

December 2003

Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

Phishing: Cute Name, Serious Crime	3
The Origins Of The Word “Phishing”	3
The Anti-Phishing Working Group: An Industry Solution For Tackling Email	
Phishing and Spoofing Attacks	4
AntiPhishing.org.....	4
Technology Solutions	4
Detection: Scanning, Filtering and Alerting	5
Preventative Solution 1: Strong Website Authentication	5
Preventative Solution 2 – Mail Server Authentication	6
Preventative Solution 3 – Digitally Signed Email With Desktop Verification.....	7
Preventative Solution 4 – Digitally Signed Email With Gateway Verification....	8
Summary Of The Proposed Preventative Solutions	9
Digitally Signed Email	10
Mail Server IP Verification.....	10
Join the Anti-Phishing Working Group and Be a PhishBuster!	10

Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

Phishing: Cute Name, Serious Crime

Spam is annoying, distracting, and burdensome to networks. But the spoofing scam known as “phishing” has the potential to inflict serious losses of data and direct losses due to fraudulent currency transfers. Phishing is the creation of email messages and web pages that are replicas of existing sites to fool users into submitting personal, financial, or password data.

Organized crime operatives typically mount these attacks in order to use the data to execute high-value currency transfers – or to mount sophisticated identity theft schemes and credit-card scams. Typically, a phishing email arrives with the spoofed company’s logo and email layout, requesting the receiver to link to what appears to be a genuine Web site where the victims are instructed to enter their account number and password. If convincing, the scammers will net some customers.

“The hottest, and most troubling, new scam on the Internet.”

Federal Bureau of Investigations, July 25, 2003

Phishing attacks are blooming in frequency, scope and rates of success with upwards of 20% of targeted users providing personal information. Recently, Citigroup, Lloyds TSB and Barclays have been subjected to phishing attacks that spoofed their identities in pursuit of customer’s account, debit and credit card data. Within the last year, Wachovia, Bank of Montreal, Bank of America, St. George Bank, and the ANZ Bank of Australia, have been hit by phishing scams. Although financial services firms were obvious initial targets for phishing attacks, highly adept identity theft rings have expanded their operations to exploit a number of Internet consumer brands including Yahoo!, eBay, Paypal, Monster.com, Bestbuy.com, Microsoft MSN and even the FBI.

The deeper the store of data that is held by the enterprise, the more likely it will be targeted for phishing attacks by identity theft rings. Retailers can retain almost any depth of data, depending on the nature of their business. Financial services usually archive substantial amounts of personal data though they are not, as a class, the most data rich source of consumer data. We believe that a highly prized target for identity theft operatives will be health care agencies and health care data processors because they archive rich, deep stores of high quality consumer data including accurate dates of birth, social security numbers and true postal addresses.

The Origins Of The Word “Phishing”

The word “phishing” comes from the analogy that Internet scammers are using email lures to “fish” for passwords and financial data from the sea of Internet users. The term was coined in the 1996 timeframe by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users. The first mention on the Internet of phishing is on the alt.2600 hacker newsgroup in January 1996, however the term may have been used even earlier in the printed edition of the hacker newsletter “2600”.

"Ph" is a common hacker replacement for "f", and is a nod to the original form of hacking, known as “phreaking”. Phreaking was coined by the first hacker, John Draper (aka. "Captain Crunch"). John invented "hacking" by creating the infamous Blue Box, a device that he used to hack telephone systems in the early 1970s.

This first form of hacking was known as "Phone Phreaking". The blue box emitted tones that allowed a user to control the phone switches, thereby making long distance calls for free, or billing calls to someone else's phone number, etc. This is in fact the origin of a lot of the "ph" spelling in many hacker pseudonyms and hacker organizations.

By 1996, hacked accounts were called "phish", and by 1997 phish were actually being traded between hackers as a form of currency. People would routinely trade 10 working AOL phish for a piece of hacking software that they needed.

Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

Over the years, phishing attacks grew from simply stealing AOL dialup accounts into a more sinister criminal enterprise. Phishing attacks now target users of online banking, payment services such as PayPal, and online e-commerce sites. Phishing attacks are growing quickly in number and sophistication. In fact, since August 2003, most major banks in the USA, the UK and Australia have been hit with phishing attacks.

The Anti-Phishing Working Group: An Industry Solution For Tackling Email Phishing and Spoofing Attacks

The "Anti-Phishing Working Group" is being organized to develop an acceptable solution to email phishing scams. This is an organization comprised of financial institutions, ecommerce providers, ISPs and web email services, and software vendors. The goal is to provide resources, technology, vision and expertise to facilitate the rapid deployment of a solution to email phishing scams.

