September 2004

McAfee Research
Technical Report # 04-004

Anti-Phishing: Best Practices for Institutions and Consumers

Gregg Tally
Roshan Thomas
Tom Van Vleck

www.mcafee.com

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. 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 E-mail appear authentic [KOPR]. 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. The APWG reported 176 unique phishing attacks for the month of January 2004 [APJA]. By April, the number of unique attacks per month increased to 1,125 [APAP] and reached 1,422 in June [APJU]. 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. We do not believe it is practical to propose sweeping changes to this installed base as part of the near-term solution. 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 term, 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.

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. The attack trees below show the steps that the attacker (and victim) must take for a successful phishing attack. The trees also show ways that existing technology can be used to reduce vulnerability to phishing attacks.

In the diagram, the 'start' state is at the top. Attacker and victim actions are shown as edges or lines between the rectangles. Each rectangle contains the resource or condition that the attacker is trying to achieve. The attack is thwarted if it moves to the state of 'Attack fails'. The attack is successful if it achieves the final state of 'Attacker gains sensitive user information'.

Due to the size and complexity of the tree, we have divided it into four sections. The first section shows the stages of the attack that are common to all of the methods. Each of the attack methods is detailed on its own diagram. Those methods 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.

As shown in Figure 1 below, 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 E-mails. 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 E-mail.

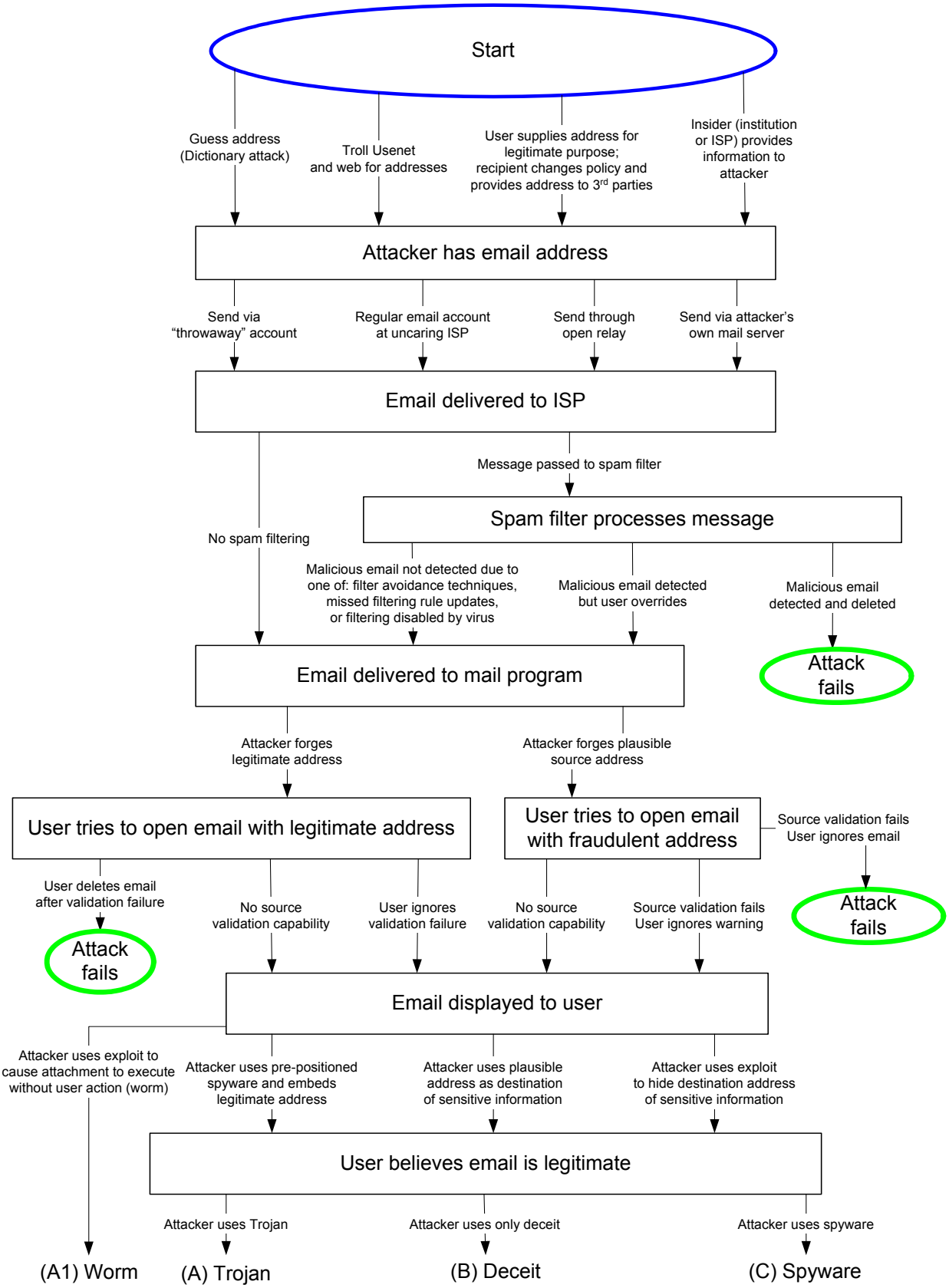

Figure 1 - Common Attack Tree Methods

Worms and Trojans

In Figure 2, the attacker continues the attack by sending an E-mail attachment purporting to be for a benign purpose, such as a greeting card or screen saver. In reality, the attachment contains an executable program that intercepts future communications between the victim's computer and a legitimate institution. The spyware transmits the information to the attacker over the network. Anti-virus software, host-based intrusion detection, and personal firewall software can block many attacks in this scenario.

