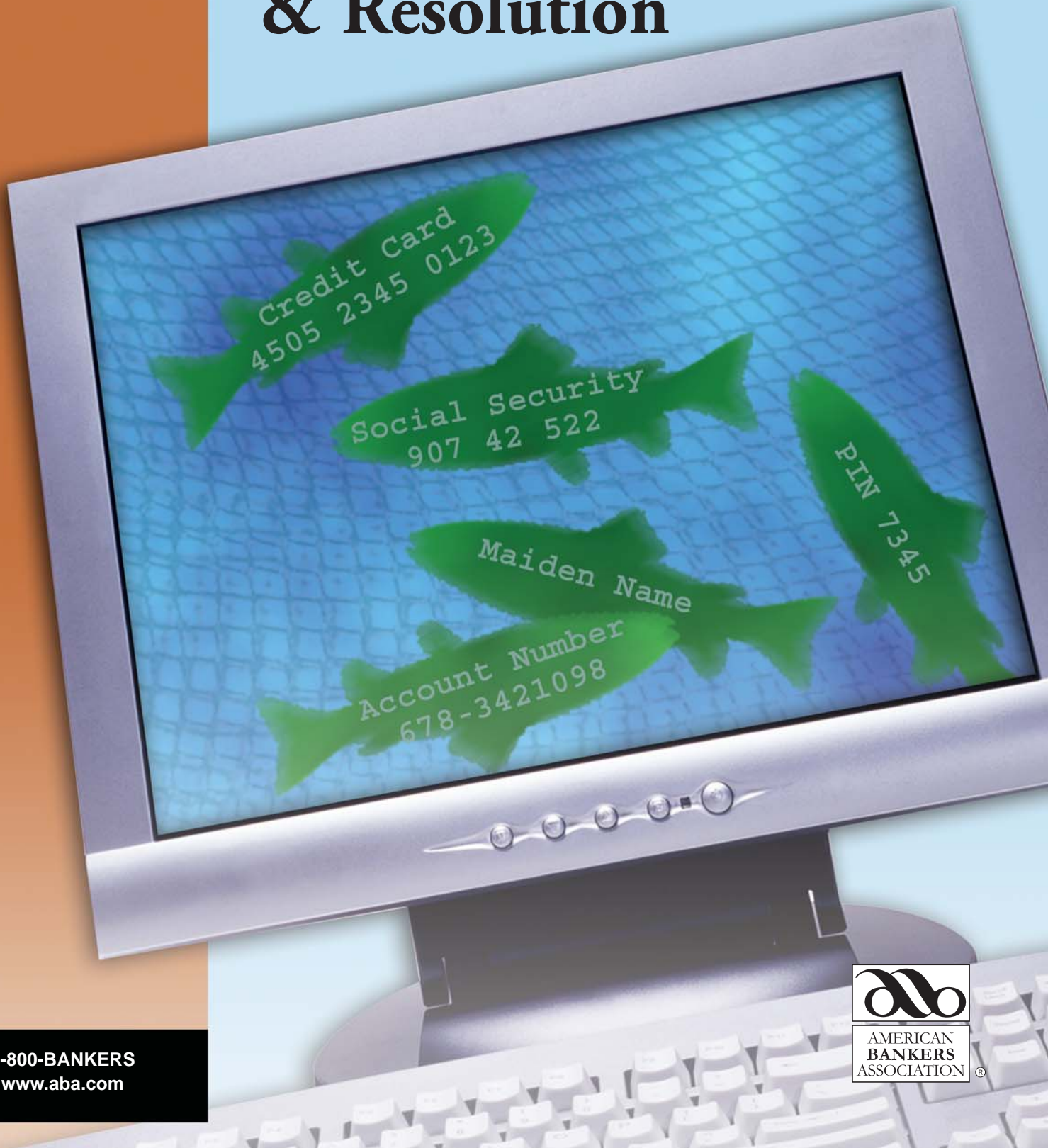


Phishing Prevention & Resolution



ABAWorks on Fraud: Phishing Prevention & Resolution

As the use of Internet banking continues to increase, understanding and addressing the threats to data security are critical to maintaining the customer's confidence in online banking — and in the financial services industry in general. Your bank can have a positive influence in counteracting these threats by operating in partnership with your customers in protecting their financial information. This ABAWorks is intended to provide you with the resources your bank needs to combat this threat.

There is a new type of Internet piracy called “phishing.” It's pronounced “fishing,” and that's what these thieves are doing: “fishing” for your customer's personal financial information. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your customer's checking account or run up bills on their credit cards.

In the worst case, your customer could become a victim of identity theft. With the information obtained from a successful phishing scam, these thieves can take out loans or obtain credit cards and even driver's licenses in their name. They can do damage to your customer's financial history and personal reputation that can take years to unravel. But if you understand how phishing works and how to protect yourself, you and your customers can help stop this crime.

Who Should Read This ABAWorks?

ABAWorks is a free, members-only publication, providing concise guidance on issues or trends of importance to the banking industry. This ABAWorks is designed to help your bank's management information system (MIS), compliance, marketing, legal and communication staffs raise awareness and reduce the risks of phishing to your institution and your customers. We have included a variety of phishing prevention, detection, and response resources for you to consider. All resources and samples are provided as a service to our members. While we hope that you find this guide helpful and informative, it should not be used as a substitute for the advice of legal counsel.

ABA Staff Contacts for Questions About Phishing

Doug Johnson

Senior Policy Analyst
Government Relations
202-663-5059
djohnson@aba.com

John Hall

Associate Director
Public Relations
Communications
202-663-5473
jhall@aba.com

Lisa Gold Schier

Associate Director
Corporation for
American Banking
202-663-5059
lgoldsch@aba.com

Nessa Feddis

Senior Federal Counsel
Government Relations
202-663-5433
nfeddis@aba.com

Don Rhodes

Policy Manager
Government Relations
202-663-7513
drhodes@aba.com

The American Bankers Association, on behalf of the more than two million men and women who work in the nation's banks, brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership — which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks — makes ABA the largest banking trade association in the country.

© 2005 American Bankers Association, Washington, D.C.

This publication was paid for in part with the dues of ABA member financial institutions and is intended solely for their use. Please call 1-800-BANKERS if you have any questions about this resource, ABA membership or would like to copy or license any part of this publication.

This publication is designed to provide accurate information on the subject addressed. It is provided with the understanding that neither the authors, contributors nor the publisher is engaged in rendering legal, accounting or other expert or professional services. If legal or other expert assistance is required, the services of a competent professional should be sought. This guide in no way intends or effectuates a restraint of trade or other illegal concerted action.

Table of Contents

Phishing: The Big Picture	1
What is Phishing?	2
Is Your Bank Really a Target?	3
How Your Customer is Targeted	4
Preventing & Resolving Phishing Scams	7
Preventing Successful Phishing Scams	8
Business Practices That Defend Your Institution	11
Detecting Phishing and Other Electronic Scams	12
Responding to a Phishing Attack	13
Appendices	17
Appendix I: Sample E-Scam/Phishing Web Site Language	17
Appendix II: Understanding Your Bank's Liability	23
Appendix III: Sample Media Talking Points	27
Appendix IV: Customer Activity Log	29
Appendix V: Phishing FAQ	31
Appendix VI: Phishing Glossary	35

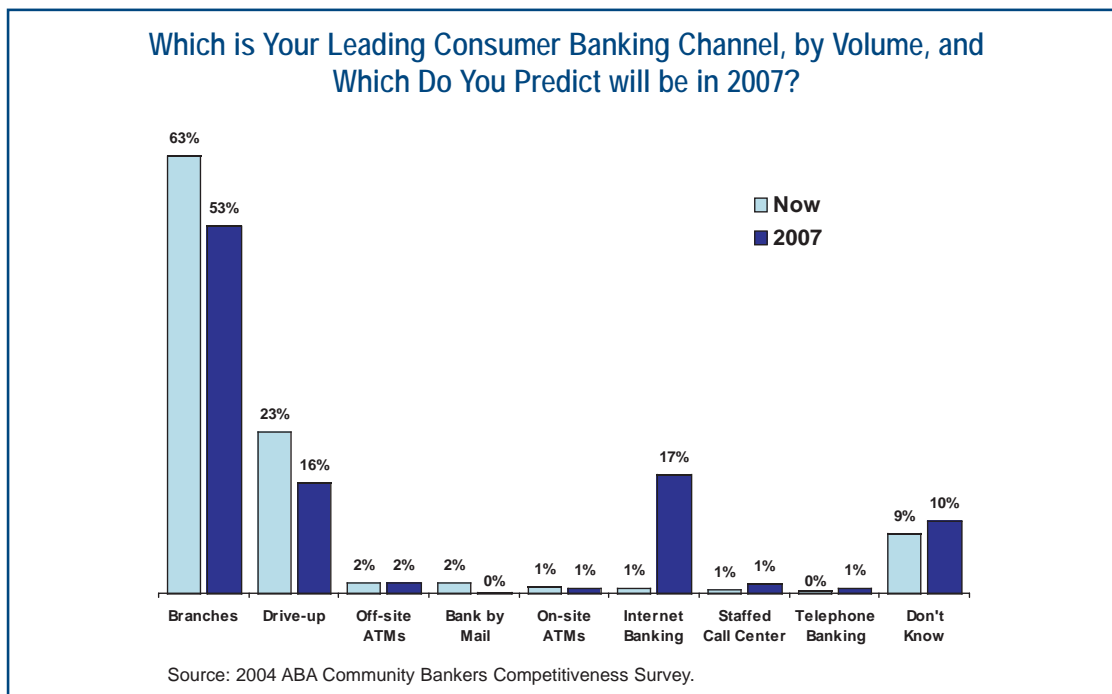


Also visit the ABA's Anti-Phishing Web page, easily accessible from www.aba.com, where the most recent information on phishing and other scams are maintained.