The Anti-Phishing Working Group meets periodically, but is largely coordinated via email communications. The group is an informal one, and will work with related industry groups such as the Anti-Spam Research Group, the Anti-Spam Alliance, the Information Technology Association of America (ITAA), and Project Lumos.

AntiPhishing.org

The Anti-Phishing Working Group has established the Antiphishing.org website as a repository of information about phishing. The site contains a news feed of articles about phishing, as well as an ever-expanding archive of known phishing attack emails and websites. Proposed technical solutions, lists of vendors and government agencies who can help combat phishing are also listed.

Financial institutions, e-commerce providers, ISPs, payments vendors, corporations, vendors and journalists are welcome to use the material on the site, and to contribute to this valuable resource.

Technology Solutions

We believe that a solution to phishing cannot simply rely on millions of users being trained to check the details of email routing headers and to scrutinize the minutia of Internet URL web links to ensure that email communications are genuine, and not from a phisher. In fact, with the URL masking vulnerability in the Internet Explorer Web browser that was disclosed on Dec 10, 2003, even the URL web address cannot be relied upon to be correct.

The basic building blocks of an effective anti-phishing effort include detection, prevention and education.

For a preventative technology solution to be effective, it must have the following characteristics:

- Limit end-user training as much as possible
- Prefer use of existing standards-based technologies
- Unilateral deployment must add value
- Must be cost-effective for both senders, recipients, and Internet infrastructure providers

We believe that there are three general classes of possible preventative technology solutions.

- Strongly authenticate any users visiting a business web site using two-factor authentication
 - *"Strong Website Client Authentication"*
- Use enhanced DNS capabilities to verify the IP address of a sender's email server
 - *"Mail Server Authentication"*
- Use S/MIME digital signatures to sign outbound mail - provide signature verification at the *gateway* or *email client*
 - *"Mail Authentication via Digital Signatures"*

Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

Detection: Scanning, Filtering and Alerting

One of the basic building blocks of an anti-phishing effort for companies and financial institutions is to know when phishing attacks have been launched, and to be prepared to take action to reduce the impact of such attacks. When a phishing attack is detected, companies can place warnings on their websites, notifying their customers of the potential threat. Some companies that are particularly vulnerable, such as online banking sites, may even go so far as to disable access to their service until the attack has been disabled or contained.

Companies should be continuously monitoring domain name registrars and the domain name system for domain names that infringe upon their trademarked names, and that could be used for launching spoofed websites to fool customers. For example, if your website is www.antiphishingbank.com, keep a watchful eye out for newly registered domains such as www.security-antiphishingbank.com, www.antiphishingbank1.com, www.antiphishingbank.com, etc. Also be mindful of domains that might be common misspellings of your domain names, such as www.antiphishinggbank.com or www.antiphishingbnak.com.

There are now commercial services available that monitor the domain name service for these types of threats, and will pro-actively notify you of potentially threatening new domain names. Services also exist that will track known hacker chat rooms for phishing and spoofing planning discussions, and alert you of these.

Anti-spam vendors can also be used as an early warning system of phishing attacks. Some anti-spam vendors offer services whereby they scan emails and spams, and will report to you if a potential phishing attack is spotted.

Companies and financial institutions should consider notifying vendors of anti-spam filter update services and anti-spam outsourcing services whenever a new phishing attack has been identified. The anti-spam vendors can then add this into their filters, and potentially block it from being delivered to their customer bases.

These approaches are good basic building blocks of an anti-phishing strategy. These are reactive approaches that can potentially reduce the impact of a phishing attack, and give a company warning of such an attack in progress. The Anti-Phishing Working Group is also investigating preventative technology approaches that could largely eliminate the potential for phishing attacks in the first place.

Preventative Solution 1: Strong Website Authentication

This approach would require all users of legitimate e-commerce and e-banking sites to strongly authenticate themselves to the site using a physical token such as a smart card.