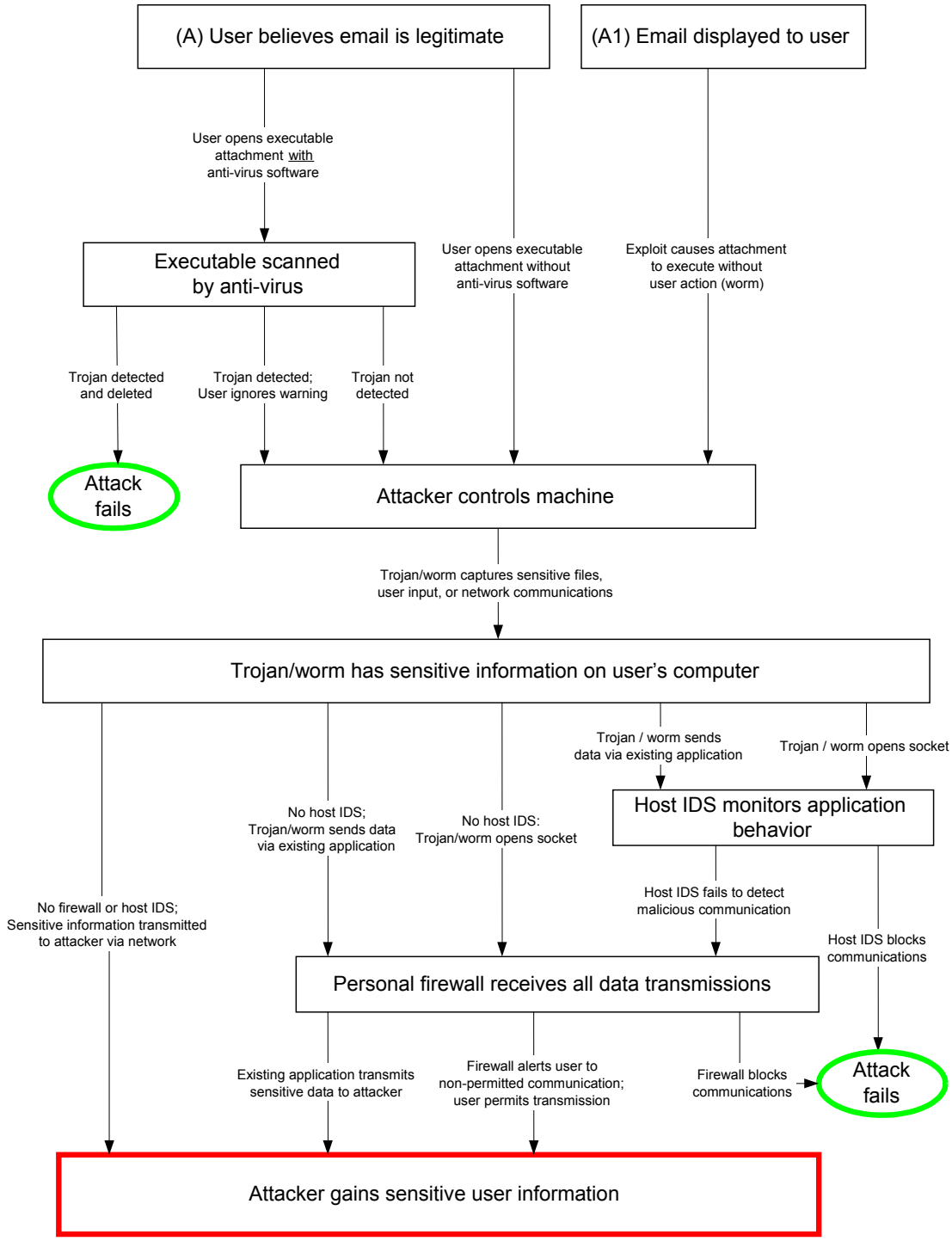

Figure 2 - Attacks with Worms and Trojan Programs

Deceit

Figure 3 shows a continuation of the attack sequence from Figure 1 relying only on deception. There are no exploits or additional software programs involved in the attack. The attacker relies on the law of large numbers to ensure that at least some of the recipients will be convinced that the E-mail is legitimate and will follow the directions. SSL (Secure Socket Layer) provides some protection if the attacker's web site uses it, but only if the recipient heeds the warnings from the browser about invalid certificates. Commercial privacy protection software can also be of help by warning the user when they are about to send sensitive information to questionable destinations.

