KnowBe4
Human error. Conquered.

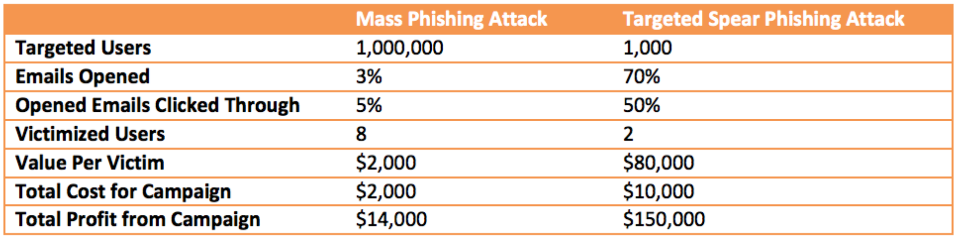
WHITEPAPER
The Ultimate Spear Phishing Defense

Strengthening the Weakest Link – the Ultimate Spear Phishing Defense

KnowBe4

whitepaper

Late in 2012 Trend Micro reported that 91% of targeted online attacks involved spear phishing, making this the most favored type of APT (Advanced Persistent Threat) attack. When spear phishing, attackers make use of information about prospective victims to increase their credibility, and the likelihood that recipients will "bite" (click a URL) in an e-mail or social media post. That's why spear phishing attacks yield a 70% open rate because people extend trust to the putative source, if not to the actual attacker. Because of the profitability and ease of spear phishing, its popularity will only continue to grow. Traditional methods don't stop spear phishing because individual employees and customers open the doors to attackers. In these circumstances, the employee/victim becomes the weak link in IT security.



	Mass Phishing Attack	Targeted Spear Phishing Attack
Targeted Users	1,000,000	1,000
Emails Opened	3%	70%
Opened Emails Clicked Through	5%	50%
Victimized Users	8	2
Value Per Victim	$2,000	$80,000
Total Cost for Campaign	$2,000	$10,000
Total Profit from Campaign	$14,000	$150,000

Source: Cisco White Paper, 'Email Attacks: This Time It's Personal'

Today's employees need next-generation security awareness training on a regular basis to keep them informed and your network protected.

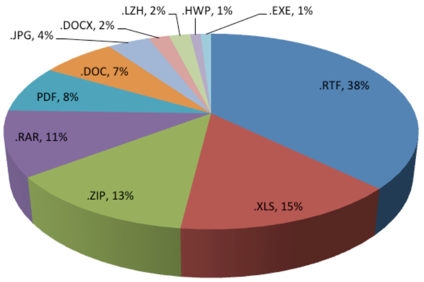
"A staggering 91 percent of targeted attacks begin with a spear phishing email"

Introduction

Spear phishing is a CSO's worst nightmare because it is the most difficult attack to protect against. The use of targeted social engineering, practically undetectable malware and zero-day exploits are just some of the reasons why this is so. Clever hackers use legitimate-looking emails from organizations like the IRS, local banks, or Internet portals, targeted directly at CEO's and other executives and employees.

One such incident occurred in 2012 when business executives received personalized emails informing them that their company was under investigation for criminal fraud. The email looked like a legitimate email from the IRS, and the link in that email directed the recipient to a website that looked exactly like an IRS webpage. But when the target clicked on a link, a Trojan was loaded into their computer which would steal everything interactive in the person's email account before it could be securely encrypted. The result of such attacks is that customers are 42% less likely to do business with a company that has fallen victim to spear phishing and a resulting data breach. Even worse, phishing costs brands and corporations more than 98 billion dollars a year.

