

June 2004



Title: How to best eliminate the threat of Phishing risks.

1 Introduction

Phishing is a form of internet scam in which the attackers try to trick consumers into divulging sensitive personal information. The techniques usually involve fraudulent E-mail and web sites that impersonate both legitimate E-mail and web sites. Some of the most popular sites to impersonate are eBay, Pay Pal and Citi Bank. The fraudulent E-mails can be considered a malicious form of unsolicited bulk E-mail generally known as “spam.”

Consumers are vulnerable to identity theft and some financial losses through fraudulent transactions. Financial institutions are at risk for large numbers of fraudulent transactions using the stolen information. Phishing attacks are often very large-scale events that target thousands of consumers, or more, in the hope that a percentage will be tricked into responding.

A relatively large percentage of recipients do respond to the E-mails since they appear legitimate and their authenticity cannot be checked easily. Estimates of the response rates vary between 1% and 20%, depending on the attack. Attackers can easily copy images, links, and text from legitimate web sites to make the Email appear authentic. Due to the scale of the attacks, there is the potential for huge financial loses. Some attacks involve one million or more phishing E-mails.

As noted by the Anti-Phishing Working Group [APWG], customers of many banks and financial institutions have been the targets of phishing attacks. The objectives have generally been credit and debit card account numbers and PINs. Customers of other businesses have also been targeted for identity theft operations. The phishing threat is increasing rapidly. As reported by the APWG, 176 unique new phishing attacks were reported in January 2004, amounting to 5.7 new attacks per day. This is a 52% increase over December 2003. Customers of financial institutions, retail companies, and internet service providers were frequent targets.

Many different organizations and companies have proposed basic changes in the E-mail infrastructure to help alleviate spam, which would eventually help reduce problems with phishing. The Anti-Spam Research Group, under the Internet Research Task Force, is one such organization [ASRG]. Until those changes are made, financial institutions and their customers can take steps to help reduce the risk of phishing attacks. Those steps include stronger authentication for electronic transactions, more widespread deployment of anti-spam, anti-virus, personal firewall products, and deployment of privacy protection software. Our proposed remedies assume that businesses and consumers will continue to use some form of current hardware and software for many years to come. Therefore, our proposed remedies are compatible with popular consumer and business products, including existing web browsers and servers, E-mail applications and servers, and standard operating systems. In the near future, businesses are unlikely to change their standard forms of identity verification, such as social security numbers and mother’s maiden name. We propose to make it more difficult for attackers to collect this information. This white paper provides an overview of the stages in a typical phishing attack. We also propose a set of “best practices” for institutions and their customers to minimize the impact of future phishing attacks.

To demonstrate an example of what lengths the phishers will resort to in their attempts to confuse the consumer, below is a record of a real phishing attack on Pay Pal on May 7, 2004. It is easy to see the domain name secured could be confusing to the consumer when content is taken from the real Pay Pal web site.

Paypal-supports.com

Domain Name..... paypal-supports.com	Admin Name..... Amy Gross	Tech Name..... Hostmaster Hostmaster
Creation Date..... 2004-05-05	Admin Address..... 2649 Lake Drive #8	Tech Address..... 1375 Peachtree St.
Registration Date.... 2004-05-05	Admin Address.....	Tech Address..... Level A
Expiry Date..... 2006-05-05	Admin Address..... Singer Island	Tech Address..... Atlanta
Organization Name.... Amy Gross	Admin Address..... 33404	Tech Address..... 30309
Organization Address. 2649 Lake Drive #8	Admin Address..... FL	Tech Address..... GA
Organization Address.	Admin Address..... UNITED STATES	Tech Address..... UNITED STATES
Organization Address. Singer Island	Admin Email..... nuclearz0r@hotmail.com	Tech Email..... hostmaster@earthlink.net
Organization Address. 33404	Admin Phone..... +1.5618813060	Tech Phone..... +1.8889321997
Organization Address. FL	Admin Fax.....	Tech Fax..... +1.7177035107
Organization Address. UNITED STATES		Name Server..... dns2.earthlink.net
		Name Server..... dns3.earthlink.net

The Phishing attack above was stopped in record time because one of the fraudulent e-mails was sent to a network using VERGL technology and the attack was quickly identified.