The positive aspects of this approach are:

- Even if a user falls for a phishing attack, a phisher can't log into real site without the right physical token
- Users are given a stronger sense of trust in their transactions with business web site

Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

The downsides of this approach are:

- User education
- Set up time delays
- Desktop software installation
- High management costs
- Potentially high cost per user

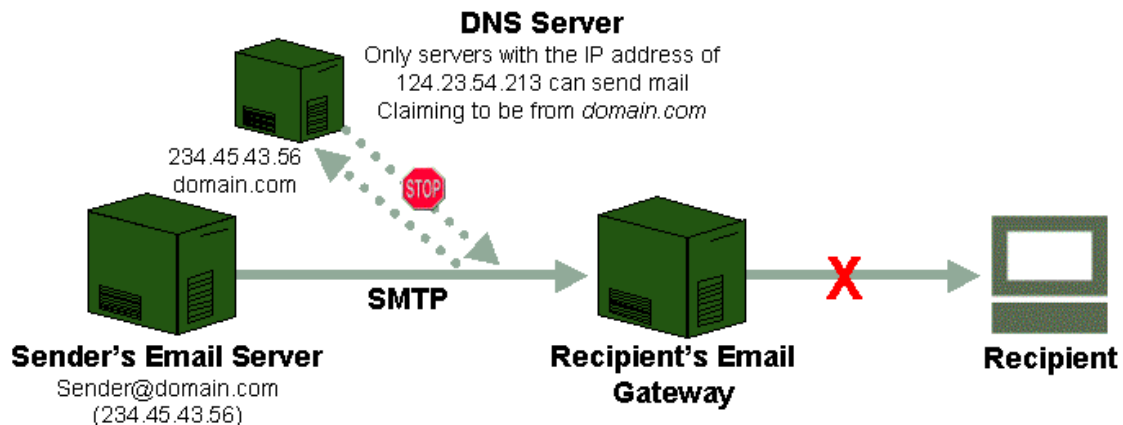
Stakeholder's effort:

- Enterprises must issue tokens (software or hardware) to their customers
- Customers must install the necessary software on their desktops
- 3rd party trust authorities may have to be involved if 3rd party certificates were to be issued on behalf of the business

We believe that this approach is feasible for e-commerce and e-banking applications that do not have a large number of users, and where the risk of a phisher gaining access to a user's account are high. Examples would include corporate banking websites and high-value brokerage trading websites.

Preventative Solution 2 – Mail Server Authentication

The Anti-Spam Research Group (ASRG) and the Anti-Spam Alliance have been investigating solutions to the growing spam problem based on authenticating sending mail servers. There are numerous technical proposals such as RMX for how this will work.



The positives of this approach are:

- Easy to configure at senders mail servers
- Makes it harder for phishers to be anonymous
- Legitimate business email can be better identified – lower spam false positives

The downsides of this approach are:

- Requires sender and recipient gateways to both use these methods
- SMTP sender is not visible to recipient
 - From: address still can be spoofed and users can be fooled
- Will be a problem for anyone using a 3rd party emailing service
- Doesn't accommodate email forwarding

Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

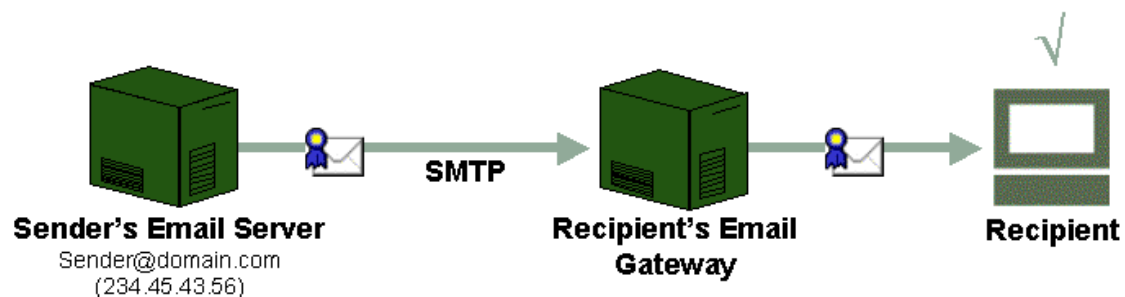
Stakeholder's effort :

- Vendors
 - Enhance email relays to look up mail server IP addresses and compare with envelope sender domain name
 - Optional: Enhance email clients to display envelope sender
- Sending enterprises
 - Must register their mail server IP addresses in DNS
- Recipient mail gateways
 - Enterprises looking to block spoofed email from Yahoo, AOL, MSN, etc.
 - Roll out enhanced email relays

We believe that mail server authentication is a necessary but not sufficient approach in the battle against spam and email scams. This approach is appealing to the large web email providers and ISPs, as it can allow them to cut down on a great volume of spam. However, for it to be effective, stopping phishing attacks will require all ISPs, web email providers and corporations to not only publish their mail server authentication information, but to install mail server authentication software as part of their email filters, with appropriate end-user quarantines when the inevitable false-positives occur. Until all of the hundreds of thousands of corporations in the world have this technology, their employees will be vulnerable to phishing attacks.