A Sorry Security Situation

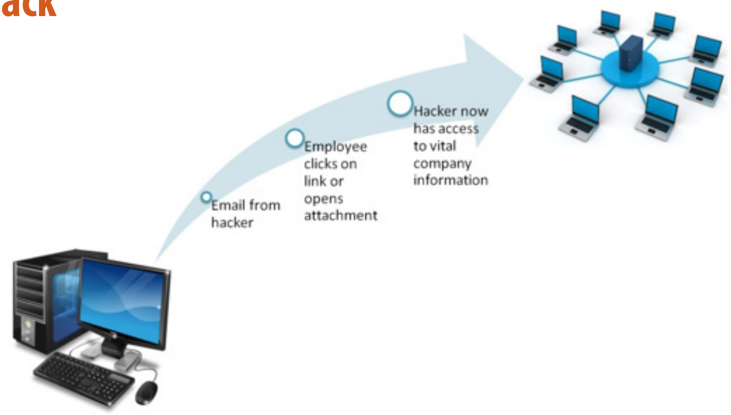


Top Spear Phishing Email Attachment Types

CSOs are responsible for a company's entire security. As such they oversee network security and are the first person everyone turns to whenever there is a breach. People expect CSOs to protect the company and prevent such breaches, but spear phishing makes even a CSO more likely to be blindsided. Once a breach occurs it is up to CSOs to act quickly and protect the company before any damage is done. Hackers count on this and act quickly to get every ounce of information they can before a breach is closed. Those who don't understand how spear phishing works may blame the CSO or the security software in use. However, even the best CSO and best security software on the planet can't stop an intelligent and motivated hacker.

If CSOs are to do their jobs well, then not only must they have the best security hardware and software, they also need the support of well-educated staff, and the ability to test their staff to find any weak links in need of strengthening. With all possible 'defense-in-depth' components properly in place, an organization becomes a very hard target, causing hackers to move on to pursue easier game.

The Attack


Email from hacker
Employee clicks on link or opens attachment
Hacker now has access to vital company information

E-mail leads to a click, then to a drive-by download, and on to data theft.

The Missing Link

Several missing components can prevent employees from unwittingly opening the door to hackers:

- How do you make sure your employees are getting the best education?
- How do you make sure after your employees are educated that they don't make security mistakes anyway?
- If you could find out if they might be vulnerable to spear phishing, how can you enlighten them?

If existing methods for educating employees were effective, then spear phishing wouldn't remain problematic for so many companies. Thus, it is obvious that a different approach is called for. Hackers aren't just looking to get at a company's financial records and information. They are also after source code and intellectual property. In fact, they are literally trying to steal the future of your company. Years of work in your R & D department could end up in the hands of a Chinese competitor thanks to a single click of a mouse from an untrained employee.

UNCLASSIFIED//FOUO
DoD Spear-Phishing Awareness Training
JOINT TASK FORCE
GLOBAL NETWORK OPERATIONS
Joint Task Force - Global Network Operations
IV 2006
UNCLASSIFIED//FOUO

Spearphishing has become so endemic in corporate and government networks that there is a joint government operation in effect to counteract it. Per the FBI: "Instead of casting out thousands of e-mails randomly hoping a few victims will bite, spear phishers target select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, [or] order merchandise from the same website.

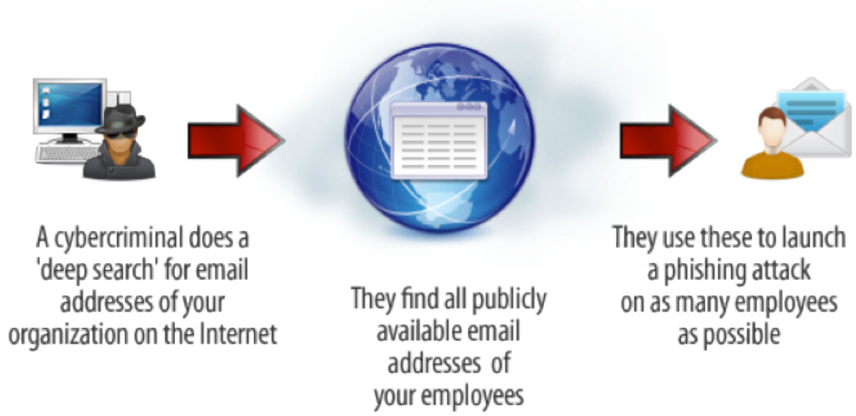
The e-mails are ostensibly sent from organizations or individuals the potential victims would normally get e-mails from, making them even more deceptive. . .
Law enforcement takes this kind of crime seriously, and we in the FBI work cyber investigations with our partners, including the U.S. Secret Service and investigative agencies within the Department of Defense."

