



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

# **Phishing:**

## **An Analysis of a Growing Problem**

**Anthony Elledge**

GIAC Security Essentials Certification (GSEC) Practical  
Version 1.4b, Option 1

May 3, 2004

## Abstract

Email has become an invaluable communication tool for both business and personal use. Among the many security issues that now affect computer users, there is a growing threat known as “*phishing*”. Phishing attacks are perpetrated by criminals who send deceptive emails in order to lure someone into visiting a fraudulent web site or downloading malicious software, expressly for stealing sensitive information such as credit card numbers, account information, passwords, etc.

This paper gives an in-depth analysis of what phishing is, the technologies and security risks it takes advantage of, the dangers it can pose to end users, and gives some insight into what might be done to curb the effects of these schemes.

## 1 - Introduction

You receive an email from your credit card company informing you that your account has been deactivated because of suspicious activity. You are requested to click on a link and verify your account information. Following the instructions, you click on the link, and are taken to what appears to be your credit card company’s “Online Update” page. Here you are prompted to enter your name, password, account number, social security number, and PIN. It all looks legitimate: the logos are correct, the web address of the page looks convincing, the format of the site is the same as you remember. The only problem is, this is a scam; the email is a fraud and now a cyber-criminal has your personal information and can begin using or changing your account, or opening new accounts in your name. You have become a victim of a growing crime called phishing.

Everyday, millions of emails are sent around the globe, and millions of web pages are accessed to gather information. We, as the users of email and the Internet, endeavor to trust the systems that are in place to deliver these messages and to route us to the proper servers to access the information we need. We expect that emails delivered to us from “reputable” sources are legitimate and offer information to assist us in our business or personal life. Unfortunately, there is a growing group of cyber-criminals using and abusing these same systems in order to steal our private information; they take advantage of people’s trusting nature, or, in some cases, their naiveté.

In this analysis I will explain the concepts and technology behind phishing, show how this threat is much more than just a nuisance or passing trend, and how gangs of criminals are using these techniques to make a great deal of money (and are getting more and more sophisticated). I will give some hints and suggestions about how users can protect themselves from these scams by using defense-in-depth techniques, and explain some of the technologies being developed to combat the serious threat of identity theft and online fraud.

## 2 - What is Phishing?

Phishing, otherwise known as “brand spoofing” or carding, is an online scam whereby emails are sent by criminals who are out for nothing other than to steal your identity, rob your bank account, or take over your computer. Counterfeit web sites are created to lure the unsuspecting to divulge information that they would normally not want to be public knowledge. These digital thugs are ‘*phishing*’ for information they can use to prey on unsuspecting computer users and further their criminal activities.

The Anti-Phishing Working Group (APWG) states that the term *phishing*, “comes from the analogy that Internet scammers are using email lures to ‘fish’ for passwords and financial data from the sea of Internet users” [2]. Apparently, the “*ph*” was used as a tribute to the term “phone phreaking”, a technique used in the early days of hacking to take advantage of security weaknesses in the phone systems. The term is used to describe the use of “spoofed” or hoax emails and fraudulent web sites in order to fool users into revealing personal data [1].

The concept of phishing has actually been around for years. Original phishing was a term used by hackers to describe stealing America Online® (AOL) accounts by acquiring usernames and passwords. With the ubiquitous spread of email and internet access, the ability of criminals to take advantage of the technology has increased significantly in the past several years, with an almost exponential increase in incidents since 2003, according to many organizations that are trying to track this trend. Flaws in email protocols, security weaknesses in browser software, and a lack of basic computer security education have all contributed to the increase in incidents as criminals are able to exploit these problems to their advantage.

## 3 - The Threats from Phishing

The biggest threat of phishing scams is identity theft. Consumers go to great lengths to protect their personal information, and any breach of that protection can open one up to many threats, including credit card fraud, damaged credit, having an identity used for other criminal activity, stolen bank accounts, unauthorized use of accounts (online and otherwise), or stolen money. There are also intangible threats, such as damage to credibility, loss of trust, or embarrassment; having personal information stolen can cost a great deal more than lost cash. According to The Identity Theft Resource Center, the average time spent repairing the damage caused by a stolen identity is approximately 600 hours and can take years to completely recover [8]. For consumers, this can equal lost salary, lost time, frustration, stress, and embarrassment, not to mention a sense of being violated.