Phishing: The Big Picture

Risks as Well as Rewards Grow As Consumers Expand Their Use of Online Services

The next few years will see a significant reordering of how you deliver services to your customers, mostly due to a substantial increase in Internet banking use. Branches continue to dominate, but more and more bankers are expecting Internet banking to soon surpass the drive-in window as the second most popular way for customers to access banking services. Community bankers share this view. In fact, over 17 percent of community bankers responding to the ABA's 2004 Community Bank Competitiveness survey felt that Internet banking would be their *primary* delivery channel by 2007, up from less than 1 percent in 2003. While this represents a substantial shift from present day, faith in the Internet as a primary banking channel actually diminished from the 2003 survey. While some of this is due to the current branch banking "renaissance," it also represents a view, by some, that security concerns are tempering the enthusiasm of banks — and their customers for the Internet.



Over 17 percent of community bankers feel that Internet banking will be their primary delivery channel by 2007.

The growth of online banking and related financial services, coupled with the ever expanding use of the Internet by consumers to manage their daily lives (view and pay monthly statements, make purchases and obtain information), has created a set of risks that are extremely difficult to manage.

Just as banks have learned that the Internet provides a low cost means of reaching customers, criminals have discovered that it also provides a low cost and relatively anonymous way to commit fraud. *Nowhere is the criminal's use of the Internet to commit fraud and identity theft more evident than the recent development and growth of phishing.*

What is Phishing?

Phishing is a relatively new, but quickly spreading online scam that seeks to steal credit card numbers, account information, Social Security numbers, passwords, and other sensitive information from your institution's customers. And criminals will tarnish your institution's good reputation in doing it. Phishing is a high-tech tactic that uses fake e-mail, fraudulent Internet addresses, imposter Web sites, and "pop-ups," to impersonate your institution and trick your customers into disclosing their personal data, which, in turn, is then used to obtain money or credit fraudulently.

Phishing is successful and particularly troubling for the banking industry because:

- Many of the elements of phishing attacks are beyond the banks' control because the activity is directed against individual users and their personal computers (PCs), as well as targeted at non-banks (utility companies, retailers, etc.) that use and retain customers' financial information.
- Monitoring for phishing e-mails and fraudulent Web sites is extremely difficult given the magnitude of the environment (the Internet) that needs to be monitored.
- Phishing can sometimes be perpetrated by foreign crime rings which can make investigation, capture, and prosecution difficult.

Anatomy of a Phishing Scam

Here's how a basic phishing scam works: A customer receives a fraudulent e-mail that purports to be sent by a trusted source, such as your institution. In order to make the e-mail convincing, it often displays copies of your institution's insignia, logos, and other trademarks. These e-mails may vary significantly, and some might only make casual reference to your institution. Some fraudulent e-mails claim that the individual's personal information is necessary to assist in the fight against terrorism or for some other alleged legal or beneficial purpose. Other e-mails purport to be from government agencies or private sector entities, such as Internet auction sites or electronic payment services. Some even tell customers that to protect themselves against phishing, they should confirm their account information by responding to the very phishing e-mail they are reading, or by clicking on a link embedded in the phishing e-mail!

While fraudulent e-mails vary in content, they generally carry a common theme essential to their success: customers must take action immediately or risk losing access to their account. This common element of what is termed "social engineering" is necessary because the likelihood of tricking or deceiving customers rises significantly if customers are pressured into taking action quickly, before they have an opportunity to validate the authenticity of the e-mail or perhaps even consider whether their bank would ever request such action.

If taken in by the fraudulent e-mail, customers will click on an image or link that directs them to a Web site where they are asked to provide confidential personal and financial information. Customers may also cut and paste a link into their Internet browser that opens such a Web site. In some cases, particularly unguarded customers will simply respond to the e-mail directly with

Phishing expeditions can range from an elaborate Web site with fake bank graphics to a simple text e-mail invitation to get a great rate on a mortgage.

personal information. Hard and fast technological solutions to stop phishing do not exist, so it is important for your institution's employees and customers to do all they can to prevent this crime from occurring. For additional detailed information about phishing, how it works, and related electronic scams please refer to Appendix I.

Is Your Bank Really a Target?

Phishers are criminals, just like other bank robbers. And as long as financial institutions are where the money is housed, robbers will continue to go after banks — but unlike in the “wild west,” their weapons of choice today are more likely to be computers than six-shooters. According to the Anti-Phishing Working Group, an industry and law enforcement association, 81 percent of the phishing attacks during March 2005 attacked a financial services brand.

Imagine this scenario: Spam e-mails appear to come from your bank. Some of your bank customers believe the e-mails are actually from your bank, and thus provide confidential information (account numbers, personal identification numbers, Social Security numbers). As a result of their actions, they then experience unauthorized withdrawals or transfers from their accounts. In some instances, criminals use this information to open new accounts at other institutions, exposing your customers to identity theft.

Concerned and, in some instances, outraged customers begin clogging your phone lines and call center. Days and dollars are spent salvaging your technology, soothing upset customers, and doing damage control for your brand.

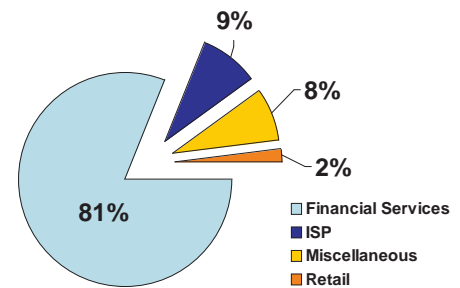
While the picture we have just painted generally depicts the impact on larger financial institutions, community banks are not immune. More phishers are targeting smaller institutions that have not yet dealt with phishing, or lack the infrastructure (technology, security, legal, communications and marketing) to immediately address it. Don't think your bank is immune. There have already been instances where customers of banks in the under \$100 million asset range received e-mails, claiming to be from their bank, asking for their personal financial information.

While community banks and their customers may become victims of elaborate phishing scams incorporating an institution's graphics or other intellectual property, more likely is the prospect of community bank customers receiving a mundane e-mail, allegedly from their bank, indicating that they stand to get a great rate on a mortgage if they “click here” and fill in the online application:

From: Bank of Anytown [loans@bankofanytown.com]
To: John Doe
Re: Bank of Anytown mortgage offer

Congratulations! Bank of Anytown is proud to offer you a home equity loan at the low rate of 2.99%. Just click here to accept this one-time only opportunity:
www.bankofanytown.com/mortgageoffer.asp.

Hijacked Brands by Industry Sector



Source: Anti-Phishing Working Group, March 2005.

There are instances where customers of banks in the under \$100 million asset range received e-mails, purportedly from their bank, asking for their personal financial information.

How Your Customer is Targeted

Even if your institution has never been the target of a phishing scam, your customers generally have. A recent First Data Corporation® poll indicated that 43 percent of respondents had received a phishing e-mail. And that is just the percentage that realized they have received a phishing e-mail. The actual percentage of those receiving such e-mails is undoubtedly much higher.

In addition to phishing expeditions supposedly from a specific financial institution, your customers' personal financial information is being phished in a variety of ways without referencing any specific financial institution. These scams are particularly dangerous to community banks. It is easy for a customer to recognize and ignore scams referring to a specific institution if they do not bank there. Scams that are not institution-specific, however, may entrap a large number of victims across a broad spectrum of financial institutions. Some recent examples of these broader-based phishing scams include:

ABA – The American Bankers Association was the target of a phishing scam. E-mails claimed that "...[due] to the extensive number of credit card frauds, ABA has decided to take preventative countermeasures in order to ensure the highest level of security and safety for the customers of its member banks." The "preventive countermeasures" included verifying bank and credit card information, in addition to Social Security numbers and other identifiers.

FDIC – The FDIC has been victimized by phishers on several occasions, with millions of spam e-mails sent to consumers allegedly from the FDIC claiming that the recipients' deposit insurance would be revoked if they did not respond with their personal financial information.

PayPal – A message, apparently from an America Online account, told recipients their account was eligible for a \$200 payment. The fraudulent e-mail linked to a fake PayPal page that collected consumers' private financial information.

American Red Cross – E-mail reacting to the September 11th disaster sent recipients to fake Web sites where people used credit cards to make "donations" that ended up in criminals' pockets.

While customers are well aware of which financial institutions they use, they are of course usually unaware of whether their bank is an ABA member, or they may be concerned that their deposit insurance might be canceled if they do not answer an e-mail claiming to be from the FDIC. The fact that organizations such as the ABA and FDIC have been victims of phishing expeditions points to phishers' adaptability. No customer is immune, regardless of the size or location of his or her financial institution.