2 Phishing Attack Stages

Phishing attacks involve several stages:

- The attacker obtains E-mail addresses for the intended victims. These could be guessed or obtained from a variety of sources.
- The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action.
- The attacker sends the E-mail to the intended victims in a way that appears legitimate and obscures the true source.
- Depending on the content of the E-mail, the recipient opens a malicious attachment, completes a form, or visits a web site.
- The attacker harvests the victim's sensitive information and may exploit it in the future.

There are numerous ways for the attacker to execute these steps. There are also countermeasures that intended victims can employ to thwart some of them. Some of the ways consumers will become victim are:

- Installing Trojan software (malicious software that does not behave as the recipient expects).
- Using deceit to convince the recipient to follow some instructions.
- Using spyware to intercept legitimate communications between the victim and a legitimate organization.

Spyware is software that covertly collects information about the user's activities (keystrokes, web sites visited, etc.), and provides that information to a third party. The phishing attack starts with an E-mail to the intended victims. The attacker creates the E-mail with the initial goal of getting the recipient to believe that the E-mail *might* be legitimate and should be opened. Attackers obtain E-mail addresses from a variety of sources, including semi-random generation, skimming them from Internet sources, and address lists that the user believed to be private [CNET]. Spam filtering can block many of the phishing Emails.

If the institution whose customers are being phished regularly uses authenticated E-mail (such as PGP or S/MIME), the recipient may notice that the E-mail does not have a valid signature, thereby stopping the attack. Once the E-mail is opened by the user, the E-mail contents have to be sufficiently realistic to cause the recipient to follow the directions in the Email. This scam is best stopped by preventing the email from ever reaching its intended target.

3 Best Practices

The corporate and consumer "best practices" that follow address many of the issues noted in the phishing attack stages discussion in Section 2. These remedies fall into two general categories:

Corporate Best Practices

- Establish corporate policies and communicate them to consumers: Create corporate policies for E-mail content so that legitimate E-mail cannot be confused with phishing. Communicate these policies to customers and follow them.
- Provide a way for the consumer to validate that the E-mail is legitimate: The consumer should be able to identify that the E-mail is from the institution, not a phisher. To do that, the sending institution must establish a policy for embedding authentication information into every E-mail that it sends to consumers.

- Stronger authentication at web sites: Mail-Block Corporation VERGL technology provides just this type of authentication needed for the banking industry. Using Verified Embedded Random Generated Link Technology
- Automatically block outgoing delivery of sensitive information to malicious parties: Even if the consumer can't visually identify the true web site that will receive sensitive information, there are software products that can.
- Be suspicious: If you aren't sure if an E-mail is legitimate, call the apparent sending institution to verify the authenticity.
- provide the consumer a secure communication channel powered with VERGL technology;
- minimize the number of phishing attacks delivered to consumers;
- increase the likelihood that the consumer will recognize a phishing attack; and
- minimize the opportunities for the consumer to inadvertently release sensitive information.

Education remains critical so consumers are aware of both the phishing techniques and how legitimate entities will communicate with them via E-mail and the web. Some of the proposed remedies require software on the consumer desktop. If one such remedy is deployed, it provides a framework for more remedies at little additional maintenance effort.

The consumer can clearly see the web site he or she is logging into is valid by an encrypted code/key placed on the user personal computer that will identify the consumer when on the correct web address. Issues with misappropriate corporate trademarks will no longer be an issue and the consumer can clearly see the fraud. To provide this level of security for the consumer we recommend using [SWB] Secure Web Browsing with VERGL Technology

Consumer Best Practices

- Automatically block malicious/fraudulent E-mail: Mail-Block Corporation provides the best solution currently available. Sometimes the most obvious solution is overlooked. We need only see the common thread that binds all scams to see how to avoid them. VERGL Technology takes all the know ways to exploit consumers and quickly verifies the information to provide a safe secure online experience.
- Automatically detect and delete malicious software: Spyware is often part of a phishing attack, but can be removed by many commercial programs.