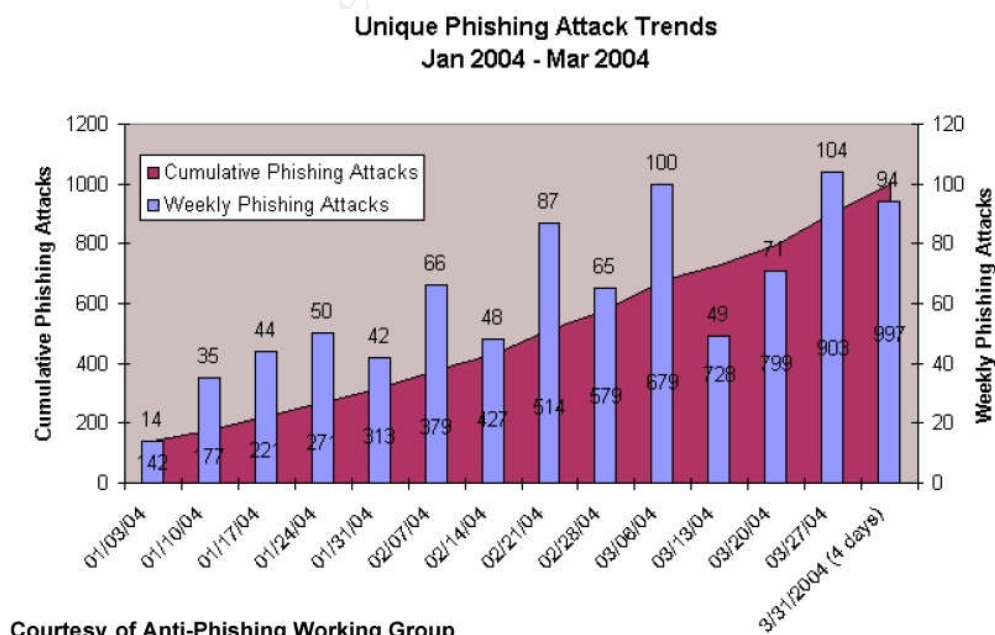
Phishing is not just a “small-time” operation. There are reports of gangs of phishers organized in Eastern Europe and Asia that are believed to be devising sophisticated and elaborate schemes in order to steal personal information. According to MessageLabs, a secure messaging service provider, many of the

phishing scams are originating in Russia and there is speculation that Russian organized crime may be involved. There is a lot of money at stake, and if a gang can steal bank account information from only a small percentage of those who get duped by the hoax emails, then thousands (or possibly millions) of dollars can be stolen. This is a very real threat, not only to consumers, but also to the companies that are targets of these scams.

Companies that are spoofed (used fraudulently) may be poised for all matter of losses. They can lose money in the form of stolen cash, lost productivity, reimbursements to customers, or they may possibly lose customers who believe the company is partly to blame for not protecting them (no matter how unfounded this may be). Scams can erode consumer confidence in companies that are targets of the schemes (especially high-profile ones), leaving the company with somewhat of a public-relations nightmare, and a company's branding has a real possibility of become irrevocably tarnished.

There are now instances of legal action being taken against companies for losses by customers. Whether or not the litigation is successful, the damage to the company's image and the cost of legal fees can be substantial. Some companies are now offering complete compensation to customers whose accounts may be abused. While this may be a good customer-relations tactic, with phishing attacks on the rise, this could cost a great deal to a high-profile company such as Amazon.com® or Bank of America®, especially if they have a substantial number of claims.

The number of phishing attacks has increased exponentially over the past few months, according to the APWG. Increasingly sophisticated techniques are being used and more devious attacks being developed. The following chart depicts the number of new schemes reported to the APWG between January and March 2004:



According to MessageLabs, in September 2003, the number of individual phishing emails seen by the company was 279; by March 2004, this had risen to 215,643 [25]. With this level of increase, coupled with the increase in sophistication, the threat to consumers and businesses is significant.

