Phishing: When E-mail is the Enemy

Phishing, once only a consumer worry, is creating headaches for e-mail administrators as businesses become the next target.

CONTENTS

Understanding the Enemy	2
Three Things You Need to Know About Phishing	3
Four Steps to an Effective Anti-phishing Solution	4
Conclusion	5

SONICWALL®

Abstract

Email phishing not only leads the loss of financial, personal and even identity information it can also lead to a loss in confidence in the use of email as a communication medium. Phishing is viewed as a consumer problem, but just as well can affect business either directly through the loss of information or indirectly through the loss of productivity of a "phished" employee. Often organizations ignore or minimize phishing assuming for their spam filter alone can detect phishing or that employees can easily tell–neither is true. This paper looks at challenges an organization faces in staying ahead of phishing and outlines a framework to incorporate anti-phishing actions into existing processes.

Understanding the Enemy

Of the many types of unwanted e-mail that threaten your business today, spam gets most of the attention, and rightly so. More than 90 percent of e-mail received by organizations is commercial spam. But e-mail threats come in many forms and new types can appear at anytime, limited only by the imaginations of their perpetrators. In fact, some of the most malicious e-mail threats aren't just carried in an e-mail message–they are the e-mail message in the form of phishing e-mails.

E-mail phishing is generally considered to be a problem for consumers, but flushed with success defrauding consumers, phishers now are turning their sights on businesses–discovering that techniques that work well with consumers work equally well with unsuspecting employees. Phishing emails aimed at employees often appear to come from trusted sources such as company management, corporate services or even partners; use legitimate company graphics, layout, content and links; and ask employees to take actions that seem reasonable in a business context, such as verifying company information.

Financial services, insurance and healthcare companies–all keepers of sensitive information–are especially prime targets for e-mail fraud attacks and the stakes are high because regulators hold them to stringent privacy and security standards. But the truth is every company is vulnerable to e-mail fraud attacks and every attack has the potential to create devastating losses.

In addition to time and money, one of the most significant losses stemming from e-mail phishing is trust. Even a single successful e-mail phishing attack can render the e-mail sent by your organization untrustworthy, transforming one of your most valuable business applications into one of your most serious business threats.

E-mail phishing attacks are an especially thorny problem for growing businesses. The impact of an attack can be just as devastating to you as it is to large enterprises, yet you may lack the financial or technical resources to fight back effectively.

In this whitepaper, SonicWALL® levels the playing field for growing businesses concerned about the escalating problem of phishing. In addition to three things you need to know about e-mail phishing–including three common myths–SonicWALL outlines four steps growing organizations can take to an effective anti-phishing solution.

Three Things You Need to Know About Phishing

To effectively combat phishing, there are three things you need to understand: The phisher, the phish and the facts.

The Phisher: The spammer's bigger, meaner alter ego

Many organizations treat phishers as "just another spammer" and in some ways, phishing e-mails do look and act like spam. They come in unsolicited and tend to request something of the recipient such as a purchase, an action or an entry of information. But the similarity ends there. While spammers send junk mail that is often blatantly spam, phishers cloak themselves in the guise of trusted partner or friend. While the spammer seeks attention, the phisher avoids it, masquerading as a trusted source and using your corporate e-mail system and your employees against you.

While neither the spammer nor the phisher is welcome on your corporate e-mail system, the phisher is by far more threatening. While a little spam might be annoying but acceptable, a phishing is totally unacceptable. A single successful instance of e-mail phishing targeted towards your organization could expose your corporate network, corporate data, employees and customers to the criminal or malicious imagination of every hacker and criminal on the Web. Even if the hole is patched almost immediately, there might be time enough for the phisher or more likely their malcontent friends to harvest an entire database of customer credit card numbers and destroy your reputation.

The Phish: Phishing, bogus updates and billing fraud

The three most common types of fraudulent emails are phishing, bogus updates and billing frauds.

Phishing

Phishing tries to hook unwary victims by leveraging their confidence in recognized brands and trusted sources. Like their consumer counterpart, enterprise phishing e-mails also appear to come from trusted sources, such as company management, your IT department or a business partner. They inform the recipient that updated information is needed immediately to keep an account open or maintain network access. They usually include a link to a "spoofed" or fake Web site. Simply by following directions, the employee unwittingly provides the phisher with sensitive financial data or network access information. With your corporate network compromised, you may have no choice but to recall and reissue all secure ID badges, check all devices for malicious software and trace all account activity for evidence of unauthorized activity.

Bogus updates

Another form of e-mail attack is the bogus update. Among the most common types of bogus update is the software update–a fraudulent e-mail that informs your employees of the availability of new versions of software and sends them to spoofed Web sites where they are asked to verify account information to receive the update and then unwittingly download malicious code. Once downloaded, the malicious code can attack in a number of ways. It can bypass security protocols to obtain enterprise information; damage hard drives beyond recovery; steal e-mail addresses for mass mailings of malicious messages; or infect other users through chat sessions. The key to having an employee detect a bogus update is having a clearly defined and communicated "how your system is updated" policy, so that bogus update e-mails would never be trusted in the first place.

Billing fraud

Fraudulent billing e-mails take advantage of the fact that no process or person is perfect. Every day in accounting departments around the world, accounting staffs process billions of dollars in legitimate business payments. When an account falls behind, sometimes a vendor sends an email notice, which in turn prompts

someone in accounting to process a payment as directed. Sometimes, to expedite payment, accounting may use a corporate credit card to pay the bill online.

