ciphertrust.com

October, 2004

No Phishing: Protecting Employees from E-mail Fraud

CipherTrust®

Peace of Mind in Messaging™

Phishing Overview

Identity theft, or stealing a person's credentials to gain access to accounts and information, has become the number one crime in the United States[1]. One of the fastest growing forms of identity theft is phishing, a relatively new form of online fraud that focuses on fooling the victim into providing sensitive financial or personal information. Phishing uses bogus e-mail and websites that bear a significant resemblance to a tried and true online brand. Typically, the victim provides information into a form on the imposter site, which then relays the information to the fraudster.

Although this form of fraud is relatively new, its prevalence is exploding. From November 2003 to May 2004, phishing attacks increased by 4000%. Compounding the issue of increasing volume, response rates for phishing attacks are disturbingly high, sometimes as high as five percent, and are most effective against new Internet users who are less sophisticated about spotting potential fraud in their inbox.

The dangers posed by phishing extend across the company, from employees to customers to the very backbone of the enterprise network. Among the many risks are employee exposure to phishing scams, company brand degradation, loss of customer trust, network intrusions, dissemination of trade secrets and violation of federal legislation regarding confidentiality. Failure to mitigate these risks can prove catastrophic to the company's ability to function.

Employee Exposure

While employees are at work, the corporate network serves as a virtual ISP. This puts the onus on the company to ensure that employees are safe from all types of e-mail threats, including phishing attacks. Failure to protect employees puts the corporation at risk of being held liable for not taking steps to prevent offensive or fraudulent material from passing through the gateway. In addition, the time and effort spent dealing with each individual incident is costly, resulting in lost productivity, frustrated employees and potential missed sales.

Brand Degradation

If a hacker impersonates a company, the company's reputation and brand may be tarnished or ruined because customers feel that they can no longer trust communication purporting to come from the company. Each time a phishing attack is launched, a legitimate company's brand equity is eroded. The more attacks a company suffers, the less consumers feel they can trust the company's legitimate e-mail communications or websites. This vicious cycle can prove nearly impossible to break.

Loss of Customer Trust

The value of trust is difficult to quantify – at least until a company begins to lose customers. If a company is victimized by a phishing scam, customers no longer trust the company's ability to protect their personal information and they often defect to competitors. Companies that fail to openly communicate with customers about the dangers of phishing and how to identify legitimate messages are in grave danger of falling victim to the ever-growing threat. For those organizations that frequently process consumer credit card transactions, the risk is even greater.

[1] *Electronic Safety and Soundness: A Four Pillar Approach, Glassner, Kellermann, McNevin, The World Bank Integrator Group, 2003*

Network Intrusions

Fraudsters use social engineering and other methods to entice employees to divulge sensitive information to persons outside the organization. With even a little knowledge of an organization's business methods, hackers can easily distribute hundreds or even thousands of spoofed messages to an organization's employees. The messages may ask for network passwords and usernames, or may attempt to fool employees into providing sensitive information to competitors. Once the hackers have the information they need to access a corporate network, the damage potential is unlimited.

Dissemination of Confidential Information

Information gleaned by fraudsters from corporate networks can be used in a variety of nefarious ways. In the financial services industry, criminals can use credit cards to deduct money straight from accounts of unsuspecting victims. Many other organizations hold private healthcare information or personal financial information that could be used by criminals to extort payoffs from corporations wishing to avoid the bad publicity of a security breach becoming public knowledge.

Regulatory Non-Compliance

With the recent Federal regulation of information security policy through legislation such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act (SOX), enterprises are charged with protecting data residing in mail servers and on other internal systems. Security breaches violate these regulations, exposing sensitive data and opening the door to serious sanctions and costly litigation.

Preventing Phishing Attacks in Enterprise Networks

A multi-tiered approach is necessary to fully protect a company from phishing attacks. Combining employee and customer education with new technology such as the Sender ID Framework and spam filtering ensures that fraudsters will not find their victims in your enterprise.

Education

Education is a strong defense against phishing attacks in corporate environments. Employees must be well-informed about phishing and how to spot fraudulent e-mails and websites. It is also important to properly train employees about what information is appropriate to share through e-mail, and specifically what steps employees should take if they are unsure about the authenticity of a request for information.