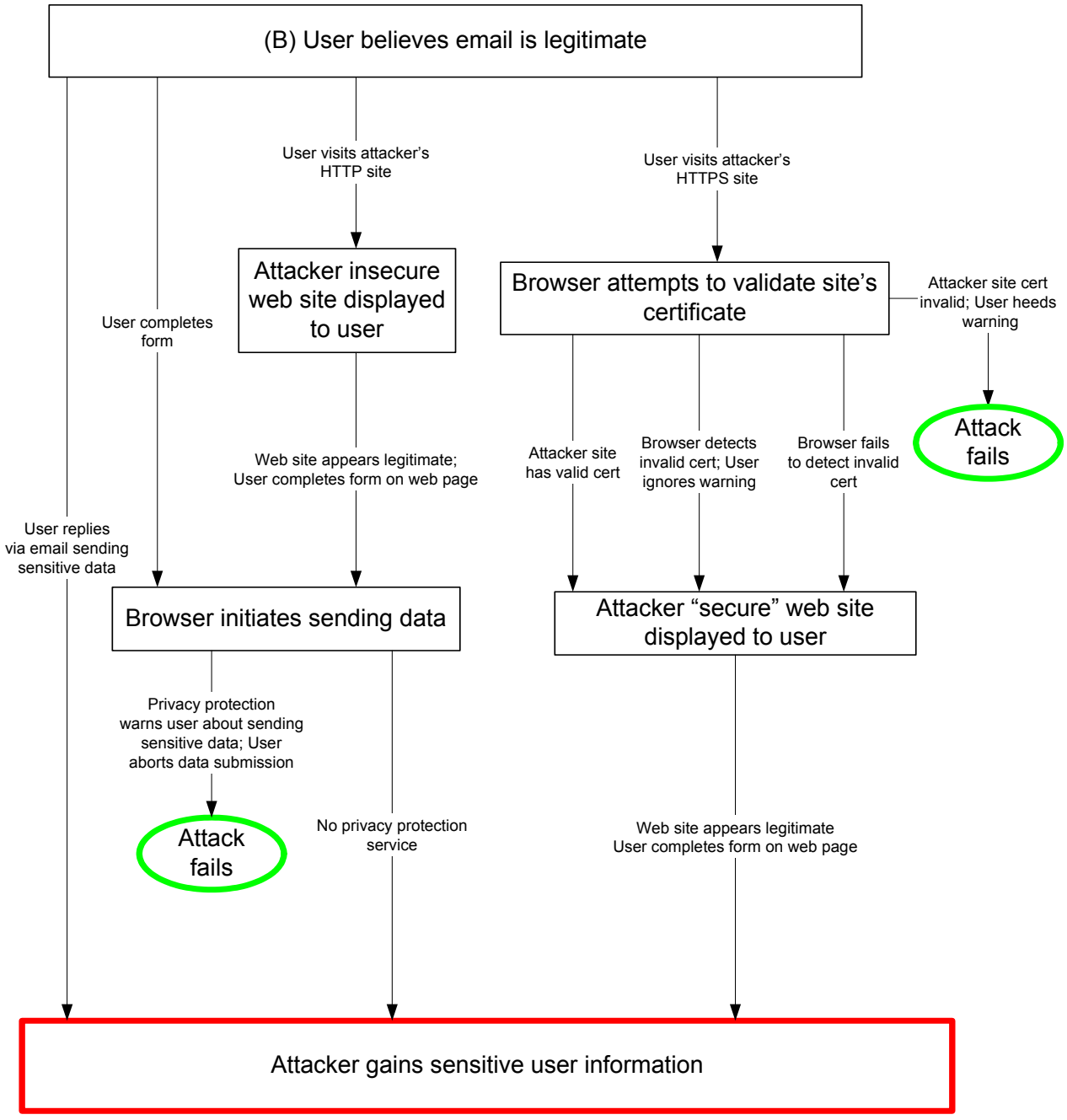

Figure 3 - Attacker Uses Deceit to Gain Recipient's Confidence

Spyware

Figure 4 shows the attacker using pre-positioned spyware on the victim's computer to extract sensitive information. This can be accomplished from a previous worm or Trojan attack (see Figure 2) or other means. Spyware can often be detected by specialized spyware detection programs and by many commercial anti-virus programs. In addition, personal firewalls and host-based intrusion detection systems can often prevent spyware from delivering sensitive information to third parties.