A threat that many experts are growing more concerned about is the level of trust consumers have in email, online commerce, and the companies they deal with online. Many institutions have stopped communicating with customer's via email altogether to help eliminate the possibility that the user may become a victim of phishing. This seems to point to a disturbing consequence of the increase in all forms of online fraud, not just phishing: if consumers become wary of using email and the Internet, then online commerce might begin to suffer, according to many experts. Could this point to a sea-change in the way online banking and commerce is implemented?

#### 4 - The Attack

A typical phishing scheme involves a criminal or criminals sending spam email messages to thousands or even millions of email addresses. These hoax emails are forged (spoofed) with a "From" or "Reply to" address that makes them appear to have come from a reputable source, such as a bank or credit card company. The messages are oftentimes sent in Hyper-Text Markup Language (HTML) format and may use logos, Uniform Resource Locators (URL), legal disclaimers, etc., that have been taken from the spoofed company's website. This makes the attack all the more insidious since the average user may not question an email if it appears to have come from his or her bank and has that bank's logo on it.

Phishers play the odds when sending their mass-mailings. Of the thousands of messages sent, only a small percentage of the recipients may actually be a customer of the spoofed company. For instance, if the phisher has spoofed PayPal®, an online payment company, the number of emails sent to actual PayPal® customers who then may fall for the scheme might be relatively small; however, it is estimated that around five percent of the phishing emails sent actually are successful [1]. This can result in quite hefty profits for the scammers.

There have been many different variations of phishing scams, but the email messages are usually structured to prey, ironically, on the user's fear of being a victim of fraud or hacking, or may be a message stating that the company needs to update the user's records:


*"Our records show your account information is out of date. Please click on the following link and confirm your information" ...*

When the victim clicks on the link, their browser will open a web site with a URL that may be very similar to the one they would expect. This is another ploy used by phishers: registering domain names with similar looking addresses or using

character replacement (using the number “1” for the lowercase letter “L” for example) to disguise that the address is phony. Many people could be fooled since they may not notice the difference in the address. The URL may also be displayed within the email as the legitimate address (e.g., www.aol.com), but another web address—the phony phisher address—has been embedded using deceptive techniques (explained later). The victim may be taken to a site that looks, for all intents and purposes, the same as their bank, or eBay®, or AOL®, with the same icons, graphics, and text. The fraudulent site is setup to display an interface where the user enters his or her information, thinking they are entering it at the company’s web site.

Some of the more well-known and publicized phishing scams of late have involved some high-profile sites such as eBay® and PayPal®. Scammers use company logos and designs to make the messages look legitimate. The message may tell the user that money needs to be transferred or that their account is out of date and needs to be modified. When the user clicks on the link, they are taken to what they believe to be the legitimate web site and asked to enter surprisingly personal information, such as their bank account or social security number or other sensitive information. The scammers capture this information and then use it to steal the victim’s identity or fraudulently use accounts.

Account Update with eBay Auction Community

 Update Your Account Information Within 24 Hours

Valued eBay Member,

**You (or someone else) entered three times the wrong password to log in with your eBay ID.**

According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be suspended within 24 hours for investigations.

**Never share your eBay password to anyone!**

Establish your proof of identity with ID Verify (free of charge) - an easy way to help others trust you as their trading partner. The process takes about 5 minutes to complete and involves updating your eBay information. When you're successfully verified, you will receive an ID Verify icon in your feedback profile.


**All fields below are required. Please double check before you click Submit button**

Enter Your Registration Information

User ID	<input type="text" value="eww"/>
Password	<input type="password"/>
Account type	<input type="checkbox"/> Seller <input type="checkbox"/> Buyer
Name	<input type="text" value="First Name"/> <input type="text" value="M.I."/> <input type="text" value="Last Name"/>
Email address	<input type="text"/>
Email password	<input type="password"/>
City	<input type="text"/>
State/Province	<input type="text" value="Select State"/>
Country	<input type="text" value="USA"/>
Primary phone #	<input type="text" value="for example, (415) 555-0304"/>
Secondary phone # (optional)	<input type="text"/>
Fax # (optional)	<input type="text"/>

[Announcements](#) | [Register](#) | [Safe Trading Tips](#) | [Policies](#) | [Feedback Forum](#) | [About eBay](#)

Copyright© 1995-2003 eBay Inc. All Rights Reserved.  
Designated trademarks and brands are the property of their respective owners.  
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#)



