



KPMG ANALYSIS

E-Mail Authentication Becomes the Weapon of Choice in Fighting Phishing

February 27, 2008

As the fight continues against e-mail phishing, which aims to harvest personal information through fraudulent e-mails, sender authentication is becoming a leading approach to fighting phishing and its cousin, spoofing. E-mail authentication frameworks such as Sender ID and DomainKeys Identified Mail assure recipients that a message has actually come from a legitimate company.

According to a report by the Authentication and Online Trust Alliance (AOTA), more than half of U.S. Fortune 500 financial services firms, retailers and consumer brands have adopted at least one form of e-mail authentication technology.

KPMG Digital Insider spoke with Sam Masiello, director of threat research at managed e-mail provider MX Logic and a member of the AOTA committee that wrote the report, about the role authentication is playing in the war against phishing and e-mail-based fraud.

Digital Insider: Can you describe AOTA?

Sam Masiello: We're an industry group [that] is interested in increasing trust on the Internet, and establishing and maintaining online trust for brand recognition. That includes not only things like authentication in e-mails, but online trust -- making sure that the e-mail you're receiving is from who you think it's from, and that Web sites you go to are the Web sites you think you're going to.

DI: What were some of the report's major findings?

Masiello: The report was prepared to highlight the fact that the brands that have been phished and spoofed the most often are authenticating their e-mail messages [more] and making a concerted effort toward establishing their credibility [with] users.

So many people have gotten to the point where they don't even read e-mail messages from companies anymore, because a lot of what they get in their inbox is spoofed.

But with 51 percent of the Fortune 500 consumer-facing brands currently authenticating their e-mail, companies that should be jumping onto the authentication bandwagon are doing so. There's still a way to go, but it shows we've made significant progress.

DI: Does e-mail authentication come primarily from companies that have been victimized?

MORE...

[IFRS for Technology Companies: Closing the GAAP?](#)

AUGUST 14 A KPMG white paper examines industry-specific issues for technology companies considering a transition to International Financial Reporting Standards.

[The Consumer Electronics Boom](#)

AUGUST 6 A new KPMG white paper identifies the critical issues inhibiting faster time-to-market for consumer electronics and semiconductor manufacturers.

[Wireless Carriers Put Money in Mobile Banking](#)

JULY 29 Cell phone carriers are targeting mobile banking applications for growth.

[Selected Technology Company Earnings](#)

JULY 25 Slowing economic conditions in the United States affected the results of several technology companies in the second quarter.

[Companies Taking Green-Tinted Look at Data Centers](#)

JULY 18 As corporations become more environmentally aware, they're looking at their data centers and PCs to reduce energy consumption and carbon footprints.

[Social Media: a New Political Animal](#)

JULY 10 Social media is reaching beyond the traditional corps of political pros and playing a major role in the fall elections.

[KPMG's Quarterly New and Emerging Markets Magazine](#)

JULY 2 In this issue, KPMG examines how the wireless revolution is shaping everyday life in emerging markets to its logistic systems.

Masiello: Yes. Many of the top retail brands and financial institutions are getting spoofed on a regular basis. They realize that this is a problem, and they're attempting to fight it.

DI: How does authentication technology help to reestablish brand identity?

Masiello: There are two approaches to authentication technologies. Let's start with the Sender ID framework [which allows companies to register their mail servers as part of their domain identification records]. That allows a brand to say, "I own a specific domain and send e-mail out on these particular IP addresses. If you see an e-mail that's from that IP address as part of my Sender ID Framework record, you can assume that the e-mail is from the domain it says it came from."

The other approach is known as Domain Key Identification, which uses signed content within the message and creates a signature within the message header.

DI: Do warnings against opening any e-mails from banks or retailers to avoid phishing attacks hurt legitimate brands?

Masiello: We need to move toward a model where companies feel they can communicate reliably with customers. I can certainly understand why that recommendation would've come down -- if consumers don't click on the links in the e-mails and don't go to the phishing Web sites, they're taking large strides toward making sure their credit cards and identities don't get stolen.

But at the same time, I don't think that's necessarily the best message to send either, to say just avoid all e-mail contact. Part of what AOTA is trying to do is help reestablish that credibility in messages so somebody can be reasonably certain that [an e-mail] is actually is from who it says it's from.

DI: Will consumers notice e-mail authentication?

Masiello: It's largely going to work in the background. A lot of Web mail providers will consider the presence of e-mail authentication along with the [general] reputation of the sender. The existence of [authentication] doesn't necessarily mean you're a good guy -- it just means that the e-mail is coming from where it says it's from.

So companies are using those technologies in combination with reputation [scores] so that [they] can say, "Okay, I know this e-mail is from [a domain], but I also know, based on reputation, that most of the mail that we get from [that domain] is spam."

A lot of that is going to happen in the background, where the mail-filtering or the mail-hosting provider will take a combination of results to determine how it wants to handle a message -- is it something they want to deliver to an in box, or is it something they want to throw into the trash folder?

DI: Do ISPs play a role in authentication?

Masiello: Absolutely. [For example], about 80 percent of the e-mail that we see in our threat center that purports to be from companies like Yahoo is spoofed. So authentication is a big part of the e-mail landscape for ISPs because it's not just

[banks] that are getting spoofed. Authentication will also help cut down on the spoof mail we get from [Web mail providers] as well.

DI: What are the obstacles to widespread use of authentication?

Masiello: There are a couple that AOTA can handle, but there are a few that the individual companies have to handle themselves. For example, AOTA needs to continue to educate companies to help them understand how the industry is moving toward requiring e-mail authentication, and validating the credibility of the mail that people are getting from [their] domains.

But the other side of that coin is that [for many organizations], those networks aren't always centrally managed to the point where people have a complete handle on their full IP range.

One of the challenges is how to collect all of the information they need internally to make sure that once they've published that record, it's not going to leave [a business unit] having mail delivery issues because their IP addresses weren't included.

To print this article or share it with a colleague, click an option below.

[Print this Article](#)

[E-Mail this Article](#)

PLEASE RATE THIS ANALYSIS

Quality of Analysis

1 2 3 4 5
POOR EXCELLENT

Comments or Questions

e-Mail Address (optional to enable Insiders to reply)

[Submit](#)