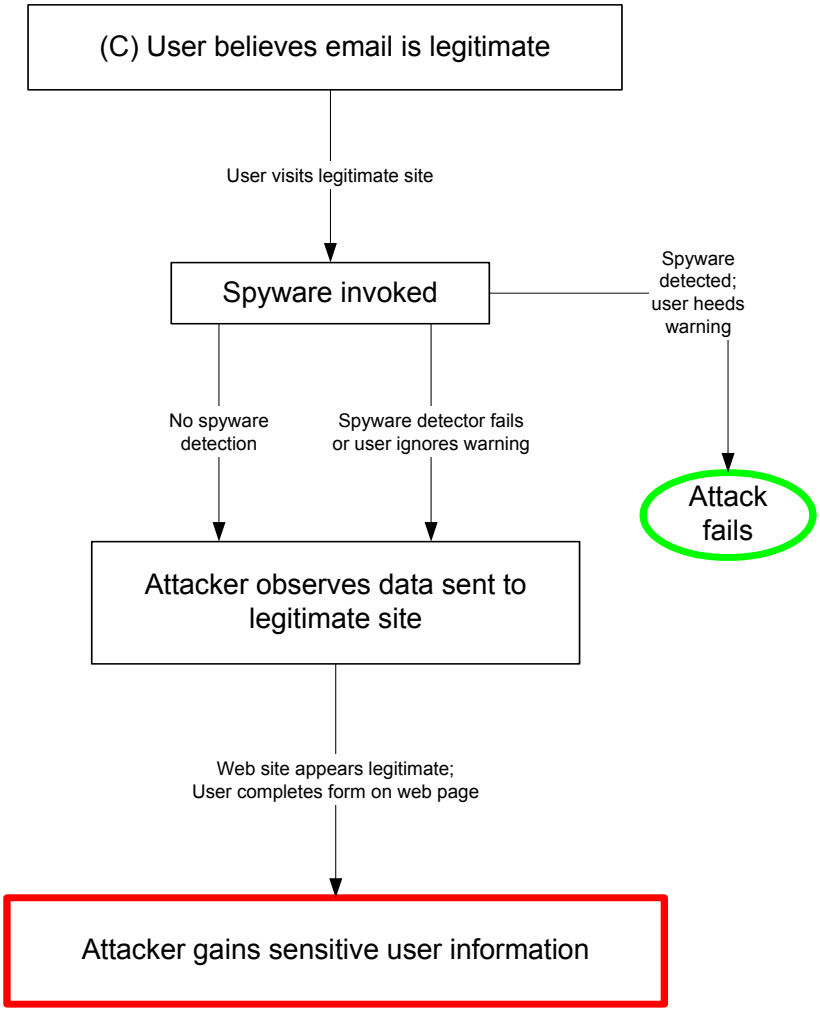

Figure 4 - Attacker Uses Spyware to Extract Information

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: If institutions did not ask consumers for sensitive information when logging onto a web site (e.g., social security numbers or passwords), then it would be more difficult for phishers to extract such information from the consumer.
- Monitor the Internet for potential phishing web sites: The phishing web site generally appears somewhere on the Internet prior to the launch of the phishing E-mails. These sites often misappropriate corporate trademarks to appear legitimate.
- Implement good quality anti-virus, content filtering and anti-spam solutions at the Internet gateway: Gateway anti-virus scanning provides an additional layer of defense against desktop anti-virus scanning. Filter and block known phishing sites at the gateway. Gateway anti-spam filtering helps end users avoid unwanted spam and phishing emails.

Consumer Best Practices

- Automatically block malicious/fraudulent E-mail: Spam detectors can help keep the consumer from ever opening the suspicious E-mail, but they aren't foolproof.
- Automatically detect and delete malicious software: Spyware is often part of a phishing attack, but can be removed by many commercial programs.
- 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.

None of these remedies individually provides a complete answer to the problem. We recommend a combination of countermeasures that will:

- 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 recommendations below elaborate on the corporate and consumer best practices listed above. There are other long-term strategies that require cooperation from Mail Service Providers and Internet Services Providers (ISPs) that should also be effective in the future. These

strategies include the Domain Keys approach recently advocated by Yahoo!™ and mail gateway scanning.

3.1 Corporate Best Practices

3.1.1 Establish Consistent Corporate Policies

3.1.1.1 Avoid Embedded 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.

Approach

While embedding hyperlinks in E-mail can make the consumer experience easier, it also creates more opportunities for fraud. Vulnerabilities in some versions of Microsoft's Internet Explorer can provide the phisher with an opportunity to disguise the true destination of a URL. A safer alternative is to provide a text-only link in the E-mail that the consumer must type or cut-and-paste into their browser. Regular customers will likely have a bookmark for the institution, which makes this process even easier.

This approach will work best 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 consumer are required to deploy new software.

Disadvantages

- The consumer experience will be adversely impacted, to a small degree.
- Some groups and individuals within the institution may not always follow the policy, leading to inconsistency and confusion among consumers.
- Consumers may not behave in their own best interests at all times. They may continue to be fooled by fraudulent E-mails with embedded hyperlinks.
- 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.

3.1.1.2 Avoid E-mail Forms

Issue

Phishers use E-mail forms to collect personal information from consumers. If the legitimate institution also uses these forms, it is difficult for the consumer to distinguish between legitimate and fraudulent E-mail.

Approach

As with embedded hyperlinks, E-mail forms can create a simplified consumer experience when an institution is requesting information. However, the mechanism is easily used by phishers to collect the same information, with little opportunity for the consumer to validate the source of the E-mail.

The institution must educate consumers that legitimate E-mail will never contain forms requesting personal information.

Advantages

- Phishing attacks through E-mail forms can be reduced.
- Neither the company nor the consumer are required to deploy new software.

Disadvantages

- The consumer experience will be slightly impacted.
- Some groups and individuals within the institution may not always follow the policy, leading to inconsistency and confusion among consumers.
- Consumers may not behave in their own best interests at all times. They may continue to be fooled by fraudulent E-mails with embedded forms.
- 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 is probably appropriate for most institutions.

3.1.2 E-mail Validation Mechanisms

3.1.2.1 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.

