

Phishing for Disaster: The Cost of Corporate Ignorance



Published July 2010

A brief whitepaper about the effects of corporate ignorance of phishing and actions companies must take to protect their financial and intellectual assets, employees and customer relationships.

Introduction

Despite multiple, widely publicized cyber-attacks that have resulted in personal, corporate data and direct financial losses reaching nearly \$1 trillion dollars, most companies still do not have adequate protection against phishing attacks. Executives ignore, downplay or misinterpret the enormous threats these attacks represent, even though 83 percent of companies have been victims of an advanced threat, according to a recent Ponemon Institute surveyⁱ of c-level executives. These threats are defined as methodologies “employed to evade an organization’s present technical and process countermeasures, which rely on a variety of attack techniques as opposed to one specific type.”ⁱⁱ Nearly half of the survey respondents reported a theft of confidential information or intellectual property. Despite these occurrences, the wake-up call has yet to be heard. At best, companies have implemented weak controls, while training and security measures are incapable of keeping pace with today’s cybercriminals. An inadequate response to these very real threats puts everything that matters at risk: intellectual property, revenues, employees, and brand reputation.

This brief white paper details the effects of corporate ignorance about phishing, and outlines the actions companies must take to protect their financial and intellectual assets, employees, and customers.

Weak Corporate Security at Best

Protecting company assets is simply a cost of doing business. In an attempt to curb corporate espionage, companies have spent billions on security guards and closed-circuit security cameras. Employees wear ID badges; lobbies and entries feature body scanners, biometrics and other security measures. While these systems are reasonable deterrents, corporate spies don’t need guns, disguises or fake badges to access corporate information when a mere keyboard will suffice.

Unfortunately, some companies scoff at the notion that phishing attacks are vectors for industrial espionage and information warfare. They fail to grasp that the personalized and targeted characteristics of spear phishing can unleash a major attack on corporate well-being. All it takes is just one naïve or careless person to fall for a well-crafted phishing campaign to make a company vulnerable.

Today’s phishing attacks pose threats on par with traditional corporate espionage, yet most companies do not have the policies and solutions in place to prevent its cyber equivalent. Indeed, conducting a phishing campaign is easy and inexpensive. In May 2009, even the editors at *BBC Click* got their hands on a botnet that controlled 22,000 infected PCs and executed a spam campaign.ⁱⁱⁱ Botnets are regularly used in phishing attack, and for these email-based attacks, the criminals with keyboards are outthinking and outworking their prospective victims.

In February 2010 NetWitness, “discovered a dangerous new Zeus botnet”^{iv} affecting more than 75,000 systems in 2,500 organizations around the world. “Deeper investigation revealed an extensive compromise of commercial and government systems that included 68,000 corporate login credentials,

TYPES OF PHISHING SCAMS

Classic Phishing

During the peak of the economic downturn, Red Condor issued warnings for classic phishing campaigns that targeted people looking for employment. Emails claimed to be offering employment from familiar, reputable companies such as Pepsi and Starbucks, or they masqueraded as messages from sites like CareerBuilder or Monster.com. Fake employment offers frequently involve “payment processing” requests, which give scammers an excuse to ask for a respondent’s bank account.

Sophisticated Phishing Attacks

In early 2010, sophisticated phishing attacks requested legal representation to help in the “collection of delinquent accounts.” Most of these messages appeared to come from legitimate corporations from the Asia-Pacific region and London. In reality, the emails originated from servers around the world with a web mail sender address such as Yahoo. The scammers used real addresses, phone numbers and other contact information that could fool even the savviest of email users.

Spear Phishing

A spear phishing campaign is a highly targeted form of phishing that focuses on a single organization or handful of individuals in that organization. Emails appear as if they come from a trusted source, such as an employer who would normally send an email to the entire company or a well-known organization. An aggressive spear phishing email campaign in early 2010 redirected users to a web site that appeared to be a Microsoft® Office Outlook® Web Access page, including official Microsoft® and Microsoft Office logos. Users were directed to “download and launch a file with a new set of settings for your e-mail account.” The executable was actually a Zbot Trojan virus.