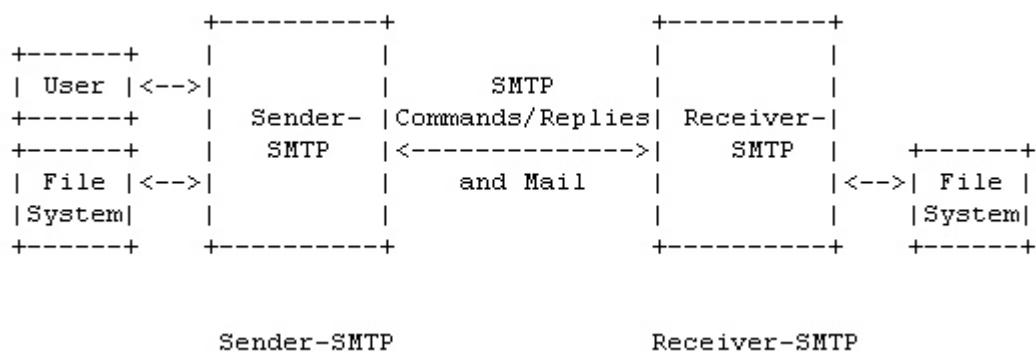
Spoofed eBay web page. Courtesy of MillersMiles.  
(<http://www.millersmiles.co.uk/identitytheft/042804-eBay-Important-Account-Information.php>)

## 5 - A Technical Background

To understand how phishing works and why it is so easy to perpetrate, a bit of technical background regarding the protocols, technology, and tactics behind the schemes may be helpful. The following are some of the main elements related to phishing attacks:

Simple Mail Transfer Protocol (SMTP) – This is the protocol used to transmit email over the Internet. It was originally described in a Request for Comments (RFC) by Dr. Jonathan Postel in 1982 (RFC 821). According to the RFC, “The objective of Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently” [13]. Notice that it doesn’t include “securely” in that statement. SMTP has no built-in security measures to authenticate who is sending an email. All it does is communicate with the SMTP server on the receiving side, in essence, telling the other system “who” it is, who the email is from (sender), and who the email is for (recipient). There is no guarantee that the sender of the email is legitimate or if the address is spoofed.

The sending SMTP server initiates a MAIL command to the receiving SMTP server. This MAIL command indicates the sender of the email. The receiving server will reply if it is able to receive mail and if a user with the specified address is a user on that system. The sending server then transmits a RCPT command to identify the recipient of the email [13]. The two systems negotiate back and forth until the message is delivered at which time the transmission is complete and the servers say “ok” and “goodbye”, so to speak. Nowhere is there any validation as to the existence of the sender of the message. Companies are working to make email protocols more secure; however, for the near future, this is what we have to work with.



The SMTP Model.

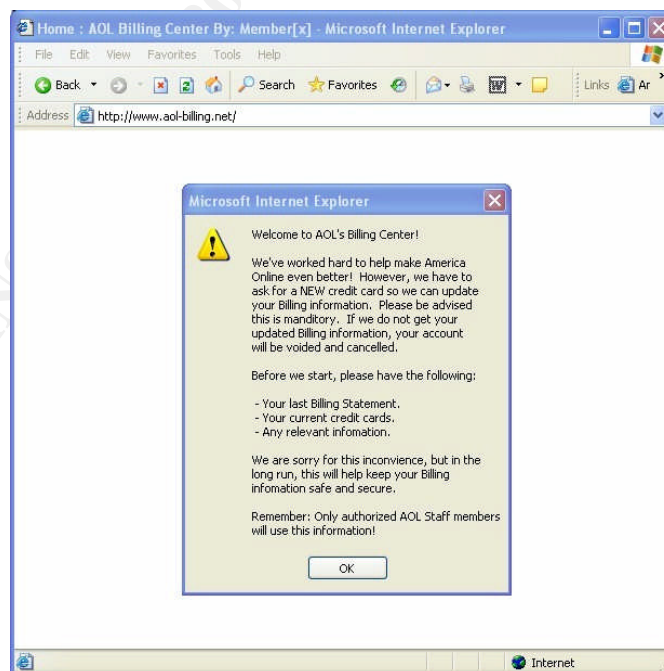
(Courtesy of The Internet Engineering Taskforce, <http://www.ietf.org/rfc/rfc821.txt>)