PGP and S/MIME are examples of digital signature technologies, but many users believe they are too difficult to use. To date, such technologies have not been widely adopted.

Advantages

- Digital signatures are unforgeable, to a high probability.
- Messages can be automatically verified by E-mail readers.
- Can be used as a recovery mechanism in a multi-factor authentication system when tokens are lost.

Disadvantages

- Average consumers are unlikely to install and maintain digital signature technology.
- Non-customers of the institution will not be aware of the institution's policy of signing all E-mail.

Recommendation

For small numbers of customer accounts with high-value transactions, this approach is worth considering.

3.1.2.2 Sender Policy Framework (SPF)

Issue

Phishing emails often forge the sending domain of the targeted institution.

Approach

The SPF specifications being developed in the IETF [SPF] are attempting to define a mechanism by which mail receivers can verify that a sending host is authorized to send mail on behalf of the source domain. By itself, SPF does not prevent all forms of spam because spammers can register throw-away domains with SPF records to pass the SPF tests. With phishing emails, this is more difficult because the sending domain on the email has to be somewhat plausible to the human recipient as a legitimate sending domain for the targeted institution.

SPF requires the owners of legitimate domains to publish SPF records in the domain name service (DNS). SPF enforcement can be performed either at the receiving mail transfer agent (MTA), mail delivery agent (MDA), or mail user agent (MUA). There are issues with mail

forwarding that can require modifications to legitimate mail forwarding, such as switching from forwarding to remailing.

End users must be aware of the sending domain when inspecting email. If the subject and body of an email claim to be from the recipient's bank, but the "From" address is nonsense, SPF will not help. It will be up to the user to realize that there is an inconsistency in the "From" address and content of the email.

Advantages

- Forces phishers to use sending domains that are not identical to the legitimate sending domain name.
- No additional software or hardware required for end-client if the ISP performs SPF verification at the MTA.

Disadvantages

- The specifications are still evolving, but some adoption has already begun.
- Not completely fraud-proof, but raises the bar. Phishers can still create domains that appear to be real and register SPF records for those domains.
- If phishers do not impersonate the sending domain, SPF will not be effective. End users must make sure that the sender is appropriate for the mail contain.

Recommendation

Institutions should publish SPF records for the sending mail domains. As more ISPs and mail servers begin checking SPF records, the solution will become more effective.

3.1.2.3 Visual or Audio Personalization of E-mail

Issue

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

Approach

This approach offers a simple visual or audio mechanism to verify the authenticity of E-mail. Similar to the current practice of placing the card-holder's photograph on bank-issued credit cards, institutions could include a photograph of the customer on all electronic communications. This provides a simple, reliable method for the banking customer to recognize legitimate messages without need for further software installed at the user's desktop. Visually-impaired clients would use an alternate (perhaps audio "image," or simple pass-phrase) identification object to be attached appropriately.

Note that the only way this mechanism will be successful is if it is accompanied by an education campaign by the institution to announce the new "Secure Communications Mechanism."

Advantages

- No additional software or hardware required for end-client.
- Messages easily verifiable by unsophisticated users.
- Value of "personalized" credit cards already established in market; may tie-in easily to that marketing message.

- Reduces the likelihood of a large-scale attack, as phishers must collect previous messages from the institution to each customer in order to obtain the personalization information.
- Can be used as a recovery mechanism in a multi-factor authentication system when tokens are lost.

Disadvantages

- Significant marketing expense in delivering the message "Don't accept messages which don't have your picture."
- Significant increase in cost of generating messages.
- Customers must physically appear at the institution's office in order to take the picture. This may not be suitable for e-businesses that lack a store-front. Other means, such as regular mail distribution of pass-phrases or photographs, may be required for those businesses. However, it would be preferable for each institution to use unique photographs so that security breaches at one do not cascade into vulnerabilities for all.
- Institutions must strongly protect the database containing the authentication data (pictures, sound clips, or pass phrases).
- Not completely fraud-proof, but raises the bar.

Recommendation

For certain institutions, particularly those that issue credit cards, this may be a viable solution if they are already collecting digital images for credit cards or other uses.

3.1.2.4 E-mail Sequence Numbering

Issue

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

Approach

Another variation of this mechanism is to embed the equivalent of sequence numbers in each E-mail from the institution. The sequence numbers would be a predictable form of authentication that could be easily verified by the consumer. An example of an authentication header follows:

```
Date: Jan. 16, 2004
Serial number: JJH0017
Our last E-mail to you was JJH0016 on Dec. 10, 2003.
Our next E-mail to you will have serial number JJH0018.
```

Note that the only way this mechanism will be successful is if it is accompanied by an education campaign by the institution to announce the new "Secure Communications Mechanism."

Advantages

- No additional software or hardware required for end-client.
- Value of "personalized" credit cards already established in market; may tie-in easily to that marketing message.
- Reduces the likelihood of a large-scale attack, as scammers must collect previous messages sent from the institution to each customer in order to obtain the personalization information.

- Can be used as a recovery mechanism in a multi-factor authentication system when tokens are lost.