How Often Are Phishers Successful?

According to the Anti-Phishing Working Group, in one month alone there are between 10,000 and 20,000 unique phishing attacks. Each phishing attempt can result in hundreds of thousands of consumers receiving fraudulent e-mail industry-wide, so even if the criminals' success rate seems relatively low — three percent or even just one percent — thousands of customers can be affected. And when phishers are successful in getting some of your customers' personal information, that can also mean that they were also successful in gaining access to their bank account or in using their credit card. A single case of identity theft can cause thousands of dollars in losses to your institution and cost both the consumer and your institution countless hours in damage control, sapping valuable business resources and straining the relationship between you and your customers.

Phishing attacks that are not institution-specific, such as e-mails purporting to be from the ABA or FDIC, may entrap a large number of victims across a broad spectrum of financial institutions.

How Phishing Scams are Evolving

Phishing scams are constantly evolving. As a result, the ABA has developed an Anti-Phishing Web page, easily accessible at <http://www.aba.com/About+ABA/phishing.htm>, where the most recent information on phishing and other scams will be maintained. Please visit it often, and consider subscribing to ABA's free eAlert bulletin, in order to ensure that your institution is aware of the most current trends in this area. To subscribe to the eAlert, or any of ABA's e-mail bulletins, please visit http://www.aba.com/About+ABA/listserv_overview.htm.

Initially, phishing expeditions generally entailed the standard bogus e-mails that we have described up to this point. Eventually, scammers found that they could take advantage of vulnerability in the Internet Explorer browser that allowed them to “spoof” or imitate, a bank's URL (Uniform Resource Locator — it's Web address) in the browser address line, making customers believe they were at the bank's site when they were actually at a scam site.

Phishing incidents have continued to become more sophisticated, relying on spyware and Trojan horses (please see glossary for these and other terms) to capture customer information by installing keystroke loggers (software that captures the user's keystrokes, usually unbeknownst to the user) on your customers' PCs. These keystroke loggers wait patiently on the PC until your customer types in a password and ID that can be associated with a financial institution Web site, at which time the information is sent from the PC to the criminal.

Phishers have also turned to “pharming,” which takes advantage of a vulnerability in the Domain Name Server (DNS) that directs traffic around the Internet. A DNS translates domain names into the numeric Internet Protocol (IP) address that is actually used to route Internet traffic. For example the domain name Mybank.com might translate to 198.105.232.4. Pharming can periodically “poison” the server, causing it to reroute Internet traffic to a fraudulent Web site when customers attempt to visit a legitimate site. While there have been few documented instances of pharming, it is a trend the financial services industry is taking seriously and is actively working to counteract.

You may have also heard or read about “spear phishing,” a more surgically precise scam in which a criminal has some specifics regarding your customer (say his or her deposit account number, for example) and e-mails him or her with a request for the PIN. The e-mail would likely contain the account number, giving your customer the impression that the communication legitimately came from your institution. The scams keep changing, making your institution's efforts to combat and manage phishing scams somewhat akin to eternal vigilance. The following section is designed to provide you with resources to develop your defenses.

Phishing scams are constantly evolving. The ABA has an Anti-Phishing Web page where the most recent information on phishing and other scams are maintained.



To sign up for the ABA's free eAlert e-mail bulletin visit:

http://www.aba.com/About+ABA/listserv_overview.htm

Preventing and Resolving Phishing Scams

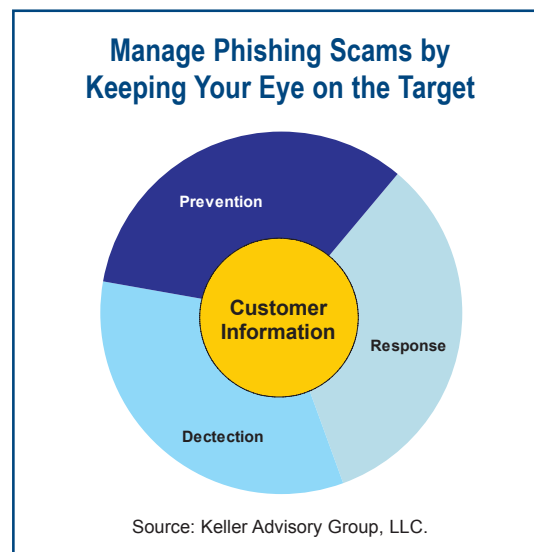
Banks can combat phishing schemes by educating their customers, installing fraud detection software, and working with industry coalitions. Industry coalitions, along with law enforcement agencies, are working to educate customers, to find phishers, shut down their Web sites and punish them. Since anonymous scammers are so elusive — and are often physically based outside of the United States — many banks have posted anti-phishing tips on their Web sites or have mailed fraud information to their customers. The more your customers know about phishing and other identity theft scams, the less likely they will be victims of these schemes.

In order to effectively address phishing and other forms of online scams, consider developing a comprehensive set of procedures that focus on **Prevention, Detection** and **Response**. We will go into greater detail on these three areas later in this chapter.

Prevention focuses on the business practices and technical solutions that either reduce the number of phishing attempts customers receive or that educate customers so they are less likely to respond to phishing attempts. There are a number of techniques that can be used in this area, but the most important are customer education and the development of effective business practices.

Detection solutions use a number of different resources to discover phishing e-mails that have just been or are about to be released. As soon as an e-scam attack hits, your bank servers will probably start getting deluged with bounce-back e-mails and calls from wary customers. Gather all the details about the attack that you can. Most importantly, determine the IP address of the offending Web site and who controls it. Some Internet Service Providers (e.g., America Online, Earthlink) will assist you with this. US-CERT will also provide assistance. In some cases, a bank must involve its legal department, as laws relating to online fraud, especially international law, are complex and evolving.

Response planning involves the creation and execution of a comprehensive set of procedures to respond to phishing incidents. It includes taking down the spoofed Web sites, keeping customers and senior management informed of the institution's progress in addressing these scams, and coordination with law enforcement. A phishing attack or other e-scam is a significant information security incident that requires a well-planned and executed response. All financial institutions should assess their risks and formulate appropriate plans to defend against and respond to attacks.



The more your customers know about phishing and other identity theft scams, the less likely they will fall victim to these schemes.

Preventing Successful Phishing Scams

Your Bank's Web Site is a Powerful Educational Tool

Internet banking is not only a safe and effective way for your customers to manage their money, it is also an effective delivery method by which to communicate important information to your customers. Your customers should understand that just as they would not share their financial information with a stranger who came knocking at their front door, they also should not give out their personal information online unless they initiated the transaction.

Fortunately, your bank's Web site is an excellent way to communicate this message — it can be a powerful tool in the fight against fraud, along with statement stuffers, in-branch collateral, advertising, and public service announcements (PSAs).

When structuring an educational eScam page, consider incorporating the following items:

Creating a Web Resource

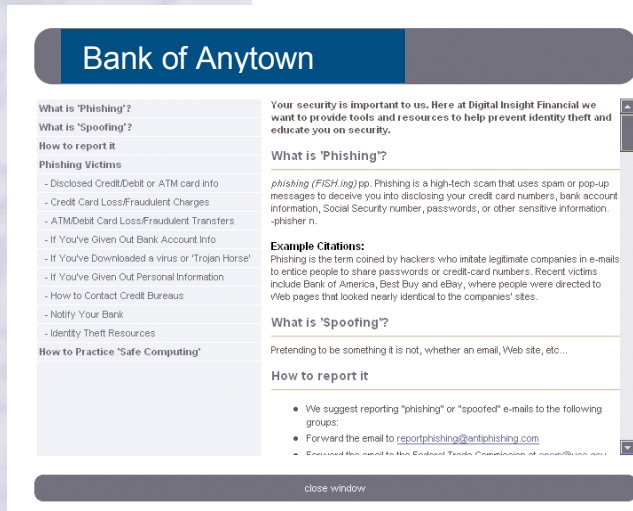
To catch your customers' attention, you may wish to begin a section on your bank's Web site about phishing with powerful language such as, "Consumer Alert" or "Alert: Don't fall victim to online scams." When clicked on, the user should land in a section that covers the various aspects of online fraud, which may include the following subsections:

- What is Phishing?
- What is Spoofing?
- How to Report Phishing/Spoofing
- Phishing Victims Assistance
- How to Practice Safe Computing

The detailed text for each of the subsections, which you can copy from this ABAWorks and use on your own Web site, can be found in Appendix I and is also available on the ABA Anti-Phishing Web page.

Your institution's Web site is an always-on representation of your business to your customers. Therefore, it must remain credible, informative, and consistent. In addition to educating your customers on the key aspects of phishing and spoofing fraud, you should use it to communicate the message that your bank is taking threats against customers' personal financial information seriously and is deploying software solutions and business policies to prevent attacks against the bank and its customers.

Internet banking is not only a safe and effective way for your customers to manage their money. It is also an effective tool to communicate important information to your customers.




Statement Stuffers Can Also be Valuable

The ABA has developed a statement stuffer, available at www.bankstuffers.com, which may be used to help educate customers as to the threat phishing presents and how to practice safe online banking.

Safe Online Banking

Technology, accountability and ongoing communication help us insure that your online banking experience is safe and secure.