In addition, companies must make a concerted effort to educate their customers about phishing. By doing so, they make themselves much less attractive targets than companies which make no effort at all. Clearly, the goal is to convince the fraudsters that a company's customers will not fall for the scam. Having an obvious anti-phishing program that is public for all to see can be very effective, as the fraudsters tend to follow the path of least resistance. Seeing that customers are well informed of how to avoid phishing attacks, the perpetrators simply turn their attention to other "softer" targets.

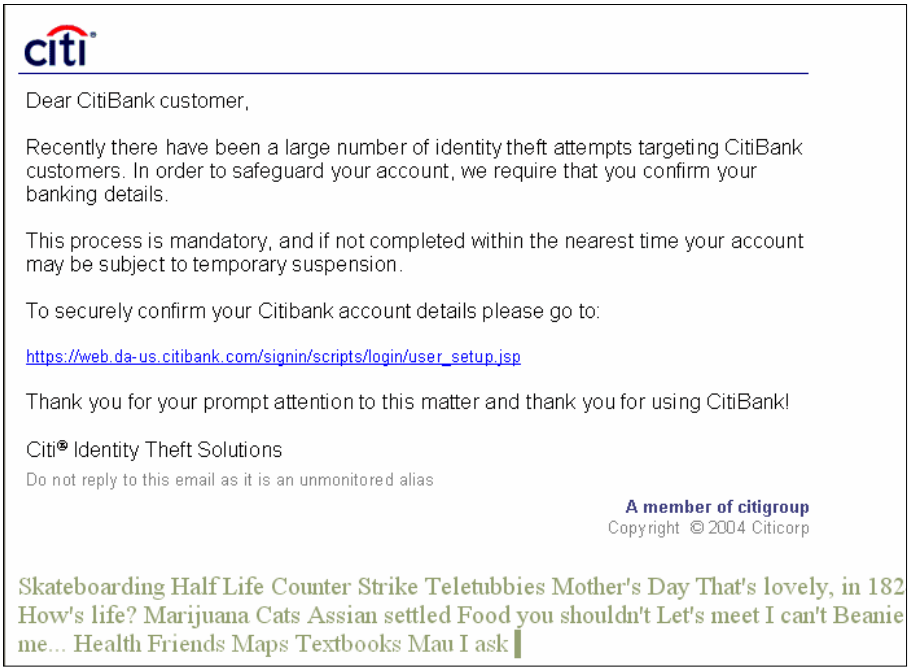
Sender ID Framework

New technologies are available to help prevent phishing. One such technology, offered as a standard by Microsoft and supported by CipherTrust, is the Sender ID Framework (SIDF), which prevents spammers from concealing their IP address by verifying the source of each e-mail. Registering its domains with SIDF helps ensure that a company's customers will not receive phishing e-mails claiming to be from them.

Of course, education and SIDF are not always enough to prevent all phishing attacks. The best protection against phishing is to keep these attacks from ever getting to the user's inbox. Since most phishing attacks proliferate through unsolicited e-mail, spam-filtering technologies can be very effective at preventing the majority of phishing attempts.

Case study: IronMail Caught It – A User May Not

Figure 1: Clever Phishing


citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup

Copyright © 2004 Citicorp

Skateboarding Half Life Counter Strike Teletubbies Mother's Day That's lovely, in 182 How's life? Marijuana Cats Assian settled Food you shouldn't Let's meet I can't Beanie me... Health Friends Maps Textbooks Mau I ask

Figure 1 is an actual e-mail recently sent to a CipherTrust employee. IronMail tagged this particular message as a threat and quarantined the message, blocking it from delivery to the employee. The following characteristics of the message are indicators that it is not, in fact, from Citibank, but a cleverly disguised phishing scam that likely fooled enough users to make the venture quite profitable for the phisher:

1. The entire message is actually presented within an image, rather than as plain text, a common trick used by spammers to fool content filtering software.

2. The URL to which the user was asked to send their information was masked in a hex encoding to prevent realization that the destination was not actually Citibank and to prevent spam and phishing detection technology from identifying a suspicious URL.

3. The Citibank graphic and the look and feel of the message is lifted directly from Citibank's website, so it is identical to a message that might come from the company and likely to be accepted as genuine by many victims.