Disadvantage

- Slightly more difficult for the recipient to validate due to the need to retain the most recent E-mail.
- Consumers may not validate sequence numbers.
- Significant increase in cost of generating messages.
- The institution must strongly protect the database containing the sequence numbers.
- Not completely fraud-proof, but raises the bar.

Recommendation

If digital images or similar personalization information is not obtainable, this is the next most reliable solution. However, it is also more prone to fail for a large number of consumers.

3.1.2.5 Embedding Consumer Name in E-mail

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, 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.

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 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.

3.1.3 Strong Authentication Mechanisms

3.1.3.1 Secure Token Authentication

Issue

Social engineering scams like phishing will always be possible as long as the victim knows all of the information necessary to make a transaction.

Approach

The ultimate goal of phishing attacks is to get the victim to divulge sensitive information. Often, this is a user ID and password that can be used to access a legitimate web site. If users do not know the authentication information, then this type of attack is impossible.

One way to do this is to provide secure tokens (hardware) to users and require a challenge-response for all electronic transactions with the institution. In this type of authentication system, the hardware token provides a one-time password that is valid only for the owner of the token. The token generates a new one-time password with each login, so it does not matter if an attacker obtains the value. Furthermore, the user cannot generate the values in advance so they cannot accidentally divulge the information to an attacker.

These tokens are already in limited use. Some companies require their employees to use such tokens for remote access to computer systems.

Some banks and credit card companies also provide a similar capability to make transactions with a smart card [GEMP] [MAST]. One alternative to issuing new hardware tokens is to integrate the functionality into new credit cards. However, the smart card remedies generally require that a reader be attached to the computer. In addition, security vulnerabilities have been found in some smart cards.

Advantages

- The user cannot accidentally divulge the information necessary to make an electronic transaction.
- All fraud requires physical access to the token.
- The user cannot opt to authenticate in a way that circumvents the security policy.
- Standards already exist for implementing such a system. See http://www.emvco.com.
- Duplicating the physical card requires much more sophistication, even if the victim provides their PIN.

Disadvantages

- By itself, secure tokens do not prevent the user from supplying information that could be used as a proxy for the information to carry out a transaction. In particular, information used to identify a person, such as their mother's maiden name, can still be obtained and could lead to fraudulent activities.
- There is a cost to issue tokens, although it will vary according to the type of hardware chosen.
- A user may need to carry multiple tokens, one for each service to which he is subscribed.
- Software upgrades at the vendor are required to perform the challenge-response authentication.
- There are significant costs to deploy and maintain the remedy, including initial assignment of tokens and revocation.

- Initially, users may balk at the additional inconvenience and at any costs that are passed on to the user.
- Secure token and smart card solutions require extensive security engineering and attention to many interlocking details in order to be secure.

Recommendation

As with digital signatures, this method may be suitable for a small number of customers with high-value transactions. U.S. consumers and corporations have been reluctant to use tokens in the past.

3.1.3.2 Software Emulation of Secure Tokens for Authentication

Issue

Social engineering scams like phishing will always be possible as long as the victim knows all of the information necessary to make a transaction. Hardware security tokens can help, but may be expensive to deploy.

Approach

The approach is very similar to the Secure Token approach, but without requiring additional hardware. Instead, a software application, keyed to a particular user, provides the response values for electronic authentication. When running on a PC, it may be possible to avoid having the user retype the challenge and response values. If this is done, the web site must authenticate itself to the Secure Token simulator in order to prevent users from being tricked into logging into malicious sites.

To use this approach, institutions must distribute the software to consumers via CD or other physical media to prevent new phishing opportunities. The software must also be keyed to each individual consumer.

One variant of this approach is to develop software compatible with cell phones and PDAs so that users can take their authentication with them and use it on additional computers. The user would key in their PIN and the challenge value into the cell phone or PDA, which would then generate the response. The user would then enter the response value into the web application to complete the authentication.

Advantages

- The user cannot give out the information necessary to make an electronic transaction.
- All fraud requires knowledge of the seed value in the Secure Token simulator.
- The user cannot opt to authenticate himself or herself in a way that circumvents the security policy.
- Software distribution costs should be much less than hardware token distribution costs.

Disadvantages

- By itself, it does not prevent the user from supplying information that could be used as a proxy for the information to carry out a transaction. In particular, information used to identify a person, such as their mother's maiden name, can still be obtained and could lead to fraudulent activities.
- There is a cost to issue the CDs.
- There are significant costs to deploy and maintain the remedy, including initial distribution of unique CDs and revocation.

- Users may not always posses the required software when away from their home computer. If the software runs in a cell phone or PDA, that may alleviate the problem.
- The Secure Token simulator may be vulnerable to corruption since it relies on standard operating system security. If the software runs in a cell phone or PDA, that may also alleviate this problem.

Recommendation

If hardware tokens are cost-prohibitive, this remedy should be considered. It should be used in conjunction with other technology that prevents unintended disclosure of other sensitive information.

3.1.4 Monitor the Internet for Potential Phishing Web Sites

3.1.4.1 Active Web Monitoring

Issue

Figure 1 illustrates that the web content provided in phishing-motivated 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, remediation actions may be taken by the client institution.