Blended Threats

The goals of a blended campaign are to capture credentials and embed malicious software onto users’ systems to facilitate stealing additional information and/or hijacking the system to send out more spam. In early 2010, Red Condor blocked a blended threat attack that spoofed eBay. An embedded link took users to a compromised site on eBay’s network and a “Download Now” button that when executed installed a Trojan virus. Victims were then directed to log into their eBay accounts—scammers then captured eBay log-in credentials.

access to email systems, online banking sites, Facebook, Yahoo, Hotmail and other social networking credentials, 2,000 SSL certificate files, and dossier-level data sets on individuals including complete dumps of entire identities from victim machines.” Zeus is a readily available malware kit that sells for between \$400 and \$700, allowing anyone with the funds and the right computer experience to create a botnet.

Economic Impact of Spear-Phishing

The economics of phishing are simple. The narrower and more focused and personalized the attack, the greater the potential for economic payoff. There are numerous examples of companies that have lost thousands to millions of dollars as a result of phishing and spear phishing attacks. Most involve the companies’ financial institutions. And unlike consumer banking laws which protect personal assets up to \$250,000, business assets in corporate accounts aren’t protected from fraudulent transfers.

In early 2010 when the owner of a California escrow firm opened an email message that appeared to come from UPS, she unwittingly clicked on an attached “invoice” file containing a Trojan virus. When nothing happened, she forwarded the email onto her assistant who repeated the process. The “silent click” resulted in the installation of a computer virus that allowed cyber-criminals to remotely manipulate security measures that would have informed the owner of the transfers, including transfer verification emails sent to both the owner and her assistant. The criminals then hijacked the firm’s bank account and sent 26 wire transfers totaling \$465,000 to 20 individuals and small businesses around the world. To survive, the owner of the firm had to acquire a \$395,000 loan at 12 percent to cover the loss.^v

In another incident involving Experi-Metal Inc. (EMI), a Michigan-based company, phishers sent an EMI employee an email that appeared to come from Comerica Bank. In the past, the bank had used email to renew its digital certificates. Assuming the email was legitimate; the employee clicked on the link in the email and provided the company’s online banking credentials, including a code from a bank-issued security token. In a three-hour period, the phishers made 47 wire transfers totaling more than \$550,000 to accounts in China, Estonia, Finland, Russia, Scotland and domestic accounts where funds

were immediately withdrawn.^{vi} EMI is currently suing Comerica in an attempt to recover the stolen funds.

The list of victims of this type of scam is long. In each case, the banks claimed they had reasonable security measures, the transfers used valid processes and procedures, and nothing looked out of the ordinary. In the end, the banks blamed the companies and their employees. These thefts did not require access to a building, bugging an office or dumpster diving. **Rather, the crimes were executed from computers thousands of miles away, for equally devastating results.**

Damage to Reputation

A successful phishing attack can damage and even destroy a company's reputation. In the examples above, the banks and their business customers suffered the consequences. While banks tout the physical and online security of their services, reality suggests otherwise--particularly for businesses whose funds are not backed by the government or the banks in the event of a phishing attack. Like their one-time customers, their reputation can be damaged.

Individual victims of phishing attacks also take hits to their reputation, which can ultimately harm the corporate brand. The California escrow firm mentioned earlier serves as a guarantor of payment for real estate transactions, holding funds until the sale of a property is complete. Had the owner of the firm not received a loan to replenish the funds in the escrow account, she could have easily faced bankruptcy or a crippling lawsuit that could have hurt her personally and professionally.

The recent attack on venture capitalist and Facebook board member Jim Beyer demonstrates how even savvy users can fall for a phishing attack that can lead to serious violation of personal reputation and social trust. On May 8, 2010, 300 Facebook friends of Mr. Breyer received a bogus event invitation that succeeded in getting users to divulge their Facebook passwords. The same email was distributed to all of *their* Facebook friends as well.

What would have happened, if rather than compromising a Facebook account, scammers had gained control of the Breyer's email account, which Facebook requires for usage? Scammers could have easily exploited this address, with far more serious consequences for Breyer and his professional and personal networks. Breyer did not escape unscathed—his own reputation as a savvy technologist was tarnished.

The recent iPad and AT&T website security breach is another chilling example of the potential dangers of how easy it is to obtain the email addresses of top officials. While the breach was conducted by security experts to prove a point, had it been executed by hackers with malicious intent, the effects could have been catastrophic. Security experts were able to "steal" the email addresses of 114,000 iPad registered users, among them White House Chief of Staff Ron Emanuel and FBI officials.