3.1 Corporate Best Practices

Establish Consistent Corporate Policies

Avoid unknown or uninvited Hyperlinks

Issue

Legitimate corporate E-mail often includes hyperlinks to the corporate web site where the consumer is requested to enter sensitive information, including their user ID and password. Phishers take advantage of those embedded links to trick consumers into revealing that information on fraudulent web sites. Within these sites there needs to be a clear window that will identify the consumer and if the consumer is not identified within this window the consumer would know this site is fraudulent. Using VERGL Technology this task can be accomplished.

Approach

.This approach will only work if the institutional policy is frequently communicated to customers and if all customer communications follows the policy. Consistency is essential.

Advantages

- Phishing attacks through deceptive URLs can be reduced.
- Neither the company nor the consumers are required to deploy new software.

Disadvantages

- Some groups and individuals within the institution may not always follow the policy, leading to inconsistency and confusion among consumers.
- Consumers who receive fraudulent E-mails, but are not customers of the institution, may not be aware of the policy.

Recommendation

Institutions should carefully evaluate the impact on consumer experience versus the increased security provided by implementing this policy. It may be appropriate for many institutions.

3.1.2 E-mail Validation Mechanisms

Digitally Signed E-mail

Issue

Customers lack a foolproof means for verifying the authenticity of potentially important messages from legitimate institutions.

Approach

Institutions would establish a policy whereby all high-value E-mail communications with customers are digitally signed with an authorized private key. Upon receipt of the E-mail, the recipient would verify the authenticity of the E-mail using the institution's public key. There is an extremely low probability that a phisher could create a valid signature on a fraudulent E-mail. VERGL provides this ability to give such a digital signature as to provide proof to the consumer that this message is valid.

Advantages

- Digital signatures are enforceable, to a high probability.
- Messages can be automatically verified by E-mail readers.

Disadvantages

- Consumers will need to contact the bank support if a major change has happened on their personal computer
- Non-customers of the institution will not be aware of the institution's policy of signing all E-mail.

Recommendation

Providing this additional security will impact the phishing activity and will be a benefit that will pay off over time with increased customer satisfaction and a renewed confidence in online activity

3.1.2.2 Embedding Consumer Name in E-mail and in Web Sites requesting Information.

Issue

Average customers lack a simple, low overhead, means for verifying the authenticity of messages from legitimate institutions.

Approach

The simplest form of this mechanism is to simply embed the customer's name in the E-mail and Form sites provided by the financial institution as in "Dear Mr. Jones". Some companies are already using this technique. However, if the consumer E-mail address contains the consumer's name; phishers may be able to guess a significant percentage of the names. Phishers don't have anything to lose by guessing incorrectly. This being said using the VERGL Technology to embed information in the email additional information can accompany the name that would be impossible for the Phisher to forge; this same ability is possible when the customer would visit the web site. Using this approach would make it near impossible for the Phisher to carry out this scam. This approach will cause the Phisher to move on to an easier target.

Advantage

- No additional software or hardware required for end-client.
- Messages easily verifiable by unsophisticated users.
- Reduces the likelihood of a successful large-scale attack, as phishers must collect or guess the personalization information for many consumers.

Disadvantages

- Consumers may not always notice that their name is missing in the E-mail.
- Significant marketing expense in delivering the message "Don't accept messages which don't have your name and verification information in the message."
- Institutions must strongly protect the database containing the authentication data (consumer name).
- Not completely fraud-proof, but raises the bar.

Recommendation

This approach should be used by all institutions. If it were to be the predominant policy across all institutions, consumers may learn to expect to see their name in the E-mail. Using the Imbedded security features for [SWB] Secure Web Browsing with VERGL Technology the random key generator will not be able to stolen by spyware or other Trojan methods.

