ADVISEN
Insurance Intelligence®


# SPEAR-PHISHING ATTACKS: REELING IN CORPORATE AMERICA

*August 2015*

*Sponsored by:*

THE HARTFORD

# SPEAR-PHISHING ATTACKS: REELING IN CORPORATE AMERICA


*Increasingly, criminals use deceptive techniques to exploit corporate business practices and circumvent controls, with the goal of tricking unsuspecting employees into sending money or diverting payments to imposters.*

## Executive Summary

Criminals often find the task of exploiting a person easier than exploiting a web application or network connection. Yet many organizations who collectively invest billions in highly sophisticated security technology fail to adequately address what may be their biggest vulnerability, deception of their employees. Increasingly, criminals use deceptive techniques to exploit corporate business practices and circumvent controls, with the goal of tricking unsuspecting employees into sending money or diverting payments to imposters. This Advisen report, sponsored by The Hartford, examines the increasingly utilized and sophisticated criminal tactic of deception fraud, and offers actionable suggestions for effective risk mitigation.

## Introduction

The weakest link in any organization's security chain may be its employees. This is particularly true if they are not educated about an increasingly prominent type of criminal attacks designed to steal from corporate America – crimes of deception. These criminal schemes manipulate, trick and play on the psyche of employees, leading to transactions involving corporate funds that fall straight into the pockets of the perpetrators. This crime tactic, known as deception fraud or social engineering, is quickly growing in prevalence, and every business is a potential target.

Crimes of deception are nothing new. Criminals have long manipulated aspects of human behavior such as emotion, impulsiveness, naivety, and trust. Confidence scams, from which the term con-artist is derived, are examples of schemes that prey on people's innate desire and willingness to trust others. As with other forms of criminal activity, these scams have evolved in the internet age and allow criminals to become more effective and efficient at executing their craft.

*Deception fraud tactics, which go by names such as baiting, phishing, email hacking and contact spamming, pretexting, quid pro quo, spear-phishing, vishing, hunting, and farming, rely more on the interaction of humans than they do on technological resources and know-how.*

Deception fraud tactics, which go by names such as baiting, phishing, email hacking and contact spamming, pretexting, quid pro quo, spear-phishing, vishing, hunting, and farming, rely more on the interaction of humans than they do on technological resources and know-how. Some of these tactics cast a wide net in hopes of luring a few unsuspecting victims, while others employ a more targeted approach.

According to IT research and advisory firm Gartner, global cybersecurity spending is estimated to reach $76.9 billion in 2015.[1] But as businesses spend billions to fill holes in technology, criminals posing as vendors, CEO's and customers are focusing their efforts on employees as a point of entry to corporate assets and data. "The weakest link in the security chain is the employee who accepts a scenario at face value and doesn't check its legitimacy" said Steven Vardilos, AVP of Fidelity/Crime at The Hartford. "The best defense is employee awareness through education and training."

Deception fraud is an organizational problem that requires an enterprise wide strategy with an emphasis on prevention. Employee education, internal controls, and behavioral practices are the only reliable way to reduce an organization's exposure to a deception fraud related loss.

## A tactical shift

This report will focus on the deception fraud tactic known as spear-phishing, a tactic that is tricking corporate America into sending money to imposters every day.

Traditional phishing attacks rely more on quantity over the quality of contacts. Phishing campaigns cast a wide net through spam emails that attempt to convince the target to click on a malicious link and unintentionally disclose their user credentials. Attackers will play on fear, authority, and urgency to convince the target to make quick decisions based on emotions.

In an example from fall 2014, the US government issued an alert to warn citizens of scams and cyber campaigns that capitalized on fear caused by the Ebola epidemic. The notification warned of online fraud schemes via email and on social media that tried to trick victims into clicking on malicious attachments or malicious links that directed them to websites which collected personal information such as login credentials.[2]

Phishing is one of the oldest deception fraud tactics, and it remains an effective one. Nonetheless, phishing rates are in decline. According to Symantec's 2015 Internet Security Threat Report, the email phishing rate dropped to 1 in 965 emails in 2014

*Spear-phishing campaigns can have various objectives, the most common being to influence employees to transmit funds to an improper source.*

from 1 in 392 in 2013, and the number of phishing URLs on social media remained significantly lower than the peak year of 2012.[3] It appears that a tactical shift is taking place and cybercriminals are becoming more strategic. Attacks increasingly involve targeted reconnaissance in an effort to find pieces of personal and professional information that can be utilized in spear-phishing campaigns.

