THE CLIPPER GROUP
Navigator™

Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2006050 June 22, 2006

Iconix's *Truemark* — Bad News for Phishers

Analyst: Dianne McAdam

Management Summary

Every day new items, some new, some used and some broken are listed on *eBay*. In fact, the first item sold on eBay was a used, broken laser printer for $13.83. Today, millions of items ranging from automobiles to computers, collectibles to appliances are sold daily. eBay has been very popular and profitable, and is the preferred web site for many consumers looking for the next *great deal*. The success and popularity has of eBay has made it the target for numerous phishing attacks.

Phishing is just like fishing, but uses emails rather than fishing poles to lure its target. Fishermen throw out bait to a school of fish knowing that many will ignore the bait but a few hapless fish will snag the bait and be someone's dinner. Phishers send out numerous emails posing to be an established business, such as eBay, *PayPal*, banks, credit card companies, or retail stores to convince a few hapless customers to hand over their credit card numbers and other confidential information so that the phishers can enjoy a great dinner (and a new wardrobe and vacation) on someone else's credit card.

Some people ignore these fictitious emails; others are not so lucky and spend months trying to resolve the problems and expense of identity theft. Phishing is annoying and can be expensive for consumers, but it is also annoying and expensive for enterprises. Banks have reported call centers flooded with phone calls asking if the email just received is legitimate. So how do you eliminate those annoying phishing emails? Iconix, Inc., of Mountain View, CA, has the answer for enterprises and their customers.

Iconix was founded in December 2004 with one clearly defined mission – to review all incoming emails and determine which emails are legitimate. They knew that banks, credit card companies and others were concerned about the cost to support customers calling in to verify email messages. These enterprises are just as concerned about the reputation of their brand and the damage to the brand that could occur, if consumers received too many phishing messages. Enterprises want to establish open lines of communication with their customers - and phishing causes mistrust of email - thereby closing the lines of communication. Ironically, some consumers blame legitimate businesses when they receive illegitimate emails. These consumers forget that the enterprises are the *target* and not the *source* of those annoying emails. Iconix initially believed that consumers were also very concerned about phishing. In fact, Iconix believed that phishing was one of consumer's top concerns. After conducting numerous focus groups, Iconix discovered that consumers felt phishing was not their major problem; managing emails were the main concern. Consumers wanted to easily find emails and not spend a lot of time managing inboxes, including examining and deleting emails that were suspicious. Here's what they want.

- An easy way to find messages that are important to them and know they were legitimate;
- To be informed which emails are not legitimate; and
- They don't want to pay for the software.

Read on, to see how this is possible.

IN THIS ISSUE

➢ **The Iconix Solution..... 2**
➢ **How Does Iconix Make Money? 3**
➢ **Conclusion 3**

The Iconix Solution

The Iconix solution is a two-step process to ensure the integrity of the sender and the originating corporation for every email. A corporation subscribes to Iconix's services and provides Iconix with its valid domains, addresses, and corporate logo. Consumers download a plug-in module that works with common email services. This plug-in is available *for free* from the Iconix website or the website of the subscribing corporation. All messages to the consumer are checked as they enter the inbox. During the first step, the authenticity of the email is verified using *DomainKeys* and *Sender ID* The second step compares the sender ID against a list of legitimate sender IDs supplied by the enterprise. If the email passes the scrutiny of both steps, then Iconix marks the email with a *Truemark* icon, which displays the logo of the sending corporation. Now, consumers can scan through these messages and know that emails that have an attached Truemark icon can be trusted. (See image at top of next column.)

Let's Go Phishing

Most email today is transmitted using the Simple Mail Transfer Protocol (SMTP). SMTP was designed in the days when the only people that used email were "techies". Techies always believed that they could trust other techie. Therefore, there was never any sender verification built into SMTP.

Phishers, unlike the original techie, cannot be trusted. Phishers have been known to copy a legitimate email from a bank and change the content of the email to direct the consumer to a fraudulent web site that looks identical to the bank's real web site. Customers log in and verify (share) their financial information to the fraudulent web site and the phisher has 'reeled' in his next victim.