4. Social engineering techniques take advantage of the victim's concerns about account security by paradoxically presenting the message as a security warning about phishing scams. By portraying the message as "mandatory" and threatening the user with "temporary suspension" of his or her account, the victim is coerced into a feeling of urgency and is more likely to fall for the fraud.

5. The random text at the bottom of the message is not contained within the graphic that houses the message body and is designed to fool Bayesian filters. At its most basic level, a Bayesian filter examines a set of e-mails that are known to be spam and a set of e-mails that are known to be legitimate. It compares the content in both e-mails and builds a database of words that will be used to filter messages entering the e-mail gateway and determine whether they are spam or not.

6. By using a white font on a white background, the fraudster intended to hide the random text from the user.

How Did IronMail Detect the Scam?

IronMail detected this message with a sophisticated correlation engine called Spam Profiler, which integrates an array of technologies and evaluates more than 1000 message characteristics to accurately differentiate legitimate messages from spam or scams. The most significant items that keyed the quarantine of this phishing scam are:

1) Header Analysis

"Spoofing" is the act of mimicking genuine e-mail addresses to give the impression of an authorized communication from a business, and is a common tactic used by spammers. In Figure 1, items such as the "From:" address and the originating mail server were inconsistent with that of mail sent legitimately by Citibank, allowing IronMail's header analysis to accurately detect that "spoofing" was employed. In addition, IronMail detected discrepancies in the headers that indicated that the sender was attempting to deceive the recipient server.

2) Bulk E-mail Detection

With more than 2000 IronMail units in the field protecting over 7 million enterprise e-mail users, CipherTrust detects new attacks quickly. While some "mass personalization" was employed to make each version of this message unique, it was detected at multiple sites and identified as a mass e-mailing and potential spam or attack.

3) URL Filtering

Despite the attacker's use of hex encoding to hide the URL of the fake Citibank website, IronMail was able to decode the URL and identify it as a suspected spammer URL.

4) Anomaly Detection

IronMail's anomaly detection engine is able to scan e-mail traffic for behavior that indicates an attack. This can include the number of messages, the origin, the delivery method or any other

Penalty

According to CNN.com, the first federal phishing case was prosecuted by the FBI in 2004.[2] Ironically, an FBI agent with an expertise in cyber crime received an e-mail purporting to be from AOL. The agent explored the link and discovered that it was directed to a site unrelated to AOL. The agent also determined that the sender's e-mail address was invalid and that the message was sent to multiple users – tell-tale signs of spam or scam. The agent called for further analysis of the message in what was then called the Bureau's Special Technologies and Applications Unit of the National Infrastructure Protection Center, and the message was confirmed as a phishing scam. Upon further investigation, the FBI uncovered a trail of several stolen accounts, as well as a computer that contained account information for over 400 credit cards acquired over the course of the scam. One person has been sentenced and another is currently awaiting sentencing.

[2] *http://www.cnn.com/2003/TECH/internet/07/21/phishing.scam/*

characteristics of the message. Anomaly detection is instrumental in detecting new and previously unknown attacks.

All of these techniques operate in real time and scrutinize the behavior of the message rather than the weaker approach of trying only to identify content. Combining these techniques in a "cocktail" approach enabled IronMail to discover the strategy of the scam artist and prevent the exposure of this message to an unsuspecting end user. If used alone, each of these techniques might contribute to stopping legitimate messages. However, IronMail's Spam Profiler enabled IronMail to consider the results of all of its detection tools simultaneously and make an accurate decision on the malicious nature of this message.

IronMail blocked this message instantly, preventing any IronMail users from being trapped by this clever phishing scam.

Conclusions

Phishing is currently a tremendous e-mail security threat that can easily result in identity theft and/or compromise of corporate networks. The most effective ways to combat phishing are a combination of education, law enforcement and, most importantly, an enterprise-wide e-mail security solution that can prevent even the most clever phishing scams from reaching the desktop of unsuspecting end users. IronMail has proven to be the most effective e-mail security solution for detecting even the most insidious attacks and protecting corporate networks from this next phase of organized crime.

This foregoing document was electronically filed with the Public Utilities

Commission of Ohio Docketing Information System on

4/16/2007 11:19:29 AM

in

Case No(s). 04-6000-XX-XXX

Summary: Agreement electronically filed by Mr. James P. Logsdon on behalf of Another Company