Spear-phishing takes a more surgical approach by targeting specific individuals. In recent years criminals have increasingly shifted to this tactic because it has proven highly effective. Symantec reported an eight percent increase in the number of spear-phishing campaigns in 2014.[4] Criminals are scouring social media sites, blogs and other websites that house information on a potential target and creating more sophisticated attacks supported by this knowledge.

Spear-phishing campaigns can have various objectives, the most common being to influence employees to transmit funds to an improper source. In one example, fraudsters successfully convinced a controller of an Omaha company to wire $17.2 million to a bank in China through targeted emails. The scam involved a series of emails supposedly from the CEO that explained the details of an acquisition the company was going to make in China, which seemed reasonable to the controller since the company had been discussing a China expansion.

The controller was asked not to discuss the deal through normal corporate channels in order to remain compliant with federal regulations, which explained why the email came from the CEO's personal address. Additionally, he was instructed to reach out to a real employee at the company's accounting firm to obtain instructions on how to wire the money. The fraudster's knowledge of corporate vendors and strategy gave the scam legitimacy in the eyes of the controller and he comfortably sent the money to the Chinese account.[5]

Other spear-phishing objectives include stealing confidential or proprietary information for the purpose of selling it on the black market, or implanting cyberespionage malware in order to gain long-term access to an organization's sensitive information. Last year, for example, a multiyear Russian cyberespionage campaign known as Sandworm was discovered. The Sandworm gang used a zero-day flaw found in all supported versions of Microsoft Windows to implant a BlackEnergy Trojan virus. The gang utilized spear-phishing emails with malicious PowerPoint presentation attachments to infiltrate energy and telecommunication companies, educational institutions, and government networks.[6]

*Although spear-phishing campaigns are becoming more sophisticated, scams need not always be complicated to be effective.*

Sadly, cases like these are becoming all too common. According to a report from the Internet Crime Complaint Center (IC3), which is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), 2014 saw a spike in spear-phishing attempts and the use of social media as a tool for criminal activities. According to IC3, 12 percent of the FBI's cyber related complaints had a social media component in 2014, a number that has quadrupled over the previous five years.[7]

Although spear-phishing campaigns are becoming more sophisticated, scams need not always be complicated to be effective. The source of vulnerability is a human, not a well-fortified corporate network, and a cleverly worded email is often all that is needed.

Masquerading, also often referred to as CEO fraud, is a scam that capitalizes on urgency and employee reverence to superiors. Criminals will gain access to corporate executive emails or make subtle changes to the email address and make urgent wire transfer requests to employees. An employee's desire to go above and beyond for their superior often leads them to follow through with the request and, in some cases, even violate corporate protocol to do so.

Recently, for example, a US magazine publisher fell victim to a costly spear fishing attack that began with a deceptive email to the CEO. The targeted attack enabled hackers to install malware and gain access to the CEO's email account. The scammers, masquerading as the CEO, then sent emails to employees who had access to the company's bank accounts and requested that $1.5 million be transferred to a Chinese bank account.

Even less sophisticated, but arguably just as effective, are masquerading scams by telephone. Fraudsters will make aggressive phone calls posing as someone of power such as the CEO, CFO or comptroller, and bully the employee into wiring the money. Fraudsters also can pretend to be someone of power from outside of the organization. In one example fraudsters pretended to be IRS agents and threatened to arrest employees for tax fraud if they failed to make an immediate transfer.