Some companies, such as NetCraft [NETC] and NameProtect, already offer services that seek out potentially fraudulent web sites for customers. It is not clear that the desired level of automated response is available.

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

- Requires active monitoring.
- Time delay between identification and action to eliminate use may still result in numerous thefts of private information.

Recommendation

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

3.1.5 Gateway Filtering

3.1.5.1 Gateway Anti-Virus Scanning

Issue

Phishing attacks often involve malicious software, including Trojans and backdoor programs that steal sensitive information. Desktop anti-virus is effective only if the rule database is updated regularly.

Approach

By scanning web traffic and email at the network boundary (gateway) for potentially malicious software, institutions can prevent a large amount of malicious code from ever entering the network. It is far easier, and faster, for a large institution to update a relatively small number of gateway scanners than it is to ensure that all desktop scanners are up to date. Automated desktop virus scan updates help, but is still somewhat slower than gateway updates. Given the speed with which some malware propagates, an hour or few minutes can be critical.

Gateway anti-virus scanning should be combined with desktop scanning. Some encrypted traffic cannot be scanned at the gateway and must be scanned on the desktop. Similarly, mobile users are not always protected by the gateway scanner when away from the office.

Advantages

- Malicious code can be blocked from entering the network.
- Gateway scanning supports rapid updates of a relatively small number of scanning nodes.
- Effective products are available now from several vendors.

Disadvantages

- Some network traffic cannot be scanned.
- Mobile users are not protected by the gateway scanning.

Recommendation

Gateway anti-virus scanning should be combined with desktop anti-virus scanning as part of a layered-defense strategy against malicious code.

3.1.5.2 Gateway Content Filtering

Issue

Phishing attacks usually involve a malicious web site that is often active prior to transmission of the first phishing email.

Approach

If the institution has knowledge of a phishing web site, it should block access to the site from the network. This can be done in a number of ways, but primarily by installing blocking rules for the malicious URLs at the gateway. By working with a network monitoring service provider, institutions (particularly ISPs) can get early warning of the phishing sites and protect their network users from accessing the sites.

Advantages

- Very effective at blocking access to known phishing sites, without waiting for an ISP to take the phishing site down.
- Effective products are available now from several vendors.

Disadvantages

- May require manual configuration of firewalls and other gateway devices to implement the blocking rules.

Recommendation

If the institution has a suitable firewall or gateway, they should consider blocking the known phishing sites.

3.1.5.3 Gateway Anti-Spam Filtering

Issue

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

Approach

As shown in Figure 1, anti-spam filtering can block some fraudulent E-mail before it is ever delivered to the user. Phishing E-mails are one particular form of spam. In this version of spam filtering, the institution installs spam filtering at the mail gateway. Spam can be handled in a number of ways, including marking (modification of the subject), deleting, and quarantining.

Advantages

- Fraudulent E-mail can be blocked before the user has a chance to respond to it, stopping the attack at an early stage.
- End users do not need to install software on the desktop.
- Effective products are available now from several vendors.

Disadvantages

- Spam detection is improving, but as spammers constantly change their spamming techniques no solution can be 100% accurate. Due to these imperfections, users may elect to review all suspected spam before deleting it. The user must learn to recognize false positives.

Recommendation

Gateway anti-spam filtering should be deployed for large networks and at ISPs.

3.2 Consumer Best Practices

3.2.1 Automatically Block Malicious/Fraudulent E-mail

3.2.1.1 Desktop Anti-SPAM Filtering

Issue

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

Approach

As shown in Figure 1, 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, the consumer must install software on the computer and configure it.

Advantages

- Fraudulent E-mail can be blocked before the consumer has a chance to respond to it, stopping the attack at an early stage.
- Effective products are available now from several vendors.

Disadvantages

- Spam detection is improving, but as spammers constantly change their spamming techniques, no solution can be 100% accurate. Due to these imperfections, consumers may elect to review all suspected spam before deleting it. The consumer must learn to recognize false positives.
- Desktop anti-spam remedies require the consumer to purchase, install, and maintain the software. Due to great variations in technical abilities, some consumers may not deploy the technology in an effective manner.

Recommendation

Consumers should consider purchasing and using spam-filtering products. They should learn to recognize both false positives and false negatives so they do not override correct decisions made by the filter.

3.2.1.2 Gateway Anti-SPAM Filtering

Issue

Consumers cannot always detect fraudulent E-mail that appears to be from a legitimate institution and may not install desktop anti-spam filtering.

Approach

As shown in Figure 1, 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, the mail service provider installs anti-spam filtering at the mail gateway.

There are several ways to inject anti-spam filtering into the E-mail processing cycle. A three-tiered approach can include the following:

- Tier 1: Filter at the service provider (ISP or mail service) for all E-mail customers;
- Tier 2: Filter in a network appliance for all users on the LAN; and

- Tier 3: Filter on the individual desktop through desktop protection application software.

Advantages

- Fraudulent E-mail can be blocked before the consumer has a chance to respond to it, stopping the attack at an early stage.
- By filtering at a service provider or in a network appliance, the consumer does not have to install any software.
- If the service provider deletes suspected spam, the consumer will never open anything that has been detected.
- Effective products are available now from several vendors.