3.1.3 Monitor the Internet for Potential Phishing Web Sites Active Web Monitoring

Issue

Web content provided in phishing E-mails is obtained from legitimate sources, with URL's directed to illegitimate sources.

Approach

This approach involves development of the equivalent of “white-list” admissibility tests of trademark and key content. Monitoring service companies deploy agent-based solutions to continuously monitor web content, actively searching for all instances of a client’s logo, trademark, or key web content. The client institution provides a “white list” of authorized users of logo, trademark, and key content to the company providing the monitoring service. When the agents detect unauthorized users of logos, trademarks, or other web content, recommendation actions may be taken by the client institution.

When the consumer is using the directed procedures and safety features provided there is ample time to identify the source of the phishing activity and the banking security department is able to take steps to notify law enforcement for rapid involvement.

Advantages

- Owners of content are made aware of potential surreptitious users of proprietary content.
- Cease-and-desist orders are generated as a result of active monitoring of content, and identification of inappropriate use.
- Spam filtering rules can be rapidly updated by vendors to block E-mail containing references to malicious sites.

Disadvantages

- None

Recommendation

This technique should be considered as a part of a package of efforts to reduce the economic impact of phishing threats.

3.2 Consumer Best Practices Automatically Block Malicious/Fraudulent E-mail Web Based Anti-SPAM Control

Issue

Consumers cannot always detect fraudulent E-mail that appears to be from a legitimate institution.

Approach

Anti-spam filtering can block some fraudulent E-mail before it is ever delivered to the consumer. Phishing E-mails are one particular form of spam. In this version of spam filtering, corporate policy must be to provide this service as an advantage to doing business with the institution. This would be well received and the cost to the corporate picture would be a savings instead of a possible liability.

Advantages

- Fraudulent E-mail can be blocked before the consumer has a chance to respond to it, stopping the attack at an early stage.
- Mail-Block powered by VERGL technology is available now.

Disadvantages

• Consumers may feel that their current anti-spam protection would be sufficient but the fact is this type of scam will not be detected by current filtering methods, most filtering methods are what we refer to as re-active, VERGL is what is called Pro-Active. There will be some education needed to have all consumers aware of the advantages.

Recommendation

Institutions should consider providing the VERGL technology to all its users to have a uniform approach to addressing the phishing problem.

4 Conclusions

Phishing differs from traditional scams primarily in the scale of the fraud that can be committed. Con-artists have been around for centuries, but E-mail and the World Wide Web provide them with the tools to reach thousands or millions of potential victims in minutes at almost no expense. With phishing attacks, con-artists must still gain the consumer's confidence to be successful. Since there is no face-to-face contact between the attacker and the consumer, the consumer has very little information to work with in order to decide if an E-mail or web site is legitimate. The final technical solution to phishing involves significant infrastructure changes in the Internet that are beyond the ability of any one institution to deploy. However, there are steps that can be taken now to reduce the consumer's vulnerability to phishing attacks. Some of those steps are:

For Corporations:

- Establish corporate policies and communicate them to consumers.
- Provide a way for the consumer to validate that the E-mail is legitimate.
- Stronger authentication at web sites.
- Monitor the Internet for potential phishing web sites.
- Implement good quality anti-virus, content filtering and anti-spam solutions at the Internet gateway (VERGL).
- Implement [SWB] Secure Web Browsing with VERGL Technology.

For Consumers:

- Automatically block malicious/fraudulent E-mail.
- Automatically detect and delete malicious software.
- Automatically block outgoing delivery of sensitive information to malicious parties.
- Be suspicious.

All of these technologies are available now and can be deployed by both consumers and institutions interested in protecting their customers

5 Acknowledgements & References

[APWG] *The Anti-phishing Working Group*, "Proposed Solutions to Address the Threat of E-mail Spoofing Scams," December 2003.

[ASRG] The Anti-Spam Research Group, <http://asrg.sp.am/index.shtml>.

[CNET] McCullagh, Declan, "Treasury breaks word on e-mail anonymity," <http://news.com.com/2100-1028-5137488.html>, CNet News.com, January 8, 2004.