SPECIAL ADVISORY:
Phishing Scams 

There is currently widespread use of an Email scam known as "Phishing," in which identity thieves send emails to bank customers asking them to "verify" information or otherwise divulge personal data.




WE NEVER SEND EMAILS REQUESTING PERSONAL INFORMATION. We will never ask you to "verify" information. We will never ask you to click on a special site link to do so. While emails of this nature may look like they are from us, and even use our logo, they are most likely a "phishing" scam. **Do not answer them.** If you receive an email purporting to be from us, do not hesitate to call us to confirm it.

When you bank online with us, your transaction is safeguarded by the full extent of available technology (*see reverse for more details*).


INTERNET SECURITY

Safe Online Banking

When you use the Internet to visit us, whether it's to learn about rates, to review your account, or to transact other business, you are entering a secure area. Here are just of the few of the safeguards we have in place to help ensure your personal security when visiting us online:

-  **Your Password**—We'll ask you to develop a secret password that only you will know. Only then will you be able to review personal information about your account.
-  **Our Privacy Policies**—Our entire staff is dedicated to protecting the personal privacy of you, our customer. We have stringent privacy policies in place, and have instituted bank-wide measures to assure that they are strictly observed.
-  **Encryption Software**—"cryptographic software" makes it possible to scramble a message between two parties (you and your bank), in a way that allows the message to be decoded *only by one of the two parties*.

When you bank with us you can bank with confidence...online, on the phone or in person!

 Presented by the American Bankers Association
© 2005 FINANCIAL EDUCATION CORPORATION



To order the "Safe Online Banking" and other statement stuffers visit:

www.bankstuffers.com

Customer Phishing Prevention Tips

This is a list of common tips that you can utilize as part of your program to educate your customers on ways they can stay safe while online. These tips have also been incorporated in the sample phishing Web site language in Appendix I.

Be suspicious of any e-mail with urgent requests for personal financial information. Phishers have been known to include upsetting or enticing (but false) statements in their e-mails to get people to react immediately, a practice known as social engineering. More recently, some phishers have toned down their language as e-mail recipients have become more aware of the use of this tactic. Either way, the e-mail typically asks for information such as usernames, passwords, credit card numbers, Social Security numbers, etc.

Be careful of e-mails that are not personalized and/or contain spelling errors and awkward syntax and phrasing. Many phishing e-mails are sent in great bulk and, therefore, are not personalized. If you are suspicious of an e-mail claiming to be from your institution that is not personalized, call your institution before responding. Many also are being sent from other countries, from individuals for whom English is a foreign language, thus resulting in misspelled words and awkward syntax and phrasing.

Be careful of personalized e-mails that ask for personal financial information. Be suspicious of any e-mail that contains some personal financial information, such as a bank account number, and asks for other information such as a PIN. Your bank will never ask for or send you personal financial information by e-mail.

Do not use links in an e-mail to get to a bank's Web page. Instead, call the bank on the telephone to confirm the address, or log onto the bank's Web site directly by typing in the Web address in your browser.

Do not complete forms in e-mail messages that ask for personal financial information. Your bank would never ask you to complete such a form within the body of an e-mail message.

Only communicate information, such as credit card numbers or account information, via a secure Web site or the telephone. A secure Web server designation can be found by checking the beginning of the Web address in your browser's address bar — the address should begin "https://..." rather than just "http://..." While you can not be completely sure that a Web site is secure when its address starts with "https," you can be sure the Web site is not secure when it does not.

Regularly log on to your online accounts and check your bank, credit and debit card statements to ensure that all transactions are legitimate. One of the real advantages of banking online is being able to regularly review your account for unauthorized or unusual activity. If anything is suspicious, contact your bank and appropriate card issuers immediately.

Ensure that your Internet browser program is up to date and that the most recent security updates have been applied. Always visit your browser provider's home page to download the latest security patches even if they don't alert you to do so. For example, if you use Microsoft's Internet Explorer, you will find security updates located on Microsoft's Web site.

Business Practices That Defend Your Institution

In addition to educating your employees and customers about how to identify and protect themselves from potential e-scams, there are concrete steps your bank can take to defend against attacks before they even happen.

Consistently communicate your bank's corporate policies to customers so they know what to expect from online communications with your bank. That way, they are more likely to detect an e-scram that tries to exploit your bank's online presence. Of course, this means your bank must create corporate policies for e-mail content so that legitimate e-mail cannot be confused with phishing. Again, communicate these policies to customers — and make sure you follow them.

Here are some guidelines to follow when establishing a policy for online content and e-mail:

Avoid embedded hyperlinks. While embedded hyperlinks in e-mail can make the customer experience easier, they can also create more opportunities for fraud. A safer alternative is to provide a text-only link (a link that when 'clicked' on, will not automatically redirect a customer to another Web page) in the e-mail that customers must type or cut-and-paste into their browser. Regular customers will likely have a bookmark for the institution, which makes this process easier. Institutions should carefully evaluate the impact on customer experience versus the increased security provided by implementing such a policy.

Avoid e-mail forms. As with embedded hyperlinks, e-mail forms can make the customer experience easier when a bank is requesting information. However, the mechanism is easily used by criminals to collect the same information. The bank should educate customers that legitimate e-mails will never contain forms requesting personal information.

Authenticate e-mails. Provide a way for the customer to validate that e-mail from your bank is legitimate. The customer should be able to determine that an e-mail is from your institution and not a phisher. To do that, the sending institution can establish a customer telephone hotline to answer any questions customers may have about an e-mail purporting to come from your bank. Another method is to repeat e-mailed information on your bank's Web site so customers who question their e-mail can check the information against that found on your institution's official Web site.

Monitor the Internet for use of your bank's name. Phishing Web sites generally appear somewhere on the Internet prior to the launch of phishing e-mails. These sites often misappropriate corporate trademarks in an attempt to appear legitimate. Your bank can utilize online search engines to monitor your appearance on the Internet to detect such Web sites before they cause harm. These search engines are available from various vendors, or this service maybe contracted to be performed by a vendor.

Brief call center personnel. Instruct call center employees to identify and notify management of reports of suspicious e-mails. Give them copies of any e-mail sent to customers by your bank so that they can confirm the legitimacy of such correspondence when customers call to confirm.

Beef up Internet security. Implement quality anti-virus, content-filtering, and anti-spam solutions at the Internet gateway (see glossary). 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 e-mails. And, of course, employ a professional-grade and constantly monitored Internet firewall, or multiple firewalls, at all times.

Promise — and deliver on — legal action. Make it known your bank will prosecute e-scram perpetrators. Have a dedicated e-mail address posted on your bank's web site for reports, e.g., **abuse@yourbank.com**, or **spoof@yourbank.com**, and encourage your customers to report all suspicious communications or Internet activity. Software companies that have set up a reporting structure for pirated software have seen declines in e-scams.

Encourage your customers to use latest technology. Advise your customers to ensure their computer's security software is current and to download and install the most recent updates. Remind customers to obtain and use the latest update for their Web browser and operating system software.

Make your communications unique. When at all possible, personalize e-mails to consumers so that consumers have a greater assurance of the e-mail's legitimacy. Register domain names that are similar to the name of your bank so that consumers are less likely to confuse a false Web site with the legitimate Web site. Practice consistent branding. Keep Web site certificates up to date so that consumers are assured of the site's legitimacy.

Explore other legal options. Consider establishing a trademark for the domain name of the bank. Under the Anticybersquatting Consumer Protection Act, 15 U.S.C. 1125(d)¹, a firm may be able to initiate immediate action in federal district court against the suspicious Web site to protect the firm's trademark.

Detecting Phishing and Other Electronic Scams

As this guide has pointed out, successful phishing depends on the criminal's ability to manipulate the behavior of a consumer. As a result, self defense relies in large part on the common sense of the user. Educating consumers is the first line of defense for both them and the banking industry; it can't be repeated enough: *Don't send personal data such as passwords or bank accounts over the Internet.* The automated detection of phishing fraud is very difficult. There is no software that can really help because only an extensive forensic analysis by law enforcement can prove the evidence of phishing. You can only mitigate the problem by:

- 1) Blocking of known URLs of phishing Web sites.
- 2) Blocking phishing scam e-mails that are sent en masse.

There are a variety of different techniques that can be used to either discover phishing e-mails that have just been or are about to be released or to recognize unusual characteristics of specific user log-ons.

Certain intrusion prevention technologies can block against URL spoofing, which is a common technique used in phishing attacks. Lists of known phishing URLs that can be used to create a block list can also be obtained from vendors or some Internet Service Providers (e.g., America Online, Earthlink). Other applications enable the bank to block a transaction or require the user to provide additional information if the account is being accessed from a mismatched or unknown location. Still others recognize various attributes of the user's PC and connection in order to detect sessions that are either risky or atypical for that particular user.

¹ <http://www.patents.com/acpa.htm>.

There are also companies that banks can hire that monitor the Internet on a continual basis, searching for the potential illicit use of bank brands and other intellectual property. These companies use applications and personnel that generally evaluate Internet activity in chat rooms and forums and analyze spam for signs of existing or potential phishing or other illegal activity.