Could we simply use the IP address of the sender to verify the authenticity of the sender? Most IP addresses that are assigned by Internet Service Providers (ISPs) are dynamic. A known phisher's IP address can be added to a blacklist of IP addresses. Unfortunately, by the time that blacklist is distributed, the phisher has resurfaced with a different IP address. Stopping phishing attacks by IP address is burdensome and not very reliable; there are about 4 billion IP addresses today. Attempting to control phishers by blacklisting IP addresses is like playing the game *whack-a-mole*. As soon as you hit one mole, another pops up to taunt you.

There are several ways detect a phisher's email. Iconix uses two such approaches – *Sender ID* and *DomainKeys*. Sender ID checks the server sending the mail against a registered list of domain servers that the corporation has authorized to send emails. DomainKeys generates a public/private key for every outgoing message. The email server uses the private key to generate a signature that is attached to the message. The receiving email system retrieves the public key, analyzes the private key and signature and determines if the email was sent by the domain server specified in the "from" address.

The Truemark Icon

Iconix uses both methods for authentication since some email services, such as *Yahoo! Mail*, use DomainKeys, while MSN's *Hotmail*, for example, uses Sender IDs. Using both methods provides better protection. This is the first step of Iconix's verification process. The second step of the process compares the senders email address with the list of valid email addresses supplied by the corporation. If the message passes both tests, then the Truemark icon is appended to the message signaling the consumer that it is safe to open the message.

Currently, Iconix supports Yahoo! Mail, MSN's Hotmail, Google's *Gmail*, Earthlink's *Webmail*, and Microsoft's *Outlook Express*. By the end of the second quarter, Iconix will also support Mozilla's *Firefox* and Microsoft's *Internet Explorer 7.0*. Support for *Outlook* and *AOL* mail will follow in the third quarter. By the end of the year, Mozilla's *Thunderbird*, Microsoft's *Windows Live Mail*, and IBM's *Lotus Notes* will be supported.

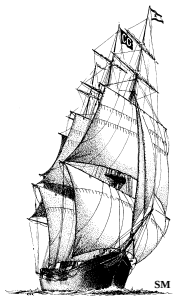
How Does Iconix Make Money?

Consumers use Google every day to search the Internet. The service is free for consumers. Enterprises pay Google every time a consumer clicks on an ad. That model has been very successful for Google and Iconix has a similar model. Consumers do not pay for the plug-in module. Similarly, enterprises pay Iconix each time a Truemark icon is displayed next to a message and each time a consumer opens a message marked by that icon.

Iconix already has about 300 corporations signed up including familiar names like eBay, Travelocity, and Home Depot and other major banks, airlines, and retail stores. Studies have shown that users open messages marked with the Truemark icon 2.7 times more often than messages that have no mark.

Conclusion

Iconix provides a much-needed service. Consumers no longer have to spend time examining messages to determine which are real and which are fake. Enterprises can use emails to communicate with their consumers knowing that consumers that have installed the Iconix software will trust the email without having to call the call center. When Iconix has support for my email service, I will be looking for those Truemark icons in my inbox.



About The Clipper Group, Inc.

The Clipper Group, Inc. is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Dianne McAdam **is Director of Enterprise Information Assurance for the Clipper Group**. She brings over three decades of experience as a data center director, educator, technical programmer, systems engineer, and manager for industry-leading vendors. Dianne has held the position of senior analyst at Data Mobility Group and at Illuminata. Before that, she was a technical presentation specialist at EMC's Executive Briefing Center. At Hitachi Data Systems, she served as performance and capacity planning systems engineer and as a systems engineering manager. She also worked at StorageTek as a virtual tape and disk specialist; at Sun Microsystems, as an enterprise storage specialist; and at several large corporations as technical services directors. Dianne earned a Bachelor's and Master's degree in mathematics from Hofstra University in New York.

- ***Reach Dianne McAdam via e-mail at dianne.mcadam@clipper.com or at 781-235-0085 Ext. 212. (Please dial "212" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, "*Navigating Information Technology Horizons*", and "*teraproductivity*" are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.