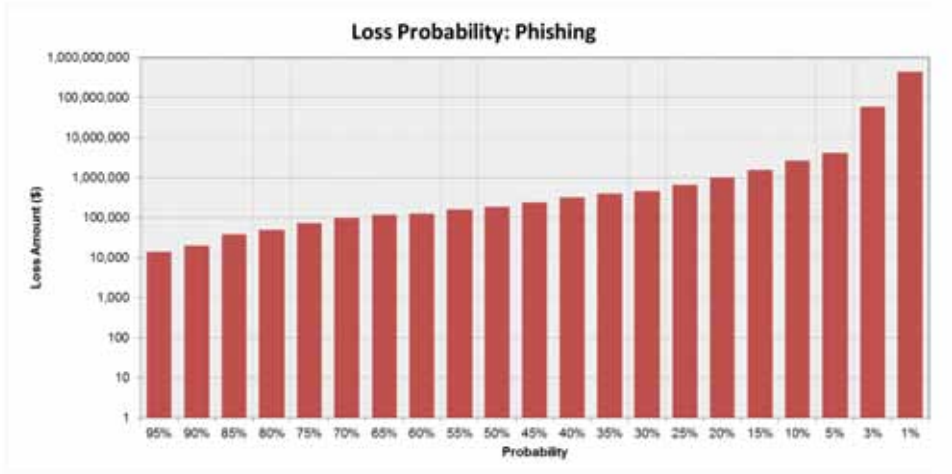
The size and sophistication of a company makes little difference: even Fortune 500 companies are vulnerable. In 2013 the DEF CON security conference held a social engineering capture the flag competition. Ten major U.S. companies were targeted via telephone and almost all released valuable information to the scammers, such as the name of vendors and suppliers, which could be utilized in an attack.[8]

*And while the potential loss from a traditional phishing attack can be severe, the increase in spear-phishing should be cause for even greater concern.*

## What are the stakes and who is most a risk?

According to an often cited report by RSA, the security division of EMC, in 2014 there were nearly 450,000 phishing attacks globally causing an estimated $5.9 billion in losses.[9] On a per loss basis, the financial impact to an organization can be significant. According to Advisen there is a 20 percent probability that a loss from a phishing attack will be in excess of $1 million. (Exhibit 1)

**Exhibit 1:**




And while the potential loss from a traditional phishing attack can be severe, the increase in spear-phishing should be cause for even greater concern. According to a report by internet security firm FireEye, "Compared to broad-based emails, spear-phishing costs 20 times more per individual targeted. However, the average return from each spear-phishing victim is 40 times more than that of phishing."[10]

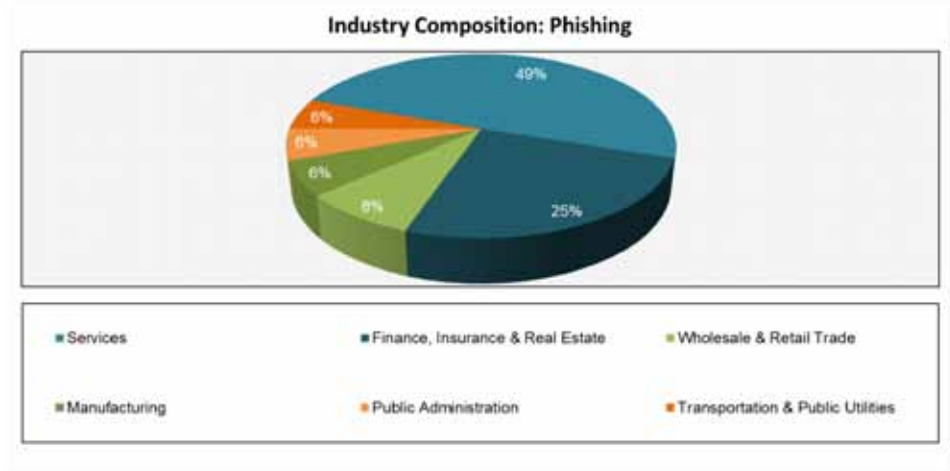
Every company, regardless of size, is vulnerable to a cyberattack with a social engineering component. The Hartford's 2014 Midsize Business Monitor, for example, reported that 45 percent of mid-sized businesses experienced a phishing incident in the past three years and 68 percent feel at least somewhat likely to experience one at some point in the next three. [11] Additionally, Symantec reported that 59 percent of all spear-phishing attacks were directed at small and medium sized businesses in 2014.[12]

Complacency is often the biggest issue for smaller businesses because they frequently have the perception they have nothing of interest to cybercriminals. They also have the false notion that they are anonymous based on their size. But in fact, the opposite is more likely the case; cybercriminals frequently target smaller companies that have proven to lack even the most basic cyber defenses.