HTML-based Email – Email messages can be transmitted as either plain text, with no graphics or formatting, or they may be formatted as mini web pages, capable of displaying graphics, formatted text, even able to run scripts. This

makes phishing a much easier task. For this reason, phishers usually send their hoax emails in HTML format, embedding graphics and formatted text to make the email look more like a legitimate communication from the spoofed company. Logos, banners, even ads are placed within the email to entice the recipient to believe that the message is authentic. If the message were in plain text, with only a URL link, the user *may* become more suspicious and less likely to click on it.

**HTML Forms** – A new scheme involves using HTML-based forms within an HTML-formatted email. The code in the form is hidden; therefore, the phisher is able to hide a bogus URL in a Submit button that the user presses after entering his or her personal information. As a result, it is more likely that the casual user will be enticed by a form-based attack [11].

**Domain Naming System (DNS)** – DNS is the hierarchical “database” that converts numerical Internet Protocol (IP) numbers to human-readable names. When you type in [www.somesite.com](http://www.somesite.com) the name is associated with the IP number and takes you to the server at that address. There are several security issues with DNS. Cyber-criminals may be able to “hijack” a domain, redirecting traffic from the legitimate site to a malicious site that is setup to look identical to that site, or (more easily) they can create a totally new domain name that looks so similar that an unsuspecting user may not notice the difference. A recent incident involved a phishing scam that came from the domain [www.aol-billing.net](http://www.aol-billing.net), a fraudulent domain name entirely unassociated with America Online, but it appears convincing to an unsuspecting user.



Fraudulent AOL billing web site. Courtesy of Anti-Phishing Working Group ([http://www.antiphishing.org/phishing\\_archive/aol\\_03-10-04.htm](http://www.antiphishing.org/phishing_archive/aol_03-10-04.htm))

*Trojan Horse* – A Trojan Horse is a malicious software program (malware) that masquerades as legitimate software. This malware can be installed by worms or viruses such as the recent Mimail virus, or unknowingly by the user thinking the software is a game or utility or browser plug-in. It may also be installed via Internet Relay Chat (IRC) sites. More sophisticated phishing scams are using Trojans to install keystroke loggers to capture a user's passwords and account numbers, or install programs to take screenshots of the system. These images may have usernames, passwords, or credit card numbers that are then forwarded to the phisher.

*Browser Insecurities* – There are security holes in some web browsers that can make a phisher's crime easier to accomplish. A recent incident involved a security issue in Microsoft® Internet Explorer. The glitch allows a specially crafted URL to load a browser window that appears to be displaying any address the attacker wants [19]. The attacker embeds a URL into an email using the form:

`http://www.sometrustedsite.com%01%00@malicious-site.com/malicious.html` [23]

When the user moves his cursor over the link, it appears to be a link to `www.sometrustedsite.com`; however, when clicked, it takes him to `malicious-site.com`, where a fake web page has been set up. This hole was eventually fixed by Microsoft, but it may only be a matter of time until another hole is found that will allow some other type of fraud.

*Malicious Javascript* – One of the most sophisticated techniques discovered to-date, according to the Anti-Phishing Working Group, involves the use of JavaScript to create a fake browser address bar. This scam bypasses the need for taking advantage of the Internet Explorer security hole which allows disguised URL's to be embedded within the email (see Browser Insecurities above). The JavaScript displays a fake Address bar in the browser that cannot be discerned from the real one. When a user types in an address, the malicious code can route them to the fraudster's web site. This technique reportedly affects multiple browsers.

*Social Engineering* – One of the most effective tools in the phisher arsenal is the ability to fool someone into divulging personal information—this is social engineering. Social engineering is a method used to make a person believe they are dealing with a legitimate person or company, when in fact they are not. The hoax emails used in phishing schemes purport to be from a trusted entity, so the user is more likely to trust its contents. Social engineering can be a very successful ploy, not only for phishing scams, but for other criminal activities as well.

