Phishing: Facing the Challenge of Email Identity Theft with Proper Tools and Practices

A Leadfusion White Paper
The Threat of Phishing

Email is an indispensable tool that has changed the way we communicate. As useful as email is, it is not immune to some of the problems seen in traditional mail such as large volumes of “junk” mail as well as fraud.

In fact, one of the primary virtues of email – the ease and low cost of communicating with many people at once – serves to make these problems more acute for email recipients. In recent years, incidents of email fraud have created significant problems for consumers and businesses. One particular scheme – phishing – has emerged as a particularly damaging means of online identity theft.

Phishing is a costly problem for both consumers and companies. In 2006, Gartner Research attributed an estimated $2.8 billion in losses to phishing scams.¹ The problem is particularly acute for the financial services industry, as 92% of all phishing scams target banks or other financial sites where consumers manage financial accounts.² Once only a problem for the largest of U.S. banks, phishing attacks now target regional banks and credit unions more often than national banks.³

Not only does phishing create costly account problems, it also erodes consumer confidence in transacting online in general and in the targeted brand specifically. Most consumers feel that financial institutions should be doing more to combat phishing fraud.⁴

Don’t Let Concerns Prevent You from Reaching Your Customers

In the face of such concerns, some financial institutions have decided not to use email as either a marketing or communication tool with their consumers. There are significant problems with this approach, the first being that any organization can be targeted for a phishing attack whether or not they use email for consumer communications. To compound the problem, companies that avoid email communications also miss the opportunity to educate their consumers and set expectations about which communications are legitimate. In fact, institutions that take a strong, visible lead in the fight against fraud such as phishing have the potential to differentiate themselves in the marketplace.

There are many reasons to take advantage of email technology. Email remains one of the best approaches for consumer outreach. A recent study by the Direct Marketing Association determined that email is the most cost-effective means of direct marketing.⁵ Used properly, it can be a valuable tool for customer acquisition, account activation, cross-selling and up-selling, retention and customer service.

There is room for optimism in the fight against phishing, as there are indications that both industry and consumers are benefiting from increased awareness of the phishing problem. The very prevalence of phishing and the exposure it has received have served to create more awareness among email users, many of whom now know to distrust such emails and recognize common phishing tactics.

Frequently targeted companies, internet service providers (ISPs) and technology companies have banded together to form industry groups, the largest of which is the Anti-Phishing Working Group (http://www.antiphishing.org/). Groups such as these raise awareness of the issue and share information about offenders and how to best combat them.

ISPs and software companies are beginning to offer technology solutions designed to help manage the problem. Emerging authentication standards, when widely implemented by both email senders and email services, will help ensure that emails are from the company that they claim to be. Recent versions of widely used software such as Microsoft Internet Explorer and Microsoft Outlook help detect common phishing tactics and can access a shared list of phishing sites to alert email recipients to potential problems. Most providers of email service also pre-filter incoming email for potentially fraudulent emails.

¹ Gartner Says Number of Phishing E-Mails Sent to U.S. Adults Nearly Doubles in Just Two Years (Press Release), Gartner Research, November 9, 2006
² Phishing Activity Trends, Anti-Phishing Working Group, November 2006
⁴ U.S. Consumer Loss of Phishing Fraud to Reach $300 Million (Press Release), TRUSTe, September 29, 2004
⁵ The Power of Direct Marketing, Direct Marketing Association, November 2006

What is Phishing?

Phishing occurs when a third party sends a fraudulent email to a consumer, claiming the email to be an official communication from a company where the recipient has an account, such as a financial institution. The email is designed to invite the consumer to a web site, which is mocked up to look like the site of the financial institution or other company. The site prompts the consumer to divulge sensitive information, such as account numbers and passwords, on the premise that this information is required to deal with a supposedly urgent account problem. When a deceived consumer provides this data to the falsified web site, phishers can then exploit the consumer’s account, try the same passwords elsewhere or even attempt to create new credit accounts.
What You Can Do Today

As we’ve seen with junk email, technological solutions certainly help, but they alone will not completely solve the problem.

If you are currently using email for consumer communications, there are a number steps you can take immediately to help educate consumers and safeguard your brand.

Email Content

First and foremost, set expectations and follow them. Tell consumers what they will receive from you and, if possible, how often. Perhaps more importantly, tell them what they will not receive from you such as emails requesting personal or account information. Make these messages a regular part of your customer communications.

Never ask recipients to access their accounts through a link in an email. If you need to request customer action through email, direct recipients to log in on your homepage through a non-clickable address or ask them to call the customer service number on their statements.

Avoid teaching consumers how to detect phishing emails based on content, as the tactics employed by phishers evolve over time and such training can create a false sense of security.6

Never use links in an email that point to an IP address (example: http://103.74.0.65) or a third-party domain name that is unfamiliar to the consumer. It is critical that consumers learn not to trust such links.

Avoid alarmist language commonly found in phishing emails such as “act now or your account will be disabled”.

Use the brand that consumers recognize in the From: address, sender name and in any links within the email. Be consistent with these addresses and names so consumers learn to recognize them.