Protect Your Company and Your Customers

To protect against cyber-crimes, companies need to make security a focal point. Today's software security flaws are tomorrow's exploits, and customer perception of your brand as secure is paramount, regardless of your industry or product category.

Facebook, Twitter and craigslist are among the dozens of brands that are continually spoofed, and whose reputation for caring about privacy and security appears, at least to the public, to be minimal. Another major brand, Adobe, has become synonymous with the word exploit, as scammers and cyber criminals continue to use holes in Adobe's software to launch and install malicious malware campaigns on unsuspecting victims. If there is any notion that a company does not care about protecting its customers, an erosion of trust follows that could ultimately impact long-term viability.

Finally, companies need to develop their products and services with the understanding that financial statements, email addresses and phone numbers are potentially sensitive information. Phishers are looking for specific information. They target users of popular sites like Facebook and Twitter and spoof local banks and famous retailers because the data they steal can be pieced together in order to eventually exploit vulnerabilities and gain access to information that will deliver bigger payoffs.

Financial institutions need to take the lead in security. Given the sensitivity of the data they protect, as these institutions adopt advanced security measures and technologies, others will likely follow.

Safer User Behavior, Stronger Policies

To counter the efforts and advancements of the scammers, the strongest defense against phishing attacks is safe user behavior, strong policies and training procedures, and technologies that support effective anti-spam filters.

Red Condor recommends the following:

- Strong corporate policies reinforced with regular in-person security briefings and education opportunities
- Isolated internal networks, accessible from protected terminals, for storing valuable intellectual property – anything connected to the Internet can be stolen.
- Stronger passwords – Establish passphrases instead of passwords. Most people use the same passwords or variations of the same passwords for multiple accounts, which makes it easy for cybercriminals to piece together identities.
- Cyber security should be treated with the same level of importance as physical security; deploy personal authentication devices, including biometrics and digital keys for all of your users.

Conclusion: Behavior Must Change

Corporations and their executives have yet to grasp the size and scope of the phishing problem. Corporate espionage through phishing is a real problem that demands new approaches and technologies. Advanced security products, services and policies will provide essential protection against phishing attacks. But user and corporate behavior must also change.

In most, if not all security breaches perpetrated via phishing campaigns, email users bear some responsibility. The end user whose actions can either aid or block the objectives of phishing attacks is the biggest challenge facing email security companies and their customers. For their part, users must be diligent about protecting their information and the company's assets. They should also demand better security from the brands they engage and use products and services that make security a priority.

Emerging cyber-security threats thwart traditional defenses. The levels of sophistication, variation of emails and intense targeting have made it difficult for most email security solutions to stop the campaigns before they reach the inbox. Stopping these attacks requires a living and breathing solution that is constantly watching for new campaigns and reacting to changes in spammers' behavior.

Estimated costs of cybercrime – half a billion dollars to nearly \$1 trillion a year – fail to account for the loss of stolen personal banking information or corporate data. As evidenced by the examples mentioned earlier, scammers and cybercriminals are leveraging phishing scams to capture usernames and passwords of unsuspecting victims to completely liquidate their financial accounts. As the criminals maximize the profit potential of these scams, they naturally move on to stealing company data and intellectual property, which carry significantly greater value and the loss of which could have an even bigger impact on corporate finances and reputation. When companies pick an email security solution that understands how the scammers operate, they can then realistically expect to stop the threats, and greatly reduce the chance that their business, their employees, or their customers will fall victim to a phishing attack.

To learn more about Red Condor's email security solutions, call 888-966-7726 or visit www.redcondor.com.

For more information about new and emerging phishing attacks and other email threats, visit <http://www.redcondor.com/blog/>

ⁱ <http://lastwatchdog.com/dealing-advanced-cyber-threats-presents-risk-cost/>

ⁱⁱ *ibid*

ⁱⁱⁱ http://www.bbc.co.uk/blogs/theeditors/2009/03/click_botnet_experiment.html

^{iv} <http://netwitness.com/resources/pressreleases/feb182010.aspx>

^v <http://krebsonsecurity.com/2010/06/e-banking-bandits-stole-465000-from-calif-escrow-firm/>

^{vi} http://www.bankinfosecurity.com/articles.php?art_id=2191