*Deception fraud related losses can cause significant damage to the targeted company, and it can be difficult to recover lost funds.*

Cybercriminals have different motives, so all businesses should assume they are a potential target. Nonetheless, certain industries are at greater risk than others. Advisen found that the services sector (e.g. healthcare, education, hospitality etc.) is targeted most frequently for phishing attacks. (Exhibit 2)

**Exhibit 2:**




With regards to spear-phishing, Symantec found that "overall in 2014, the manufacturing sector was targeted with the greatest volume of spear-phishing attacks, as 1 in 5 were directed at manufacturing organizations." Other highly targeted sectors included nontraditional services, finance, Insurance & real estate, professional services, and wholesale.[13]

When normalized by the number of companies in a particular industry, Symantec found "the mining industry was the most heavily targeted in 2014, with 43 percent of mining organizations being targeted at least once during the year." Other heavily targeted industries included wholesale and manufacturing.

## Risk Mitigation

Deception fraud related losses can cause significant damage to the targeted company, and it can be difficult to recover lost funds. For example, when a U.S. based escrow firm wired payments to fraudulent accounts in Russia and China totaling more than $1 million, it was only able to recover a third of the lost funds, forcing it out of business. In addition to any immediate financial losses, other costs associated with responding to the fraud such as investigation and litigation can also be substantial. There are also the less quantifiable costs such as the impact the fraud may have to brand and reputation.

*Unfortunately, even companies with a strong internal control environment are not immune to these crimes of deception…*

Unfortunately, even companies with a strong internal control environment are not immune to these crimes of deception, explained Vardilos. "The weakest link in the security chain may ultimately be an employee who accepts an email instruction or a phone call request to transfer company funds at face value. That's why it is so important for companies to offer employees' anti-fraud training on the potential 'red flags' associated with deception fraud scams."

Below are some actionable suggestions from The Hartford for mitigating the risks of deception fraud losses.

- Education/Training:
  - Keep employees informed on the type of scams being perpetrated.
  - Provide anti-fraud training on how to recognize an attack and report suspicious behaviors that violate company policies and procedures.
  - Train employees on what information is confidential and what should never be released unless approved by management.
  - Train employees to slow down if the message conveys a sense of urgency, intimidation, or high pressure sales tactics.
  - Train employees not to forward, respond to, or access attachments or links within unsolicited emails.
  - Hold employees accountable but also create a culture where they are rewarded for verifying suspicious activity.

- Internal Controls
  - Authenticate changes to vendor or customer contact information and internal bank information.
  - Require supervisor sign-off on any changes to vendor and client information.
  - Validate requests from vendors and clients.
  - Validate all internal requests to transfer funds.
  - Limit wire-transfer authority to specific employees.
  - Guard against unauthorized physical access (theft of keys, access cards, ID badges etc.).
  - Keep physical documents locked and secured and shred documents no longer in use.
  - Monitor the use of social media.
  - Develop reporting and tracking programs that document incidences of deception fraud or attempts of deception fraud.
  - Keep cyber security software up to date.
  - Implement mobile device security procedures.
  - Use two factor authentications on your organizations computer platform(s).

*Although deception fraud attacks will likely continue with increased frequency and sophistication, every company has the capability to minimize the risks.*

Organizations should continually monitor the effectiveness of their education, training, and internal controls by conducting third party penetration testing. These fake hacks provide valuable information on how to focus training and educational efforts.