Preventative Solution 3 – Digitally Signed Email With Desktop Verification

This approach is based on the use of the existing industry standard S/MIME, which is a secure email standard supported by most email client software that is in use in corporations today. Companies who are vulnerable to phishing attacks, such as financial institutions, payment processors and e-commerce vendors, would send their emails with a digital signature attached. Note that the digital signature would be attached at the outbound gateway, rather than requiring the individual sender to apply the digital signature. This automation at the gateway would further increase the adoption rate of such a solution. When users receive these digitally signed emails, their business email clients (e.g. Microsoft Outlook, Lotus Notes, Novell Groupwise, etc) will automatically verify the signature for authenticity. If an email arrives to a user that is either not signed, or the signature can not be verified, the user would know that it is not a genuine email from the sending bank or e-commerce provider.



The positives of this approach are:

- S/MIME is a standard in business email clients – would work without any additional software deployment to email users
- Makes the "From:" address impossible to spoof without detection
- Any phisher who digitally signs their email must register with a certificate authority – provides a stronger identity audit trail when prosecuting the phisher
- Legitimate business email can be better identified by end-users – provides better trust with customers

Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

The downsides of this approach are:

- Recipients still have to inspect the "From:" address for misleading domains (e.g. a phishing email could have a valid digital signature with the email address of account.update@ebay.custservices.com. The end user would have to know that ebay.custservices.com is not in fact Ebay because ebay.com is not in the domain portion of the address.)
- Not all email clients support S/MIME (e.g. Hotmail, AOL, Yahoo! Mail, Outlook Web Access for Exchange 5.5)
- Recipients may not check certificate revocation status

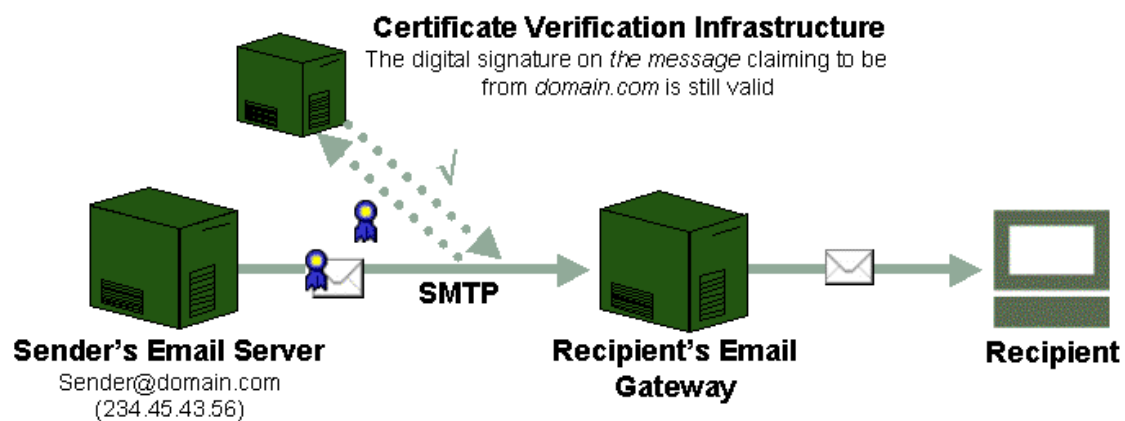
Stakeholder's effort:

- Sending enterprises must sign on behalf of their users. Doing this at the gateway is better than training end-users to sign at their desktops
- Recipients' business email clients that understand S/MIME
 - **YES:** MS Outlook, Lotus Notes, Novell Groupwise, Netscape Communicator, Eudora
 - **No, but message is still readable by users:** Yahoo, AOL, MSN Hotmail, Earthlink
 - **No, and message unreadable without special plug-ins:** Outlook Web Access for Exchange 5.5
- 3rd party trust authorities must provide certificate issuance and revocation services

We believe that this approach provides clear and useable value by strongly authenticating senders in a way that will work with the majority of email client software in use today. However, this does not solve the problem of people who receive their email through a web email provider such as Yahoo! or Hotmail as those systems do not support signed email today. They would have to take a gateway approach to validate email signatures or use the authenticated mail server approach.