To assist in finding solutions in the fight against phishing, the Anti-Phishing Working Group has published an Anti-Phishing Solutions Directory that can be found on the ABA Anti-Phishing Web site at <http://www.aba.com/About+ABA/phishing.htm> or on the Anti-Phishing Working Group Web site at www.antiphishing.org.

Responding to a Phishing Attack

Response planning involves the creation and execution of a comprehensive set of procedures to respond to phishing incidents. It includes taking down the spoofed Web sites, keeping customers and senior management informed of the institution's progress in addressing these scams, and coordinating with law enforcement. A phishing attack or other e-scam is a significant information security incident, requiring a well-planned and well-executed response. All financial institutions should assess their risk and formulate appropriate plans to defend against and respond to attacks. A comprehensive response plan should, at a minimum, include three core steps:

Step 1: Investigate

Keep in mind that a phishing attempt — both the e-mail and the spoofed Web site (if there is one) — must appear legitimate in order to be successful. Accordingly, phishing investigation procedures must examine both the phishing e-mail itself and the capture site, which is the site to which consumers are directed to enter their personal and confidential information.

- An initial investigation of the e-mail should involve the collection of information to assist in identifying the original source of the e-mail. Capturing the URL of the phishing e-mail will help trace the fraudulent e-mail.
- An initial investigation of the spoofed Web site should include an examination of the phishing e-mail and Web site sufficient to determine the true IP address of the capture site and data transfer site (where possible).
- Prioritize the incident based on the scope of impact on your bank's customer base, nature of the phishing attack, and location of the phish capture site. This must be a subjective decision by your bank.
- Notify law enforcement. While this is not always the most effective way to get a fraudulent site taken down, it is a positive and important step to inform the authorities of the problem. The FBI and Secret Service are generally more concerned with large scale patterns and mass deceptions than they are individual smaller dollar ones, and — until a customer has fallen for a scam and suffered damages — there may have been no law broken. Nevertheless, agents may be able to intervene on your behalf and contact the offending Internet Service Provider (ISP) that is hosting the fraudulent Web site. The threat of subpoena alone may be enough to trigger a response. If the phisher is physically located outside of the United States, you will need to work with U.S. law enforcement agencies in order to involve Interpol and other nation's law enforcement agencies.

Step 2: Respond

E-mail Server

- If different from the fraudulent e-mail server, contact the fraudulent e-mail server's owner for evidence and have the mail server shut down. Monitor and follow up in case the server administrator fails to properly secure hacked equipment or close any hidden means of server access.

Spoofed Web Site

- Contact the ISP or host company and demand that information related to the phishing incident be secured and the site be dismantled.
- For a domestic ISP/host company, determine whether a demand may be made under the Digital Millennium Copyright Act.² Contact the U. S. Computer Emergency Response Team³ at: <http://www.us-cert.gov>.
- For a foreign ISP or hacked site: Determine if the country has a Computer Emergency Response Team (CERT) and contact them for assistance. Also contact US-CERT.
- Once the site is down, continue to monitor the bank's primary IP address for a period of time. Sites often reappear shortly after they are first taken down and may continue to appear and reappear for a period of days depending on the security of the site and the technical capability of the host ISP site administrator.

The ABA's Anti-Phishing Web site contains a listing of ISPs, as well as a link to the US-CERT³ site, for your use in the event of an attack.

Step 3: Communicate

A comprehensive response plan includes a communications plan. Communications should be based on the incident's priority level and should include both **internal** and **external** communications.

Internal Notification

All customer contact personnel — from frontline tellers and customer service representatives to all call center personnel — should be able to provide a clear and consistent message to customers who ask about a phishing attempt. Appropriate protocols should be in place to provide employees with timely and consistent information to distribute to customers. Senior management must be kept informed of the status of current phishing attempts and bank personnel's efforts to terminate them. Appendix IV contains a customer activity log to assist in maintaining a written chronology of phishing and spoofing incidents. Investor relations, public relations, and marketing personnel should know the status of active phishing scams. Members of the media can and frequently do either receive the phishing e-mail themselves or are contacted by a financial institution customer under attack; be ready to answer their questions with a message that includes the importance of educating all consumers about online safety. In addition, customer loss prevention or similar ID theft unit personnel should be contacted immediately. They should be given any information on customers who say their personal information or credentials have been compromised as a result of an e-scam.

² <http://www.copyright.gov/legislation/dmca.pdf>.

³ The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

All customer contact personnel should be able to provide a clear and consistent message to customers who ask about a phishing attempt.

External Notification

Follow up with law enforcement and any other agencies you communicated with during the initial investigation. Report the phishing attempt to the appropriate agencies listed below. It is important that information about the e-scam be provided to the appropriate agency in order to track trend information and for the various agencies to determine other information that may aid future investigations and prosecutions. There are a number of agencies and groups where e-scam reporting benefits the banking industry:

- Internet Crime Complaint Center (IC3) FBI: www.ic3.gov
- Federal Trade Commission (FTC): www.consumer.gov/idtheft
- Forward fraudulent e-mails to the Federal Trade Commission at: spam@uce.gov
- Anti-Phishing Working Group (APWG): www.antiphishing.org/report_phishing.html
- Local Law Enforcement

In addition, if you come across e-scams targeting other institutions, forward the fraudulent e-mails to the “abuse” e-mail address at the company that is being spoofed (e.g., spoof@mybank.com or phishing@mybank.com), or if such an address is unavailable, to the company’s Web master.

When forwarding spoofed messages, always include the entire original e-mail with its original header information intact. To learn how to do this, please visit <http://www.uwo.ca/its/doc/hdi/email/forwardwithheaders.html>.

If you contract for your Internet banking services with a third-party provider, contact them to determine the tools, policies, and procedures they have in place to prevent, detect, and respond to phishing scams perpetrated against their client base.

If it’s not something you’ve done already, your bank can also contract with companies to handle these tasks for you. Cyota, Corillian, Verisign, Internet Identity, MarkMonitor, NameProject and Watchfire all offer take-down services. *(Note: The ABA does not endorse or have any relationship with these companies or any other similar companies and lists them for informational purposes only.)*

When appropriate, depending on the size and effectiveness of the attack, your customers should be notified that your bank has been the victim of a phishing attack. Posting such a notice on your bank’s Web site is one way to notify your customers to be aware that they may receive a potential fraudulent e-mail. Your notice should include instructions on how they may report this activity to you and include guidelines about phishing and how they can avoid becoming a victim.

Sample Web site language that your bank may use can be found in Appendix I.

Examples of corporate anti-fraud policies may be found on the Anti-Phishing Working Group Web site at <http://www.antiphishing.org/resources.html#advice>.

External communication also entails addressing any questions the media may have about the phishing attack and its impact on your institution. Appendix III and V contain some phishing FAQs and media talking points to assist you in your communications.

APPENDIX I

Sample E-Scam/Phishing Web Site Language

The ABA thanks Digital Insight® Corporation for assistance in preparing this ABAWorks. We especially thank them for their contributions made for Appendix I.

Consumer Alert: Don't Fall Victim to Online Scams

Your security is important to us. Here at Bank of Anytown we want to provide tools and resources to help prevent identity theft and educate you on security.

What is "Phishing"?

Phishing (FISHing)

Phishing is a high-tech scam that uses spam or pop-up messages to attempt to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, and/or other sensitive information.

Example Citations

Phishing is the term coined by hackers who imitate legitimate companies in e-mails to entice people to share passwords or credit card numbers.

What is 'Spoofing'?

Pretending to be something it is not, on the Internet, usually an e-mail or a Web site.

How to report Phishing:

We suggest reporting phishing e-mails or spoofed Web sites to the following groups:

- Forward the e-mail to reportphishing@antiphishing.org.
- Forward the e-mail to the Federal Trade Commission at spam@uce.gov.
- Forward the e-mail to the "abuse" e-mail address at the company that is being spoofed (e.g., spoofof@ebay.com).
- When forwarding spoofed messages, always include the entire original e-mail with its original header information intact.
- Notify the Internet Crime Complaint Center of the FBI by filing a complaint on their Web site: www.ic3.gov.

Recommended Actions if You've Become a Victim of a Phishing Scam

If You Have Given Out Your Credit, Debit, or ATM Card Information

- Report the incident to the card issuer as quickly as possible.
- Report using toll-free numbers and 24-hour service that many companies have established to deal with such emergencies.
- Request your card issuer close your compromised account number and reissue you a new card with a different number.
- Monitor your account activity and review account statements carefully after the information loss.
- If any unauthorized charges appear, call the card issuer immediately and follow up with a hard copy letter via a traditional delivery service such as the U.S. Postal Service (keep a copy for yourself) describing each questionable charge.

Credit Card Loss or Fraudulent Charges

Your maximum liability under federal law for unauthorized use of your credit card is generally \$50. However, that \$50 potential liability probably does not apply for unauthorized telephone and Internet transactions because there is “no means to identify the cardholder” in those cases. For more information, please see Appendix II.

ATM or Debit Card Loss or Fraudulent Transfers

- Your liability under federal law for unauthorized use of your ATM or debit card depends on how quickly you report the loss.
- You risk unlimited loss if you fail to report an unauthorized transfer within 60 days after your bank statement containing unauthorized use is mailed to you for transactions made after that 60-day period.