Personalize emails with consumer names or other information such as partial account numbers to demonstrate that you have a trusted relationship with the recipient.

Review communications for HTML or spelling errors, as phishers typically make basic mistakes in their messages.

Use consistency in branding and language.

Anti-Phishing Services

Since 2003, a number of companies have brought packaged anti-phishing services to the market. These services typically include the following:

Phishing prevention. These services monitor the Internet for the creation of new sites that mimic your domain name or use your digital assets such as images. Once a suspicious site is identified, they evaluate it and decide whether further action is required.

Phishing detection. Since consumer emails are typically obtained by pulling the addresses from web sites and registration sources, anti-phishing services can create email accounts and strategically distribute them so they’re likely to be picked up by phishers. By constantly monitoring those addresses for suspicious activity, they are able to detect phishing activity early. Consumer-initiated fraud alerts can also be routed through these services.

Shutdown service. Anti-phishing services maintain a 24x7 operations center prepared to respond to phishing attacks. The most important of their tasks is to contact hosting companies and Internet Service Providers to initiate the removal of a phishing site as quickly as possible. This often involves establishing relationships with hosting providers in multiple countries and serving legal papers in multiple languages. Some services will even, with their client’s guidance, attempt to disable the site and corrupt or dilute the captured consumer data.

Forensics and Reporting. The best of these offerings include analysis of the phishing site to see if compromised customer data can be retrieved or whether the phisher’s identity can be established. They will also monitor the site for reemergence after takedown and keep a log of activity to keep the financial institution and law enforcement informed.

Some of the more mature offerings in the market include:

- MarkMonitor (www.markmonitor.com)
- Internet Identity (www.internetidentity.com)
- RSA FraudAction (www.rsa.com)

---

6 An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks, Stanford University and Microsoft Research, 2006
Phishing: Facing the Challenge of Email Identity Theft with Proper Tools and Practices

- On web site pages, do not disable browser navigation tools that would allow consumers to see where they are within your site. Consumers that are able to see where they are at all times are more likely to notice when they’ve been redirected to another web site.

**Technical Infrastructure**

- Adopt email authentication standards such as SPF, DomainKeys and Sender ID to confirm that you are the legitimate sender of email from your domain.

- Establish email accounts for abuse@yourdomain.com, fraud@yourdomain.com and phish@yourdomain.com. Publish and monitor these addresses and, if possible, thank those that report suspicious emails.

**Business Processes**

- Consider contracting with an anti-phishing service such as MarkMonitor, Internet Identity or RSA who offer services designed to detect phishing attacks and disable fraudulent web sites (see sidebar).

- Alternatively, establish a cross-department, 24 x 7 response team capable of monitoring phishing incidents and responding to them aggressively and quickly.

- Establish processes for responding to abuse reports by consumers, whether they believe they have divulged account information or simply received a phishing email.

- Report incidents of email fraud to the Internet Crime Complaint Center of the FBI (http://www.ic3.gov/) and the Anti-Phishing Work Group (http://www.antiphishing.org/). When doing so, send the suspicious email as an attachment rather than forwarding it to prevent the loss of critical tracking data.

- Establish a working relationship with law enforcement agencies, providing them with information they need to pursue offenders.

**Selecting an Email Solution**

When selecting an Email Service Provider, companies should consider what features and services each vendor offers to help combat phishing. These include:

- The ability to generate event-triggered emails, allowing you to follow up with consumers when they most expect communications from you.

- Personalization features that allow you to demonstrate that you have an established relationship by placing consumer information inside of emails.

- Email evaluation services that check emails for content that might cause automated filters or email recipients to confuse a legitimate email with a phishing attack.

- The ability to use your domain in the From: email address and any links included in the email so recipients see your trusted brand.

- Knowledge and capability to deploy email authentication technologies.

**Conclusion**

Phishing is a serious concern but should not prevent institutions from doing important business online. By being informed about phishing, taking time to educate consumers and putting appropriate policies in place, a conscientious company can mitigate many of the risks associated with phishing. Safeguarding consumers not only allows a company to avoid costly problems associated with fraud – it gives that company a chance to stand out in a crowded marketplace as an organization that actively protects its customers and their confidential data.
Recommended Reading

- *How to Foil a Phish*, CSO Magazine, October 2005
  Web link: http://www.csoonline.com/read/100105/phish.html

  This article highlights the experiences of an anonymous mid-sized U.S. bank, documenting its transformation from an organization caught unaware by phishing to an organization that confidently manages and contains phishing attacks.


  This recent white paper outlines some recent trends in phishing and explains new tactics employed by phishers.

- *Anti-Phishing: Best Practices for Institutions and Consumers*, McAfee Research, September 2004

  This whitepaper contains several helpful flow diagrams depicting the anatomy of a phishing attack and tiers of security at which an attack might be prevented. It also contains a list of recommendations for combating phishing.

- *Anti-Phishing Working Group Trends Reports*
  Web link: http://antiphishing.net/phishReportsArchive.html

  Each month, the Anti-Phishing Working Group releases statistics and analysis of phishing trends. This report is very helpful for organizations combating phishing, particularly in identifying new approaches employed by phishers.