MOUNTAIN VIEW, CA -- (MARKETWIRE) -- 01/31/13 -- As a follow-up to a story run by the New York Times on Wednesday, Jan. 30, 2013 announcing they had been the target of a cyber attack, Symantec issued the following statement:

"Advanced attacks like the ones the New York Times described in the article underscore how important it is for companies, countries and consumers to make sure they are using the full capability of security solutions. . .' 'We encourage customers to be very aggressive in deploying solutions that offer a combined approach to security. Anti-virus software alone is not enough."

During a recent Microsoft TechEd conference, held in June 2012, Proofpoint surveyed 339 IT professionals about their concerns regarding targeted phishing attacks and enterprise data loss risks. Half of all respondents (51%) believed that their organization were targeted by a phishing email in the past year designed specifically to compromise their users.

How The Bad Guys Attack



A cybercriminal does a 'deep search' for email addresses of your organization on the Internet

They find all publicly available email addresses of your employees

They use these to launch a phishing attack on as many employees as possible

Dramatic examples of recent spear phishing attacks include:

The White House - China-based hackers breached a network used by the White House Military Office. According to their website, this office provides military support for White House functions, including food service, presidential transportation, medical support and hospitality services. There is no clear report on what the hackers were trying to access. An Obama administration national security official simply said: "This was a spearphishing attack against an unclassified network."

Google, Inc. – A US official says that the same group that attacked the White House also broke into Google. Among those targeted were people who work at the White House. It is presumed that they were hoping these people would discuss secure information or conduct administrative business using their personal Gmail accounts.

South Carolina Department of Revenue – According to an official report, "A malicious email was sent to multiple Department of Revenue employees. At least one Department of Revenue user clicked on the embedded link, unwittingly executed malware, and became compromised. The malware likely stole the user's username and password." These attackers then gained access to "millions of Social Security numbers, bank account information and thousands of credit and debit card numbers" SearchSecurity's coverage notes that, "In addition to the 3.8 million people whose data were exposed, the breach included information on 1.9 million dependents. It also included data on 699,900 businesses. Information on 3.3 million bank accounts were also stolen."

The New York Times – The same China-based hackers who have wreaked havoc on the White House, Google, and others have been named as the responsible parties for this breach, too. In this particular case, the newspaper blames Symantec's antivirus software for not foiling a malware installation.

Attacks against Google, Adobe and at least a dozen other advanced persistent threats (APT) that have been publicly documented have been initiated at least in part through targeted spear phishing emails. By itself, software alone is not a completely effective defense.

SC Magazine reports:
"Researchers have noted an increase in spear phishing targeting numerous industries, primarily in the United States, where malware evades detection by hiding inside Windows help (HLP) files attached to emails. The HLP files are embedded in attachments that appear to users to be ZIP files. Once the files are opened, however, one of several backdoors will be downloaded, allowing an attacker to carry out a range of feats – from changing users' passwords to logging keystrokes to capturing screenshots or a number of other information-stealing tactics sent from the command-and-control server."

Strengthening the Weakest Link

There is an important conclusion to be drawn from all this recent news. Security products continue to become more advanced and sophisticated, and that will certainly help. But to cope with the current situation and future attacks, end-users must be educated and informed. The more knowledge they possess, and the better informed those users are about attacks, the less likely they are to fall prey to scammers, online or off.

We are also starting to see an increase of social engineering over the phone. Hapless users are being called on behalf of 'Microsoft' or well-known security software companies and directed to allow access to their computers. Educated end-users do not fall prey to such scams.
But how do you train jaded users? Users who think they know everything. Users who have heard it all and are more sophisticated than average users. It's not good enough that the trainer is a highly regarded security expert. You need that training to come from someone who understands hacker culture and how hackers think.