If You Have Given Out Your Bank Account Information

- Report the theft of this information to the bank as quickly as possible.
- Request your bank close the compromised account and re-open a like account with a different number.

If You Have Downloaded a Virus or ‘Trojan Horse’

Some phishing attacks use viruses and/or “Trojan Horses” to install programs called “key loggers” on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, user names and passwords, Social Security numbers, etc. If this happens, it’s likely you may not be aware of it until you notice unusual transactions on your account.

To minimize this risk, you should:

- Install and/or update anti-virus and personal firewall software.
- Update all virus definitions and run a full scan.
- If your system appears to have been compromised, repair it and then change your password again, since you may well have transmitted the new one to the hacker.
- Check your other accounts! The fraudsters may have helped themselves to many different accounts: eBay account, PayPal, your e-mail ISP, online bank accounts, online trading accounts and other e-commerce accounts, and everything else for which you use online passwords.

If you have given out your personal identification information

If you believe you have given out personal information such as your name, address, and Social Security number to someone who may use it for fraud:

Contact the three major credit reporting agencies — Experian, Equifax and TransUnion — and do the following:

- Request that the agencies place a fraud alert and a victim’s statement in your file.
- Request a free copy of your credit report to check whether any accounts were opened without your consent.
- Request that the agencies remove inquiries and/or fraudulent accounts stemming from the theft.

Major Credit Bureaus

Equifax - www.equifax.com

- To order your report, call: 800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241.
- To report fraud, call: 800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241.
- Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to request a copy of your report.

Experian - www.experian.com

- To order your report, call: 888-EXPERIAN (397-3742) or write: P.O. Box 2002, Allen, TX 75013.
- To report fraud, call: 888-EXPERIAN (397-3742) and write: P.O. Box 9530, Allen, TX 75013. TDD: 1-800-972-0322.

Trans Union - www.transunion.com

- To order your report, call: 800-888-4213 or write: P.O. Box 1000, Chester, PA 19022.
- To report fraud, call: 800-680-7289 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634 TDD: 1-877-553-7803.

Additional Actions to Take

- If bank accounts were set up without your consent, close them.
- Contact your local police department to file a criminal report.
- Contact the Social Security Administration's Fraud Hotline to report the unauthorized use of your personal identification information.
- Notify the Department of Motor Vehicles of your identity theft.
- Check to see whether an unauthorized driver's license number has been issued in your name.
- Notify the passport office to be on the lookout for anyone ordering a passport in your name.
- File a complaint with the Federal Trade Commission. Ask for a free copy of "ID Theft: When Bad Things Happen in Your Good Name," a guide that will help you guard against and recover from your theft — and guard against it in the future.
- File a complaint with the Internet Crime Complaint Center (IC3) by visiting their Web site: www.ic3.gov. IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), with a mission to address fraud committed over the Internet. For victims of Internet fraud, the Center provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation.
- Document the names and phone numbers of everyone you speak to regarding the incident. Follow up your phone calls with letters. Keep copies of all correspondence.

Identify Theft Resources

<http://www.consumer.gov/idtheft/>

<http://www.identity-theft-help.us/>

<http://www.identitytheft.org/>

<http://www.usdoj.gov/criminal/fraud/idtheft.html>

<http://www.ic3.gov>

<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>

How to Practice Safe Computing

The number and sophistication of phishing and spoofing scams sent out to consumers is continuing to increase dramatically. While online banking is widely considered to be as safe as or safer than in-branch or ATM banking, as a general rule you should be careful about giving out your personal financial information over the Internet. Remember, no reputable financial institution will ever request your personal information via e-mail.

Here is a list of recommendations to follow in order to avoid becoming a victim of scams:

1. **Be suspicious of any e-mail with urgent requests for personal financial information.** Phishers have been known to include upsetting or enticing (but false) statements in their e-mails to get people to react immediately. More recently, some phishers have toned down their language, as e-mail recipients have become more aware of the use of this tactic. Either way, the e-mail typically asks for information such as user names, passwords, credit card numbers, Social Security numbers, etc.
2. **Be careful of e-mails that are not personalized and/or may contain spelling errors and/or awkward syntax and phrasing.** Many phishing e-mails are sent in great bulk and, therefore, are not personalized. If you are suspicious of an e-mail claiming to be from your institution that is not personalized, call your institution before responding. Many also are being sent from other countries from individuals for whom English is a foreign language, thus resulting in misspelled words and awkward syntax and phrasing.
3. **Be careful of personalized e-mails that ask for personal financial information.** Be suspicious of any e-mail that contains some personal financial information, such as a bank account number and asks for other information, such as a PIN. Your bank will never ask for or send you personal financial information by e-mail.
4. **Do not use links in an e-mail to get to any Web page.** Instead, call the bank on the telephone to confirm the address, or log onto the Web site directly by typing in the Web address in your browser.
5. **Do not complete forms in e-mail messages that ask for personal financial information.** Your financial institution would never ask you to complete such a form within an e-mail message.

How to Practice Safe Computing - Continued

6. **Only communicate information, such as credit card numbers or account information, via a secure Web site or the telephone.** When submitting financial information to a Web site, look for the padlock or key icon at the bottom of your browser, and make sure the Internet address begins with “https.” A secure Web server designation can be found by checking the beginning of the Web address in your browser’s address bar — the address should begin “https://...” rather than just “http://...” While you can not be completely sure that a Web site is secure when its address starts with “https,” you can be sure the Web site is not secure when it does not start with “https.”
7. **Regularly log on to your online accounts and check your bank, credit and debit card statements to ensure that all transactions are legitimate.** One of the real advantages of banking online is being able to regularly review your account for unauthorized or unusual activity. If anything is suspicious, contact your bank and all card issuers immediately.
8. **Ensure that your browser is up to date and security patches applied.** Always visit your browser’s home page to download the latest security updates even if they don’t alert you to do so.
9. **Use online statements to reduce the volume of paper mailed.** Paper today is the cause of more actual instances of identity fraud than are electronic thefts.

APPENDIX II

Understanding Your Bank's Liability

Below is general information about liability laws and regulations that may apply when information gathered from electronic scams are used for fraud. It provides only guidance and does not constitute legal advice. Banks should consult counsel.

Regardless of how information is obtained to perpetrate fraud, generally consumers are not responsible or liable for accounts that they did not open. Nor are they liable for unauthorized transactions against their own, legitimate accounts, assuming they have notified the financial institution in a timely fashion. However, the specific limitations of their liability for unauthorized transactions on their account vary depending on the type of account as well as the type of transaction.

Accounts Fraudulently Opened in a Customer's Name

If information obtained through phishing is used to open a new account, whether it is a deposit account or credit account, under basic contract law, consumers are not liable for transactions on the account because they did not agree to open the account. This applies whether the account is a checking account, credit card account, mortgage loan, car loan, etc.

Unauthorized Credit Card Transactions

The Truth in Lending Act and Regulation Z governs consumers' liability for unauthorized transactions on credit card accounts. Under Regulation Z, authorized transactions are those transactions made by someone who has actual, implied, or apparent authority to use the account, as determined by state law. Criminals who obtain credit card information through phishing and use that information to make charges on the account generally do not have authority to use the card, even though the consumer gave the information to the phisher. Card holders are generally only liable for the first \$50 for unauthorized use of their credit card. However, that \$50 potential liability probably does not apply for unauthorized telephone and Internet transactions because there is no means to identify the cardholder in those cases.

Under Regulation Z, the consumer must mail a notice about a billing error, which includes unauthorized transactions, no later than 60 days after the card issuer sent the first statement containing the unauthorized transaction in order to trigger the billing error procedure provisions.

The notice must contain information that allows the card issuer to identify the account name and number and the type, date, and amount of the unauthorized transaction.

Once the card issuer receives the notice, it must deliver written acknowledgement within 30 days of receipt, assuming the issue has not been resolved beforehand. The card issuer must resolve the matter and notify the consumer within two complete billing cycles (but not later than 90 days) after receiving the notice of the unauthorized transaction.

Until resolution of the claim, the consumer need not pay the amount or any related charges, such as finance charges, nor can the creditor report or threaten to report the consumer to a credit bureau or anyone else.

Deposit Accounts

E-scams can supply sufficient information to access customer deposit accounts in a variety of ways. Using the information obtained, criminals might be able to use account or debit card numbers and other information to make purchases over the Internet or by phone. They might be able to create counterfeit checks. Using online banking, they could transfer funds out of the customer's account into another account. In sophisticated schemes, they might even be able to create a counterfeit debit card. While generally consumers are not liable for these unauthorized transactions, the rules governing consumer liability for unauthorized transactions on deposit accounts vary, depending on whether the transaction was made electronically or by paper.

Electronic transactions are subject to the Electronic Funds Transfer Act (implemented by Regulation E). Liability for paper transactions is usually determined by the state Uniform Commercial Code, though there are some instances when Check 21 (Regulation CC) may apply.

Electronic Funds Transfers

Electronic fund transfers subject to Regulation E include debit card transactions (ATM, point of sale transactions, and those made via the Internet and by phone), online banking transactions, transfers initiated by telephone, and Automated Clearing House (ACH) transactions, including those initiated by check and converted to ACH.