## 6 - What Can Be Done?

Many experts contend that phishing is less of a “technology problem” and more of a “user problem”; that the responsibility ultimately lies with the user being aware of where they are browsing, what information they are giving over the Internet, and to whom they are giving the information. Others are becoming more concerned that the sophisticated techniques used by phishers are becoming more difficult to detect, even for experienced computer users; casual or less-technical users are much less likely to be able to discern a legitimate email, web address, or web site from a fake one. Social engineering ploys can be very effective in these situations.

### Education

Education is, indeed, a vital component of battling phishing—as well as other online scams. The Federal Trade Commission suggests some things to remember:

*(paraphrased from <http://www.ftc.gov/bcp/online/pubs/alerts/phishregsalert.htm>)*

- Don't reply to emails asking to confirm account information. Call or logon to the company's web site to confirm that the email is legitimate.
- Don't email personal information. When submitting information via a web site, make sure the security lock is displayed in the browser.
- Review credit card and bank account statements for suspicious activity
- Report suspicious activity

The Department of Justice recommends that users Stop, Look, and Call [26]:

*(paraphrased from [http://www.antiphishing.org/doj\\_special\\_report\\_on\\_phishing\\_mar04.pdf](http://www.antiphishing.org/doj_special_report_on_phishing_mar04.pdf))*

- Stop: Don't react to phisher ploys of “upsetting” or “exciting” information
- Look: Look closely at the claims in the email. Also look at the links and web addresses
- Call: Call or email the company in question to verify if the email is legitimate

Computer users should try, if possible, to keep abreast of computer security issues in the news, and use common sense when giving information anywhere: online or otherwise. If an email (or phone solicitor or web site, etc., etc.) asks for personal information, that should be an immediate red flag that something may not be legitimate and needs to be confirmed. Legitimate companies will generally not solicit personal information via email. If personal information is

requested via a web site, the user should make certain he or she is connected to the proper site and that the communications are encrypted.

## Technology

Unfortunately, phishing usually involves social engineering tricks, and, thus, even the best defenses that a company might have in place to combat outside threats are sometimes useless against these types of attacks. Although education is likely the best defense against phishing scams, there are technologies that make phishing harder to accomplish. When implemented with a defense-in-depth approach, software and hardware can be installed to slow the phishers down.

### *Two-factor Authentication:*

One of the more promising technologies to thwart phishing schemes involves two-factor authentication. This method uses a layered approach to validate a user's credentials by using two separate methods to verify a user. A two-factor authentication technique, currently being offered, uses one-time passwords that expire after a single use. These passwords are generated using a shared electronic key between the user and a bank. A login is authenticated by not only the user's credentials (username/one-time password), but also the key that generates the password. If a password does happen to get stolen, it will not matter since it expires after a single use.

### *Firewalls:*

There are email firewall products that implement rules to block spam and phishing scams at the perimeter. These products offer "heuristic" rules that are updated as new phishing schemes are found. They not only block the spam, they verify the IP numbers and web addresses of the email source and compare them to known phishing sites. For larger organizations, this can be an effective defense against spam and phishing.

### *Anti-virus Technology:*

Though phishing scams are usually not considered a "viral" problem, if a user is infected with a worm that, in turn, installs a Trojan that can capture personal data, then anti-virus technologies are effective. Security best-practices direct that all users should implement an anti-virus product regardless of whether they are concerned about phishing or online fraud.

### *Digital Certificates:*

Security begins with establishing trust between a user and a web site. Digital certificates are a way to establish this trust in the form of an encrypted digital key

system. A public and private key structure is established whereby a company has a private key, obtained from a Certificate Authority (CA), and a user who wishes to make secure transactions obtains the corresponding public key from the company. When the user logs into the company's server, the keys have to match or the transaction will not be processed. The problem with this method is that the private keys could be stolen if not kept completely secure. If the private key is compromised, then a hacker could use the digital key to masquerade as the key's owner.

### *Secure Email Protocols*

There is currently a push within the industry to modify the existing email transport protocols and include built-in security at this lower level. Validating the identity of the originating sender of a message would go a long way in preventing phishing attacks. There are encryption methods for sending email, but many believe they are difficult for the average user to implement. Built-in encryption may eliminate the need for using separate encryption methods, allowing transparent authentication for the user. It would also eliminate the possibility of keys being stolen or hacked, thus allowing an attacker to decrypt secure messages. Several companies are working on this, but it may be years before something is available.

