for the Enterprise" (Syngress, 2007)



Glossary

Bcc (Blind Carbon Copy)	Email receiver field: recipients listed in the Bcc field are not shown in the copies sent to the primary recipient(s) in the To field, or to the secondary recipient(s) in the Cc (Carbon Copy) field. This terminology dates back to typewritten business letter practice, of course.
Bot herder, botmeister	Someone who controls a botnet for diverse criminal or malicious purposes such as spam distribution, malware distribution, and DDoS orchestration.
Botnet	Network of bot-compromised/infected systems under the control of a bot herder.
Cybersquatting	Registration of a domain with the intention of benefiting in some way from a perceived but deceptive or malicious association between the registrant and a legitimate site or business.
DDoS	Distributed Denial of Service attack: a DoS attack amplified by delivering it through a network of compromised systems, nowadays usually a botnet.
DoS	Denial of Service attack: an attempt to prevent a computer system from functioning normally. Frequently associated with extortion: the criminal threatens to prevent systems from functioning so that the victim organization cannot carry out its normal business.
Hashbuster	Some spam filters use a database of "hashes" to identify spam messages: these are a kind of "fingerprint" of a message: an MD5 hash, for instance, represents a string or message as a sequence of 32 hexadecimal digits. (This kind of hash is often referred to as a Message Digest.) A more secure family of hash algorithms is the SHA (Secure Hash Algorithm) group of hash functions. Hashes have a variety of uses in security. It has long been common for spammers (among others) to include random text in the subject or body of a message, so as to generate random changes from one spam iteration to another, thus throwing off filters that rely on checksums or hashes (not exactly the same thing). More recently, similar techniques have been applied to image spam.
Keylogger	As applied to phishing, a form of spyware or Trojan that records a computer user's keystrokes without his or her knowledge and passes the information on to a criminal, bot herder etc.
Lottery scam	Advance fee fraud that works by telling the victim they've won a huge amount of money, but have to pay some money upfront before they can receive it.



Mule	In organized crime, the term has a number of meanings, including someone who's used as a courier for drugs, money etc. In phishing, usually refers to someone who is involved with money laundering by receiving and forwarding fraudulently acquired funds, goods or services.
Multi-Level Marketing (MLM)	A legitimate business model which may have a hierarchical/pyramidal structure, but is not a pyramid scheme.
Pennystox, Penny Stocks, Small Caps	Businesses with low initial stock values characteristically victimized by criminal groups executing pump and dump schemes.
Phising	An alternative term for phishing sometimes encountered: the etymology is uncertain, but may be due to misunderstanding of the etymology of the term "phishing" in combination with erratic typing skills)
Pump and Dump (Hype and Dump)	A form of stock fraud in which the value of stock is artificially inflated so that dishonest speculators can make a profit by selling off when the price is high. This works well for the scammer, but not for the (usually small) company, or for the scam victims whose contribution to the raising of stock value is typically rewarded with heavy losses when the scammer sells the stock and stops hyping.
Pyramid Scheme	Scam in which new entrants pay for the chance to move towards the top of a pyramid and take a cut out of payments towards later entrants. The appeal of the the scheme is based on the improbable premise that the scheme will continue to attract entrants indefinitely, so at best the major returns on the scheme go to the initiator and, maybe, the earliest entrants. Participation in such schemes is illegal in some jurisdictions.
Social Engineering	Term applied to a wide range of techniques for causing a desired change in behavior or gaining some advantage by psychological manipulation of an individual or group. The term actually derives from social science, where it doesn't necessarily have a negative connotation, but as used in security it almost invariably involves some form of deception, malice or fraud.
Spyware	More or less generic term for a range of malware such as keyloggers, Remote Access Trojans, backdoor Trojans and so on. Malware used for frankly criminal activities such as phishing may also be referred to as crimeware.



Tsunami scams	A range of charity scams and hoaxes allegedly raising funds for victims of the 2004 tsunami. Examples include many 219s and phishing mails. [Harley: UK CERTs presentation]
Vishing	The use of VoIP as a vector for phishing attacks: approaches used include directing the victim to a spoofed phone number to verify sensitive data, as well as directly approaching the victim. The moral? Phone numbers in emails are no safer than URLs.
VoIP	Voice over IP: telephony and related services that work over the Internet rather than over older messaging media and protocols.



Corporate Headquarters

ESET, spol. s r.o.
Aupark Tower
16th Floor
Einsteinova 24
851 01 Bratislava
Slovak Republic
Tel. +421 (2) 59305311
www.eset.sk

Americas & Global Distribution

ESET, LLC.
610 West Ash Street
Suite 1900
San Diego, CA 92101
U.S.A.
Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400
Fax. +1 (619) 876-5845
www.eset.com



© 2009 ESET, LLC. All rights reserved. ESET, the ESET Logo, ESET SMART SECURITY, ESET.COM, ESET.EU, NOD32, VIRUS RADAR, THREATSENSE, THREAT RADAR, and THREATSENSE.NET are trademarks, service marks and/or registered trademarks of ESET, LLC and/or ESET, spol. s r.o. in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.