Generally, under Regulation E, consumers' liability for unauthorized electronic funds transfers made with an access device such as a card or passcode is limited to \$50 if they notify the financial institution within two business days after learning of the loss or theft of the access device. Consumers who fail to report the loss of the access device within two business days may face an increased liability up to \$500.

If the consumer fails to notify the bank about unauthorized transfers appearing on a statement within 60 days after the bank's transmittal of the statement, the consumer's liability is unlimited for subsequent unauthorized transfers — i.e., those made 60 days after transmittal of the statement. However, these periods can be extended for extenuating circumstances, for example, if the consumer was on vacation or ill.

Generally, banks must complete their investigation of a Regulation E claim within 10 business days (20 days for new accounts) and report to the consumer with 30 days after completing the investigation. The time to investigate may be extended to 45 days provided the bank provisionally credits the

account within 10 business days. The period to investigate may be further extended to 90 days if the transfer was not initiated within a state, resulted from a point of sale card transaction, or was made from a new account.

Under Regulation E, the consumers' negligence is not a factor for determining liability. For example, that the consumer wrote the PIN on the back of a card does not absolve the bank from liability if someone steals the card and uses it at an ATM. Similarly, subject to the conditions described above, consumers are generally not liable for losses even if they negligently provided information to a phisher.

Paper Transactions

The liability rules for unauthorized checks, generally governed by state UCC law vary in some important aspects from the laws governing electronic funds transfers. Check the state UCC law applicable to your own bank for specifics.

Under UCC laws, banks may only pay items that the holder of the account authorized in accordance with the bank agreement. Thus, if the criminal uses information obtained from phishing to create a counterfeit check or an unsigned draft, the consumer usually will not be liable. However, under most state UCC laws, the customer's negligence may decrease the bank's liability for any loss. UCC is also less rigid and specific than Regulation E. For example, the time frames for handling a check dispute are not specified. However, because banks may face significant liability for consequential damages if the customer's claim was valid and other items are not paid because the money was not yet recredited, banks should resolve disputes as soon as possible.

In addition, the consumer protection provisions of Check 21 may also have some application. If an item created or submitted by the fraudster is converted into a substitute check, the consumer actually receives the substitute check and not just an image, and the original item or a better copy is necessary to determine the validity of the check, the expedited recrediting provisions of Check 21 apply.

If the consumer submits such a claim, the bank must:

- Produce the original check or a copy that accurately represents the check and demonstrates that the charge is valid, or recredit funds on the first business day following the business day the bank finds the claim valid. If, in the case of a large-dollar item, the bank cannot determine the validity of the claim by the 10th business day, it must recredit the first \$2,500, with the remainder due by the 45th day if the claim still cannot be validated.
- Exceptions are made for new accounts, repeated overdrawers, and when there is "reasonable cause to believe" that fraud is involved. Consumer claims generally must be made within 40 days after the statement is delivered or the date the substitute check is available to the consumer, whichever is later. Longer periods are permitted for extenuating circumstances.

APPENDIX III

Sample Media Talking Points

Reporters may be interested in your bank's perspective regarding phishing and other electronic scams. Listed below are talking points that the ABA uses when talking about phishing. Other talking points are available on a variety of issues in the "Communications Tools" section of www.aba.com.

Key Messages

- Phishing scams — the latest in a long line of criminal attempts at fraud and identity theft — are currently a top priority for all bank security personnel.
- Banks combat phishing schemes by educating their customers, installing fraud detection software, and working with industry coalitions.
- Consumer education is a powerful weapon in the fight against phishing. Many banks have anti-phishing tips on their Web sites and/or have mailed fraud information in their monthly statements.
- Banks have sophisticated software that can detect fraudulent transactions even before the customer may notice. Called "neural network" technology, this software can detect unusual spending patterns and alert bank employees, who can then contact the customer and protect their account.
- Banks work closely with industry coalitions, such as the Anti-Phishing Working Group (www.antiphishing.org), to team up against scam artists. These groups help identify new schemes and develop counter-phishing methods.
- Phishing is a new twist on an old telemarketing scam, it uses new technology — e-mail. Criminals steal the identity of a trusted company and often threaten the consumer with dire consequences if they don't act immediately.

Consumer Tips

- Never give out your personal financial information in response to an unsolicited phone call, fax, or e-mail, no matter how official it may seem.
- Do not respond to e-mail that may warn of dire consequences unless you validate your information immediately. Contact the company to confirm the e-mail's validity using a telephone number or Web address you know to be genuine.
- Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.
- When submitting financial information to a Web site, look for the padlock or key icon at the bottom of your browser, and make sure the Internet address begins with "https." This is no guarantee, but the lack of these icons or "https" does indicate that the Web site is NOT secure.
- Report suspicious activity to the Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center. www.ic3.gov.
- If you have responded to a fraudulent e-mail, contact your bank immediately so they can protect your account and your identity. For information on identity theft, visit ABA's Consumer Connection at www.aba.com.

Background

Phishing attacks use spoofed e-mails and fraudulent Web sites designed to attempt to fool recipients into divulging personal financial data such as credit card numbers, account user names and passwords, Social Security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers, and credit card companies, phishers are able to convince up to five percent of recipients to respond to them.

APPENDIX IV

Customer Activity Log

The Customer Activity Log is designed to assist your bank in maintaining a written chronology of what happened, what was lost and the steps your customer took to report the ID theft incident to various banks and agencies. This log is also available in electronic format at: http://www.aba.com/aba/PDF_Files/GR_idtheftkitcustomer2.pdf.

Incident Details (date, time, location and circumstances of incident)
Methods of Discovery (how did you first discover the incident?)
Statement Review (list of any unauthorized withdrawals, transactions or charges)
Other Information

APPENDIX V

Phishing FAQ

Use this more extensive list of frequently asked questions (FAQ) and answers to help your employees and customers understand common electronic scam tactics.

Q How does phishing work? What is phishing?

The term phishing (FISH-ing) refers to a scam thieves attempt to undertake to steal victims' personal financial information. Most often the scammer sends an e-mail to thousands of people asking for information such as Social Security numbers, credit card numbers, bank account numbers, and personal identification numbers (PINs). Although it seems obvious, the trick to phishing is creating a counterfeit Web site of a trusted financial or other company Web site to which the unsuspecting consumers are directed. The subjects of these e-mails are often "Account Information Update Required" or other phrasing that suggests that the account with the "spoofed" company has been compromised or will be canceled. The counterfeit Web sites register the data entered by the victim and scammers can then use this information to commit fraud and steal the victim's identity by charging purchases and opening new accounts.

Q Where did the term phishing come from?

The term phishing (FISH-ing) was coined because thieves are fishing for your personal financial information. They send out thousands of lures and hook only a few victims. The "ph" comes from a common hacking term. The first type of hacking was called "phreaking." In the mid-1990s, America Online accounts were some of the first hacked accounts and were called "phish." These phish were treated as a form of currency where scammers could trade phish for hacking software.

Q What is spoofing?

Spoofing is something pretending to be something it is not, on the Internet, usually an e-mail or Web site. Typically, it is a technique used to gain unauthorized access to computers, whereby the intruder hijacks a target's root Internet address (known as an Internet Provider or IP address) to make it appear fraudulent e-mails are from a trusted source. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify its identifying information on the Internet. Once criminals have your customer's password, they can use your bank's online banking site to withdraw or transfer funds. Spoofers can be anyone. They can be ordinary criminals out to steal money, competitors trying to cripple your business, disgruntled employees or irate customers. Attacks can be personally motivated or simply random. Spoofing of a bank Web site is nothing more than just another attempt to rob that bank.

Are people falling for phishing scams?

Because, most people have grown increasingly aware of this scam, most phishing e-mails are deleted. However, the sheer quantity of attacks has increased, thus reaching more victims — and the technology the criminals employ has become more sophisticated. Overall, the number of successful attacks is small in comparison to the number of e-mails that are sent out each day as lures. Yet, it's still important to note that roughly 3 percent to 5 percent of people who receive phishing scams take the bait.

How do you know if an e-mail or phone call is “phishy”?

If the e-mail you receive is unsolicited and from a company with which you do no business, you know it is a scam. If you receive an unsolicited e-mail from a company you do hold an account with, you know it's a scam if it asks for personal information the company should already have on file about you: These companies will NEVER ask for personal data by e-mail. If you're still not sure about the legitimacy of an e-mail, call the company at a phone number you know to be accurate.

What should you do if you've given personal information to phishers?

Act immediately. Contact your bank and the companies you deal with and make them aware of the problem as well. Check your bank and credit card statements and contact all credit reporting agencies, such as Experian, Equifax and TransUnion if appropriate. Change all of your online user names and passwords associated with personal accounts.

How do phishers get your e-mail address?

Phishing e-mails are essentially dangerous spam. Spammers utilize a variety of techniques to gather e-mail addresses — Web sites, newsgroups, guesswork and list trading. These are the same methods used by phishers. Phishers do not gather e-mail addresses from bank records; unfortunately, one common misconception by consumers is that their bank actually provided the criminals with their names and e-mail addresses. This is simply not the case.

How do I report a phishing attack?