By closely mimicking the look and feel of a trusted vendor or partner, phishers use fraudulent billing e-mails to obtain credit card information, illegal payments or both. In extreme cases, phishers change your processes for electronic invoicing, re-directing all payments to a particular vendor to the phisher instead.

The Facts: Anti-spam and anti-virus solutions alone won't stop phishing

Businesses are well aware that email threats such as spam and viruses can cripple productivity, increase liability and cause IT costs to skyrocket. As a result, they have invested millions of dollars in anti-spam and anti-virus protections.

- Myth #1: The best way to prevent phishing is to stop phishing e-mails just as you stop spam–with your spam filter.

  Fact: Phishing e-mails are specifically created to imitate legitimate e-mails. They are well-written, business-oriented e-mails from an apparently trusted source–exactly what anti-spam filters must allow into your organization. Some phishing e-mails carry out this deception so well that they consistently elude spam filters. While it is tempting to equate the two, phishing is not spam. Phishing requires specific analysis, identification, and handling in order to keep it from having a negative impact on your organization.

- Myth #2: Using a URL blocking service will block phishing e-mails.

  Fact: A URL blocking service is a list of known phishing Web sites. The links in an e-mail is tested against this list and if there is a match, the e-mail is a phishing e-mail. This method is good, but slow. Phishers can launch attacks and collect their desired information in just few hours, often before the URL is reported, verified and listed on the URL block list. What is needed is an analysis of the content to help identify it as a potential phishing e-mail. Spam filters are trained to discover spam–that is e-mail that looks bad, what is needed is a phishing filter that looks for e-mail that looks good, but has a few subtle tricks such as URL masking or spoofed sender.

- Myth #3: If phishing detection technology fails, employees can recognize phishing e-mails.

  Fact: You cannot count on the abilities of your employees to distinguish legitimate content from its phishing twin. SonicWALL research shows that when people are asked to determine is a suspect e-mail is a phishing e-mail or a legitimate e-mail they are wrong 22% of the time. In addition, 1 in 10 people will act on a phishing e-mail even after they have been told it is suspicious, this includes opening the phishing email, clicking on the links, and even entering data into the phishers Web site.

Four Steps to an Effective Anti-Phishing Solution

An effective anti-fraud solution combines innovative tools and techniques specifically designed to combat phishing with consistent and accurate communication. SonicWALL recommends four steps: Detect, protect, align and inform.

Detect: Use analysis techniques specifically designed to detect fraud

Spam filters, which are specifically designed to let legitimate e-mail into your corporate network, will not stop phishing e-mail that looks identical to the real thing. An effective anti-phishing solution must be able analyze a variety of message attributes that set phishing e-mail apart from spam and legitimate e-mail–including sources, formats, structures and content–and make definitive judgments about authenticity.

Protect: Develop containment and control protocols specifically for phishing e-mail

Phishing e-mail is not spam. It should not be placed into quarantine with spam and allowed into your corporate network where your employees might remove it from quarantine and act on it. An effective anti-phishing solution must be able to segregate phishing e-mails immediately from other types of unwanted e-mail and offer your IT department the option of deleting them at the perimeter of your network, before they have a chance to reach any recipient. In fact, SonicWALL strongly recommends that only members of your IT staff are authorized to view and delete phishing email once it has been identified and segregated.

Align: Make your anti-phishing solution part of an overall e-mail security solution

Your anti-phishing solution should not stand alone. An effective solution should offer a number of options that align with other corporate security processes. Your legal department may want a paper trail of all attempted phishing attacks, while corporate security may want alerts about new types of phishing as they emerge. Your anti-phishing solution also should be linked into a greater network of security entities outside your business that send out regular alerts about emerging fraud techniques, giving your IT department the best possible information and the longest possible lead time to build new defenses before a new phishing outbreak hits your organization.

Inform: Improve the Phishing IQ of your organization

The more your employees know about how they are being targeted and what they should do when they suspect e-mail phishing, the more likely they are to take appropriate action when you are hit by a phishing attack. An effective anti-phishing solution needs distinct phishing reporting and alert and feedback tools, so that administrators can be kept aware of trends, make necessary modifications at the network level and report those findings back to other entities that are part of your security network both inside and outside your organization. Alerts should be educational, instructional and should heighten awareness and caution.

SonicWALL offers a free Web-based Phishing IQ quiz, which anyone can take just by visiting http://www.sonicwall.com/phishing. This quiz is just part of the education employees need to receive to perform their jobs in a safe manner. The more they know, the better prepared they can be.

Conclusion

Phishing is not new and businesses have fought the phisher since the beginning of e-commerce. But just as business practices evolve to keep pace with emerging technology, phishers also adapt to the new opportunities that technology offers. Nevertheless, by understanding phishing as a distinct and more sophisticated type of email threat, and by seeking solutions designed specifically to stop phishing e-mail, you can protect yourself and your organization.

While specialized applications to prevent spam and virus attacks are available, a solution that integrates anti-spam, anti-virus and anti-phishing detection makes the most sense. Not only does an integrated solution reduce administration and increase efficiency, it also allows you to analyze the sources of greatest threat and respond accordingly. Most important, all elements of an effective anti-phishing solution should be transparent to your employees and performed automatically at the perimeter of your network.