### *Communication:*

Companies need to communicate with their customers to keep them apprised of scams or other threats. They should make policies clear and make sure the customers are aware of how information will be gathered and disseminated.

### *Defense-in-Depth*

To be secure, a defense-in-depth approach should be put in place. Users and companies need to be educated about the scams and risks, authentication methods need to be employed, firewalls should be in use, anti-virus technologies should always be installed, companies should communicate with their customers, and digital certificates and other encryption schemes should be implemented. When these layers of protection are utilized, the chance of a phishing attacks being successful is greatly reduced.

### Companies Need to be Prepared

Regardless of education or technology put in place, companies need to be prepared for the impacts of phishing and other online fraud attacks. Costs related to reissuing credit cards, re-establishing accounts, reimbursing customers for losses, and possible litigation, are just a sampling of costs a company may

have to absorb. These costs could possibly become quite significant, especially if hundreds of accounts were compromised.

Many experts suggest that companies have disaster recovery plans in place to cover phishing attacks, similar to plans that cover any type of digital security breach or a natural disaster. Recovering from a large-scale phishing scam could, in theory, be detrimental to a company's revenue and to its customer's trust.

## **7 - Conclusion**

Phishing scams can pose a significant threat to consumers and the companies they deal with. The number of online scams has increased significantly, and the techniques the criminals employ have become more and more sophisticated. These and other online cons show little sign of slowing. On the contrary, scams are on the rise, and companies and individuals need to be aware of the consequences.

There is no "magic bullet" or "pixie dust" that can make these threats go away. No single technology can keep fraudsters at bay and keep our personal information completely safe. There are ways to make the crimes a bit harder to accomplish, but a well-crafted phishing attack has a significant chance of being successful. There will have to be more done to stop the spread of these attacks and make them unprofitable and less appealing for the would-be phishers.

More research and development of anti-fraud technologies, more education of computer users, and aggressive prosecutions of the criminals who perpetrate these loathsome acts will go a long way to curb the threat, but these alone will most likely have little impact in the number of schemes. Consumers need to become more educated concerning online threats and vulnerabilities. Companies need to make sure that online fraud and scams are reported and that their customers are kept apprised of scams that may affect them. The security community needs to work to find new ways to make email and online commerce as bullet-proof as it can possibly be. This is a monumental task, but there are a lot of extremely talented people with a lot of extremely brilliant ideas out there. If something is not done, the way we do business online will change, and almost certainly not for the better.

© SANS Institute

## List of References

1. The Anti-Phishing Working Group. "What is Phishing?"  
URL: <http://www.antiphishing.org/> (March 2004)
2. The Anti-Phishing Working Group. "Origins of the Word Phishing."  
URL: [http://www.antiphishing.org/word\\_phish.htm](http://www.antiphishing.org/word_phish.htm) (March 2004)
3. Author Unknown. "How to Obscure any URL". PC-Help. January 2002.  
URL: <http://www.pc-help.org/obscure.htm> (March 2004)
4. Library of Spoof Email Hoax Scams and Fake Web Pages. MillersMiles.  
URL: <http://www.millersmiles.co.uk/identitytheft/spoof-email-and-spoof-web-page-library.htm> (April 2004)
5. Bright, Mat. "Spoof Email Phishing Scams and Fake Web Pages or Sites. Part 1". February 2004.  
URL: <http://www.millersmiles.co.uk/identitytheft/gonephishing.htm> (April 2004)
6. Bright, Mat. "Spoof Email Phishing Scams and Fake Web Pages or Sites. Part 2". February 2004. URL: <http://www.millersmiles.co.uk/identitytheft/oah-2.htm> (April 2004)
7. Bright, Mat. "Remember the Phone Phreaks?" February 2004.  
URL: <http://www.millersmiles.co.uk/identitytheft/phishing.html> (April 2004)
8. The Identity Theft Resource Center. Identity Theft Facts and Statistics. February 2004. URL: <http://www.idtheftcenter.org/facts.shtml> (April 2004)
9. Gelles, Jeff. "Consumer Watch: 'Phishing' Scams Continue to Bite". March 27, 2004. URL: [http://www.philly.com/mld/philly/business/columnists/jeff\\_gelles/8288622.htm](http://www.philly.com/mld/philly/business/columnists/jeff_gelles/8288622.htm) (April 2004)
10. Hurst, Pat. "Millions at Risk from Cyber 'Phishing' Gangs". February 29, 2004.  
URL: <http://www.crime-research.org/news/29.02.2004/95> (April 2004)
11. Glenbrook Partners Consulting. "Phishing". Customer briefing. February 23, 2004. URL: <http://www.paymentsnews.com/2004/02/phishing.html> (April 2004)
12. Dvorak, John C. "Gone Phishing. Scams for Personal Information Are Getting Worse". April 15, 2004. URL: [http://abcnews.go.com/sections/scitech/ZDM/phishing\\_commentary\\_pcmag\\_040415.html](http://abcnews.go.com/sections/scitech/ZDM/phishing_commentary_pcmag_040415.html) (April 2004)