Many companies that have been spoofed have an e-mail address to which you can send e-mails you receive, for example, **abuse@mybank.com** or **Phishing@mybank.com**. The Internet Crime Complaint Center and the Anti-Phishing Working Group also register phishing scams and are a good resource for more information on what to do if you're a victim of phishing.

What is pharming?

Pharming is a scam that often relies on infected, hacked, or otherwise compromised computers. Once a computer has been compromised, customers attempting to navigate to a legitimate bank's Web site by a customer will be re-directed to a spoofed Web site. This can be accomplished in a number of ways. A virus or malware on a PC can re-route a customer to a spoofed Web site even

when the customer has directly entered the address on their browser. Domain Name System (“DNS”) cache poisoning (altering DNS re-routing) by phishers causes customers to be re-directed by the Domain Name System. DNS addresses are text, such as www.google.com but these are translated into numeric IP addresses. Phishers attack the translation process and redirect your computer to the scamming IP address and Web site. The sites will likely look similar and the information you enter will be sent to the scammer, not to your trusted company.

What is Malware?

Malware (malicious software) is software that is surreptitiously installed on a private computer’s hard drive that is designed to harm or take unauthorized control over a computer system or to steal the data it contains. Malware is often distributed as an attachment to spam and phishing e-mails. When a customer reads the e-mail, they unknowingly install the malware on their computer. Numerous terms are used for different types of malware, usually based upon how they spread and what they are intended to do. Computer viruses, Trojans, and worms can all be used to install malware on a vulnerable computer. Monikers such as spyware, adware, key loggers, and back doors refer to the goal of the malware. Some malware attacks attempt to capture the actual keystrokes entered by an individual on their computer’s keyboard. Your institution may employ sophisticated protections against malware — such as powerful anti-virus programs and firewalls — but often customers’ personal computers are not as highly guarded. Once again, the primary purpose of malware is to steal private information that can be exploited in some way.

What is being done to stop phishing?

Banks combat phishing schemes by educating their customers, installing fraud detection software and working with industry coalitions. These coalitions, along with law enforcement agencies at local, state, federal and international levels, are working together to find phishers, shut down their Web sites and prosecute them to the full extent of the law. Since these anonymous scammers are so elusive — and often based outside of the United States — consumer education is extremely important. That is why most banks have posted anti-phishing tips on their Web sites and have mailed fraud and identity theft prevention information to their customers. The more people know about phishing and other identity theft scams, the fewer victims will be affected by these schemes.

Is online banking still safe despite phishing and pharming?

Online banking is a safe and effective way to manage your money; however, just as you would not share your financial information with a stranger who knocked at your front door, so should you be guarded when online. Treat unsolicited e-mails asking for information with extreme caution and do not click on links within e-mails. Go to the Web addresses you know to be accurate and confirm that the sites you are viewing are secure — shown by a padlock in the bottom right corner or “https” at the beginning of the Web address. Also, make sure your computer’s security software is current and that you have downloaded the most recent updates.

APPENDIX VI

Phishing Glossary

Capture Site

A fraudulent Web site that supports a phishing e-mail and is designed to mirror the legitimate Web site it is purporting to be. Criminals use multiple methods to design capture sites, including using genuine looking images and text, disguising the URL in the address bar or removing the address bar altogether. The purpose of the Web site is to trick consumers into thinking they are at the company's genuine Web site, and are giving their personal information to the trusted company with which they think they are dealing with.

Browser

Short for Web Browser, it is the software that allows users to surf the Web. Currently, the most popular Web browsers are Netscape Navigator and Microsoft Internet Explorer.

DNS (Domain Name Server)

The system that translates Internet domain names into IP numbers, is similar to a phone book for the Internet. A "DNS Server" is a server that performs this kind of translation. Because domain names are alphabetic, they are easier for humans to remember than IP addresses, which are numeric. The Internet, however, is really based on IP addresses.

Firewall

Software, hardware, or a combination of the two, that restricts access into or out of a network.

Gateway

The technical meaning is a hardware or software set-up that translates between two dissimilar protocols. For example, America Online has a gateway that translates between its internal, proprietary e-mail format and Internet e-mail format. Another, less technical meaning of gateway is to describe any mechanism for providing access to another system, for example, AOL might be called a gateway to the Internet.

Harvesting

The process of scanning the Internet to identify e-mail addresses in order to create lists for spamming.

Hyperlink

An element in an electronic document that links to another place in the same document or to an entirely different document. Typically, you click on the hyperlink to follow the link. Hyperlinks are the most essential ingredient of all hypertext systems, including the World Wide Web.

IP (Internet Protocol) Address

The address that provides a unique identification of a server and the network to which it belongs. An IP address is expressed as four numbers separated by dots (e.g., 197.92.96.105). Also see DNS.

ISP (Internet Service Provider)

A company that provides an Internet connection, for example, America Online or EarthLink.

Internet

A global network linking millions of computers for communications purposes. The Internet was developed in 1969 for the U.S. military and gradually grew to include educational and research institutions before expanding to its current popularity with individual users. The use of the Internet has mushroomed primarily due to the popularity of the World Wide Web and e-mail.

Keystroke Logger

Software that captures the user's keystrokes, usually unbeknownst to the user.

Link

In hypertext systems, such as the World Wide Web, a link is a reference to another document. Such links are sometimes called hyperlinks because they take you to other document when you click on them.

Log-in

To make a computer system or network recognize you so that you can begin a computer session. Most personal computers have no log-on procedure — you just turn the machine on and begin working. For larger systems and networks, however, you usually need to enter a username and password before the computer system will allow you to execute programs.

Malware

A generic term increasingly being used to describe any form of malicious software. Examples include viruses, Trojan Horses, malicious active content, etc.

Pharming

Software that allows a hacker to exploit a DNS server to acquire the Domain Name for a site, and to redirect traffic from that Web site to another Web site. DNS servers are the giant computers that “run” the Internet. Also known as “DNS poisoning.”

Phishing

Phishing is the name given to the practice of sending at random e-mails that purport to come from a genuine company operating on the Internet, in an attempt to trick customers of that company into disclosing information at a bogus Web site operated by criminals. These e-mails usually claim that it is necessary to “update” or “verify” your customer account information and they urge people to click on a link from the e-mail which takes them to the bogus Web site. The criminals who are on the receiving end of the phished information will then use it to commit financial fraud and/or identity theft.

Social Engineering

In this usage, conning e-mail recipients into opening messages, revealing passwords and/or providing other confidential information by appealing to their curiosity, gullibility or computing naiveté.

Spam

The Internet version of junk mail. Spamming is sending the same message to a large number of mailing lists or newsgroups, usually to advertise something.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge.

Spoofing

Spoofing is the act of impersonating another person, computer or Web site. This is usually done by providing a false e-mail name, URL or IP address. Also refers to the use of other media, including telephone and in-person, to con people into revealing confidential information.

Trojan Horse

A destructive software program that masquerades as a benign application. For example, a program that appears to be a game or image file, but in reality performs some destructive or malicious function.

URL (Uniform Resource Locator)

The standard way to give the address of any resource on the Internet that is part of the World Wide Web, (e.g., <http://www.aba.com>).

Virus

A destructive computer program that has the ability to reproduce itself and infect other programs or disks. Typically a virus will not show itself immediately, but will add itself to programs and disks to spread itself widely on many computers before it is triggered into its destructive phase. The best defense is to run anti-virus software and use it on all new software and disks introduced to your system. Anti-virus software should be updated monthly.

WWW (World Wide Web)

The collection of pages that are accessed via the Internet using a browser. Often mistakenly used to refer to the Internet as a whole.

Banker Review Committee

Larry J. Callais
President & CEO
MC Bank & Trust Co.
Morgan City, LA

Charles R. Haley
President
Peoples Bank
Eatonton, GA

Tom Mantor
President & COO
Bank of Walnut Creek
Walnut Creek, CA

John Eilering
President & CEO
Mount Prospect Natl. Bank
Mount Prospect, IL

Thomas L. Hoy
Chairman, President & CEO
Arrow Financial Group
Glens Falls, NY

Contributing Authors

Kristi Lamont Ellis
Senior Vice President
Regions Financial Corp.
Birmingham, AL

Brad Keller
Principal
Keller Advisory Group, LLC.
Atlanta, GA

Digital Insight® Corporation
Calabasas, CA

ABA Staff Contacts for Questions About Phishing

Doug Johnson
Senior Policy Analyst
Government Relations
202-663-5059
djohnson@aba.com

John Hall
Associate Director
Public Relations
Communications
202-663-5473
jhall@aba.com

Lisa Gold Schier
Associate Director
Corporation
American Banking
202-663-5059
lgoldsch@aba.com

Nessa Feddis
Senior Federal Counsel
Government Relations
202-663-5433
nfeddis@aba.com

Don Rhodes
Policy Manager
Government Relations
202-663-7513
drhodes@aba.com

ABA Staff Contributors

Jim Chessen
Chief Economist
Office of the Chief Economist

Christine Walika
Director
Community Bankers Council

Adam Wasch
Policy Analyst
Office of the Chief Economist

Susan Einfalt
Associate Director, Graphics
Communications

Michael Potter
Program Manager
Community Bankers Council

Ellen Collier
Manager
Office of the Chief Economist

Melissa Frankel
Senior Program Assistant
Communications



1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com