In one example 280 employees of the city of Kansas City fell for a fake phishing attack conducted by city auditors. In this case, the auditors sent 3,115 fake phishing emails to employee inboxes. Within hours hundreds had clicked on the link. It took four hours for the city's IT staff to identify the phishing email and begin to alert employees and a full day to delete the phishing email so no one would be able to click on it. Employees who had clicked on the link were instructed to change their log-in passwords of which two thirds did within 24 hours, but thirty percent did not within 48 hours of the attack.[14]

These audits provide an abundance of teachable moments, they also provide a baseline for the effectiveness of an organizations security education and training, and identify employees who need additional training.

Lastly, organizations should purchase insurance as a last line defense from deception fraud losses. Many traditional crime policies are not intended to provide coverage for these types of losses. However, a few leading carriers, including The Hartford, are providing coverage for deception fraud via an endorsement to the crime policy. The coverage pays for loss of money or securities when an employee is misled by an imposter email, phone call, or text message and induced to surrender corporate assets.

## Conclusion

Although deception fraud attacks will likely continue with increased frequency and sophistication, every company has the capability to minimize the risks. The good news is that it does not require a massive IT budget, but instead a commitment to invest the time and resources into employee education and training. As a result, there is no excuse not to implement basic deception fraud security measures, and every company should consider insurance as an important component of their overall risk management program.[15]

*This Report was written by Josh Bradford, Senior Editor, Specialty Editorial, Advisen Ltd.*

[1] Gartner, Press Release, "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware", (August 22, 2014), http://www.gartner.com/newsroom/id/2828722

[2] US-CERT, "Ebola Phishing Scams and Malware Campaigns", (October 16, 2014), https://www.us-cert.gov/ncas/current-activity/2014/10/16/Ebola-Phishing-Scams-and-Malware-Campaigns

[3] Symantec Corporation, "Internet Security Threat Report", Volume 20, (April 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[4] Symantec Corporation, "Internet Security Threat Report", Volume 20, (April 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[5] Maria Korolov, CSO, "Omaha's Scoular Co. loses $17 million after spearphishing attack", (February 13, 2015), http://www.csoonline.com/article/2884339/malware-cybercrime/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html

[6] Amber Corrin, Federal Times, "'Spear-phishing' tactics becoming more sophisticated", (October 24, 2014), http://archive.federaltimes.com/article/20141024/CYBER/310240013/-Spear-phishing-tactics-becoming-more-sophisticated

[7] Federal Bureau of Investigation, Internet Crime Complaint Center,"2014 Internet Crime Report", https://www.fbi.gov/news/news_blog/2014-ic3-annual-report

[8] Rob Waugh, welivesecurity, "Big Companies still fall for social engineering 'hacks' by phone – and it's not getting better", (October 31, 2013), http://www.welivesecurity.com/2013/10/31/big-companies-still-fall-for-social-engineering-hacks-by-phone-and-its-not-getting-better/

[9] RSA, 2013 A Year in Review, http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf, (January 2014)

[10] FireEye, "Spear Phishing Attacks – Why They are Successful and How to Stop Them: Combating the Attack of Choice for Cybercriminals", (2012)

[11] The Hartford, "2014 Midsize Business Monitor", (2015)

[12] Symantec Corporation, "Internet Security Threat Report", Volume 20, (April 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[13] Symantec Corporation, "Internet Security Threat Report", Volume 20, (April 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[14] Mark Davis, The Kansas City Star, "280 Kansas City employees fall for fake hack", (March 26, 2015), http://www.kansascity.com/news/business/technology/article16376894.html

[15] This document outlines in general terms the coverages that may be afforded under a policy from The Hartford. All policies must be examined carefully to determine suitability for your needs and to identify any exclusions, limitations or any other terms and conditions that may specifically affect coverage. In the event of a conflict, the terms and conditions of the policy prevail. All coverages described in this document may be offered by one or more of the property and casualty insurance company subsidiaries of The Hartford Financial Services Group, Inc. Coverage may not be available in all states or to all businesses. The Hartford is not responsible for the content of this report. The Hartford® is The Hartford Financial Services Group, Inc. and its subsidiaries, including Hartford Fire Insurance Company. Its headquarters is in Hartford, CT.