13. Postel, Jonathan B. "Simple Mail Transfer Protocol". RFC 821. August 1982. URL: <http://www.ietf.org/rfc/rfc821.txt> (April 2004)
14. Trinity Security Services. "Identity Thieves go PHISHING". January 31, 2004. URL: <http://www.itsecurity.com/papers/trinity14.htm> (April 2004)
15. Jack, Rodney. "Online Phishing Uses New Bait". April 6, 2004. URL: <http://www.vnunet.com/News/1154101> (April 2004)
16. Columbo, Jon. "Bugwatch: Foiling Phishers". April 7, 2004. URL: <http://www.vnunet.com/News/1154148> (April 2004)
17. Moulds, Richard. "Whose Site is it Anyway?". March 29, 2004. URL: <http://www.net-security.org/article.php?id=669> (April 2004)
18. Barrett, Jennifer. "Phishing Fallout". April 15, 2004. URL: <http://msnbc.msn.com/id/4741306/> (April 2004)
19. Gray, Patrick. "IE Bug Provides Phishing Tool". December 10, 2003. URL: <http://news.zdnet.co.uk/internet/security/0,39020375,39118421,00.htm> (April 2004)
20. Gonsalves, Antone. "Latest Trojan Phishing for Personal Data". January 16, 2004. URL: <http://www.techweb.com/wire/story/TWB20040116S0007> (April 2004)
21. Lemos, Robert. "New Mimail Mixes Tricks for Paypal Scam". January 16, 2004. URL: <http://news.com.com/2100-7349-5142647.html> (April 2004)
22. Festa, Paul. "IE Bug Lets Fake Sites Look Real". December 10, 2003. URL: <http://news.com.com/2100-7355-5119440.html?tag=nl> (April 2004)
23. Secunia Advisories. Internet Explorer URL Spoofing Vulnerability. February 2, 2004 (Last update) URL: <http://secunia.com/advisories/10395/> (April 2004)
24. Author Unknown. "Phishing Tackle". January 12, 2003. URL: [http://www.cbronline.com/cbr\\_archive/538daca4f949786480256e12004a1d48](http://www.cbronline.com/cbr_archive/538daca4f949786480256e12004a1d48) (April 2004)
25. Author unknown. "Huge Surge in Phishing Scams As Fraudsters Seek Financial Gain". April 21, 2004. URL: <http://www.message-labs.com/news/virusnews/detail/default.asp?contentItemId=850&region=america> (April 2004)

26. Criminal Division, Department of Justice. "Special Report on Phishing". March 2004. URL: [http://www.antiphishing.org/doj\\_special\\_report\\_on\\_phishing\\_mar04.pdf](http://www.antiphishing.org/doj_special_report_on_phishing_mar04.pdf) (April 2004)
27. News Release. "Tumbleweed announces new release of email firewall to stop email phishing scams and improve anti-spam effectiveness". October 28, 2003. URL: <http://www.itsecurity.com/tecsnews/oct2003/oct277.htm> (April 2004)
28. Federal Trade Commission Consumer Alert. "Is Someone "Phishing" for Your Information?". March 2004. URL: <http://www.ftc.gov/bcp/online/pubs/alerts/phishregsalrt.htm> (April 2004)
29. SANS Security Essentials Training. December 2003.

© SANS Institute 2004, Author retains full rights.