Disadvantages

- Targeted institutions are not able to control whether or not their customers' ISPs provide gateway spam filtering.
- Spam detection is improving, but as spammers constantly change their spamming techniques, no solution can be 100% accurate. Due to these imperfections, consumers may elect to review all suspected spam before deleting it. The consumer must learn to recognize false positives.

Recommendation

Many ISPs and institutions already provide anti-spam filtering at their mail gateways. If yours does not, ask for it.

3.2.2 Detecting and Deleting Malicious Software

3.2.2.1 Anti-Virus and Anti-Spyware Software

Issue

Spyware invisibly intercepts communications between the consumer and legitimate institutions.

Approach

As shown in Figure 2 and Figure 4, spyware can be distributed to consumers via E-mail and later intercept communications between users and legitimate web sites. Many consumers have already installed anti-virus software, which helps reduce the risk of this form of attack. Anti-virus software detects many forms of malware, including spyware, and can delete the spyware when found. Most anti-virus software runs nearly invisibly to the consumer with little impact on their normal operations. Anti-spyware programs can scan the computer for potential spyware and can generally remove it.

Advantages

- Detects and deletes spyware before it can intercept sensitive information.
- There are few false positives.

Disadvantages

- Detection is imperfect, but getting better.
- Signatures files must be updated regularly or the software loses effectiveness against current attacks.
- Anti-spyware software may occasionally remove some spyware that is required for legitimate programs to fully function. The consumer is generally notified when removal of spyware has these consequences.
- The consumer must purchase and install the software, unless the computer vendor pre-installs a version prior to purchase.

Recommendation

Consumers should install anti-virus software, with options enabled to detect potentially unwanted programs. Consumers must also keep their anti-virus software up to day. Consumers should also consider installing one of the free spyware detection applications. However, they should take care to install a reputable spyware detection application as some have been accused of being spyware themselves.

3.2.3 Automatically Blocking Delivery of Sensitive Information to Malicious Parties

3.2.3.1 Desktop Privacy Service

Issue

As shown in Figure 3, users may be tricked into submitting sensitive data to malicious non-secure web sites.

Approach

Commercially available software packages can monitor outgoing web traffic for a user-definable set of data. The data is typically defined to be information that identifies the user, such as names, social security numbers, and credit card numbers. If any of that set of data appears in the outgoing packets, the packet is halted until the user confirms that the data should be sent to the true destination, or that the data delivery should be aborted. If the user indicates that the data should not be sent , the sensitive data is removed.

One of the challenges for consumers with this type of product is to identify the sensitive information to protect, and the specific web sites to put on permit/deny lists. When the information is well-maintained, it can do a very effective job at preventing a wide variety of phishing attacks.

Advantages

- Commercial products are available today.
- Even though the destination URL may not be apparent to the consumer, the software has visibility into the true destination and can block unwanted information disclosures.

Disadvantages

- Requires software installation on the consumer's computer.

Recommendation

This approach is essential to block some social engineering attacks that will succeed in spite of strong authentication, anti-virus, anti-spyware, and anti-spam software. Consumers can install these products now.

3.2.4 Be Suspicious

3.2.4.1 Type Web Addresses and Verify Authenticity

Issue

Various exploits can hide the true web address of an apparent link and redirect the browser to a phishing web site.

Approach

There are several ways that a phisher can make an E-mail appear to be legitimate. Furthermore, it may difficult to determine the true web address behind embedded links in E-mails. It is generally safer to type the desired web address into the browser than to click on embedded links. If you are unsure of the authenticity of an E-mail, contact the sending institution directly.

Advantages

- No additional software is required

Disadvantages

- Long web addresses are tedious to type and prone to error.
- It may be difficult to validate some E-mails.

Recommendation

Know your institution's policy for requesting sensitive personal information. When in doubt, check with the institution via telephone or by sending E-mail to a previously known contact.

4 Conclusion

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.

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

In addition to the authors on the cover page, the following McAfee Research scientists and engineers contributed to this white paper:

Brian Appel
David Carman
Mark Feldman
Michael Heyman
Jim Horning
Roger Knobbe
Patrick LeBlanc
Erik Mettala
Steve Schwab
Deborah Shands

6 References

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

[APJA] *The Anti-Phishing Working Group*, "Phishing Attacks Trend Report, January 2004".

[APAP] *The Anti-Phishing Working Group*, "Phishing Attacks Trend Report, April 2004".

[APJU] *The Anti-Phishing Working Group*, "Phishing Attacks Trend Report, June 2004".

[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.

[GEMP] *GEMPLUS S.A.*, "GemAuthenticate flyer," 2003.

[KOPR] *Koprowski, Gene J.,* "Beware of 'Spoofing' Scams," UPI Technology News, January 2004.

[MAST] *MasterCard International, Inc.,* "OneSmart Growth Opportunity: Three Business-building Packages for Issuers," 2003.

[NETC] *NetCraft Ltd,* http://news.netcraft.com/archives/2004/01/02/phishing_identity_theft_and_banking_fraud_detection.html, 2004.

[SPF] M. W. Wong, M. Lentczner, "The SPF Record Format and Test Protocol", IETF MARID Internet-Draft, July 11, 2004.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.