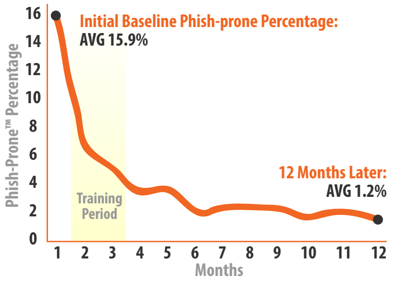
The key here is to employ a trainer who is so knowledgeable about hacking that he can predict their behavior. What better person to do this than a reformed hacker who was at one time the most wanted computer criminal in the United States? That man is Kevin Mitnick. He renounced hacking completely. In fact, since 2000 Mitnick has become a leading expert on computer security. Kevin is an authority in hacking and security, so he is not just any security expert because he has on played both sides. Thankfully, he has put his past behind him which is to your benefit. Kevin has teamed up with KnowBe4 to help develop the ultimate computer security educational program – Kevin Mitnick Security Awareness Training for you and your employees.

Security Awareness Training

Traditional once-a-year Security Awareness Training doesn't hack it anymore. Today, your employees are exposed to advanced phishing attacks weekly, if not daily. Your users are now the weak link in your network security. They need to be trained by an expert like Kevin Mitnick, and after that training to stay on their toes, by keeping security uppermost in their minds.

This is a brand-new, high quality 30-40 minute web-based interactive training. It uses case-studies, live demonstration videos, and short tests to entertain and inform its audiences. The Kevin Mitnick Security Awareness Training specializes in making sure employees understand the mechanisms of spam, phishing, spear-phishing, malware and social engineering, and are able to apply this knowledge in their day-to-day jobs. The secret is to tie the training directly to actual practical applications at work. This is not just a tap-dance orchestrated to PowerPoint slides over a yearly lunch. After this class, there's no going back to the work cheerfully oblivious to clear and present security threats. This course will wake up the audience, and teach them how to put what they learn to work the instant they return to their desks.

Our hard-hitting approach makes a huge difference in the effectiveness of this training. Each case study ends with its own short multiple choice test, there is a quiz at the end of the course, and trainees get a unique job-aid: Social Engineering Red Flags™ with 22 things to watch out for. After the training is done, KnowBe4's highly effective scheduled Phishing Security Tests will keep your employees on their toes. From your Admin Console you can schedule regular Phishing Security Tests (PST for short) using any of dozens of our templates. If an employee falls for a simulated phishing attacks, you can apply several options for correcting their lapses, including instant remedial online training. You can schedule one-shot, weekly, bi-weekly or monthly simulated phishing attacks and immediately see which employees fall for any of these social engineering tricks.



Visible proof the training works, dramatic drop in Phish-prone percentage.

Based on Kevin's 30+ year first-hand hacking experience, you will get next-generation web-based training and testing, to address the needs of C-level Executives, IT, HR, and employees. KnowBe4 is the market leading on-demand Internet Security Awareness Training (ISAT) provider and enables you to quickly address the urgent security problem of social engineering. With world-class, user-friendly and effective Internet Security Awareness Training, KnowBe4 gives you self-service enrollment, and both pre-and post-training phishing security tests to show you what percentage of end-users are Phish-prone. KnowBe4's unique scheduled Phishing Security Test keeps employees on their toes, and provides instant remedial online training whenever an employee falls for a simulated phishing attack.

The Internet Security Awareness Training project leader at every KnowBe4 customer gets access to user provisioning, and comprehensive training reporting. Every end-user gets an engaging and effective 30-40 minute training course. After being trained, attendees may receive ongoing testing. Executives get the insight they need to maximize training ROI and track security compliance (the Admin Console provides instant graphs of training effectiveness).

The most well trained CSO combined with the most effective security software won't stop a hacker when your employee opens the door to attack. The missing component to complete security for your company is an effective training solution that ensures your employees don't become your weakest link. Your solution is KnowBe4: Human error. Conquered.

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created by two of the best known names in cybersecurity, Kevin Mitnick (the World's Most Famous Hacker) and Inc. 500 alum serial security entrepreneur Stu Sjouwerman, to help organizations manage the problem of social engineering tactics through new school security awareness training.

More than 1,700 organizations use KnowBe4's platform to keep employees on their toes with security top of mind. KnowBe4 is used across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance.

- KnowBe4 wrote the book on cyber security (8 books and counting between Mitnick and Sjouwerman).

- KnowBe4 is the only set-it-and-forget-it security awareness training platform "by admins for admins" with minimum time spent by IT to get and keep it up and running.

- The platform includes a large library of known-to-work phishing templates.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com