Preventative Solution 4 – Digitally Signed Email With Gateway Verification

Similarly to Solution 3 proposed above, this approach uses the S/MIME standard for email that is widely available today. Instead of relying on the end user's email client to verify the signature on the email, a gateway server at the mail relay level would verify the signatures before they were even received by the receiver's email server. This approach would work well for ISPs and web email providers who wish to support signed email as a way to defeat phishing attacks.



Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

The positives of this approach are:

- S/MIME is a standard today that is supported by many email gateways
- Makes the “From:” address impossible to spoof without detection
- Any phisher who digitally signs their email must register with a certificate authority – provides a stronger identity audit trail when prosecuting the phisher
- Legitimate business email can be better identified by end-users – provides better trust with customers

The downsides of this approach are:

- Sender and recipient gateways must both understand S/MIME digital signatures
- Doesn’t prevent valid signatures from having misleading From: addresses (e.g. a phishing email could have a valid digital signature with the email address of account.update@ebay.custservices.com. The recipient gateway would likely pass the email on and the end user would have to know that ebay.custservices.com is not in fact Ebay because ebay.com is not in the domain portion of the address.)

Stakeholder’s effort :

- Sending enterprises must sign on behalf of their users
- Recipients’ mail gateways must validate digital signatures
 - Yahoo
 - AOL
 - MSN
 - Enterprises looking to block spoofed email
- 3rd party trust authorities must provide certificate issuance and revocation services

This approach may be a viable way for the web email providers to support signed email verification without having to extensively modify the way that they handle email, or their existing user interfaces.

Summary Of The Proposed Preventative Solutions

Solution Requirements	Two-Factor Authentications	IP Filtering	Digital Signature (Desktop)	Digital Signature (Gateway)
1. Limited End-User Training	X	✓	X	✓
2. Standards-Based	X	X	✓	✓
3. Unilaterally Deployable	X	X	✓	X
4. Cost Effective for Sender	X	✓	✓	✓
5. Cost Effective for Recipient	✓	✓	✓	✓

The above matrix shows that a combination of signed email with desktop verification, and either gateway verification or mail server IP verification would solve all aspects of the phishing problem for both consumer and business users.

Proposed Solutions to Address the Threat of Email Spoofing Scams

The Anti-Phishing Working Group

Digitally Signed Email

Digital signature verification and signing capabilities are built into most email client software on the PC desktop today, including Microsoft Outlook and Lotus Notes. Still, most people do not have a certificate to sign with. The key lies not in the cumbersome, manual desktop certificate issuance mechanisms offered by many certificate authorities today. Rather, it is in email signing certificates managed at the email gateway that only confirm a sender's email address. The certificate authorities and email gateway vendors will need to find ways to make digital signatures on email transparent and interoperable.

It's important to note that historically potent leaders in security and authentication technologies have begun to adopt signed email as a matter of policy. The Department of Defense, for example, is rolling out its signed email program that would require all DoD communications to be digitally signed. As has been the case with two-factor authentication technologies and even drug testing, the DoD has been the pioneering institution from which many important security technologies and techniques have proliferated into general circulation.

Enterprises can easily implement this scheme by signing all outgoing emails to their customers with an email proxy server – without having to implement a costly PKI digital certificate infrastructure. End users can simply and inexpensively validate that the emails are from the online companies with whom they actually transact business, without the need for costly proprietary software. There are a number of ancillary benefits to using this kind of scheme. First, email filters that might normally falsely label legitimate electronic business correspondence as spam, would be able to check the signatures on the email, and avoid erroneously classifying these emails as spam, or so-called “False Positives”. What's more, the signature-checking regime would, itself, establish cryptographically based trust relationships between banks and their customers, an infrastructure that could enable a number of secure services in the future.

Mail Server IP Verification

RMX and other proposed new standards for authenticating mail servers are being seriously considered by the large web email providers as weapons in the war against spam. By combining this approach for the web email vendors, with a digitally signed email approach when sending to corporate users, a complete anti-phishing solution may be at hand.

Join the Anti-Phishing Working Group and Be a PhishBuster!

In the coming months, the Anti-Phishing Working Group will be working with technology partners, government regulators, and leaders in industries being victimized by phishing attacks to sculpt the most efficient and elegant digital signing and authentication solution that can be employed by large user communities. We are sending calls to action to all stakeholders in the hopes that by year end, a consensus will be formed among them as to how the effected industries can establish a digital signing and authentication regime that can be deployed post haste to end phishing attacks, preclude regulatory adventurism and, ultimately, to establish a technological foundation for a broader spam-proof electronic mailing infrastructure.

To participate or learn more, please contact info@antiphishing.org or visit our website, www.antiphishing.org.