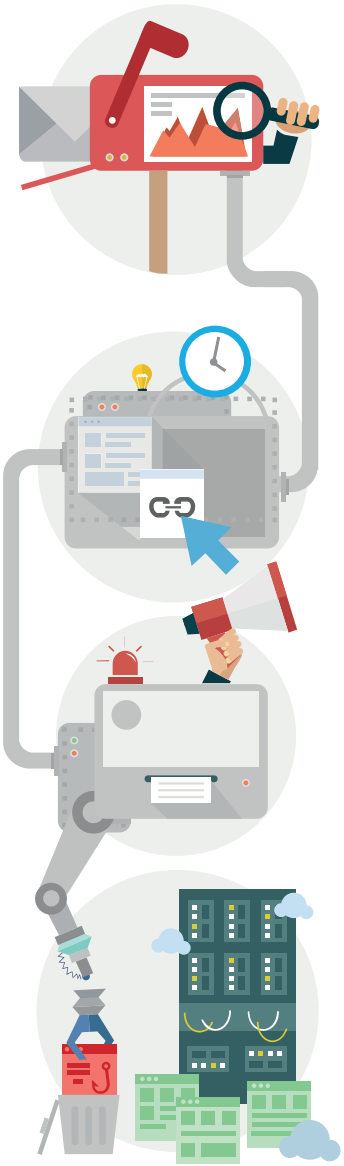
Vade Secure
Advanced Email Protection

Phishing & Spear Phishing

Understanding an Emerging Threat to Healthcare Organizations

Table of Contents



Executive Summary

Phishing, the email-borne hacking technique that lures message recipients into disclosing confidential information, poses a serious security threat for healthcare organizations that are regulated by HIPAA. Spear phishing, where the hacker impersonates someone the target knows or references specific projects or mutual social connections, is even more dangerous. Spear phishing is extremely effective at penetrating large, otherwise well-secured enterprises. This brief looks at unique phishing risks faced by healthcare organizations and suggests some approaches to mitigating them.

Overview

Healthcare organizations are uniquely vulnerable to security threats. Working under tight regulatory strictures, healthcare entities can suffer from significant financial penalties in the event of a data breach. The reputational impact can also be serious. Health providers are entrusted with sensitive personal information, so breaches of data are perceived as breaches of trust, which can cause extensive damage to the healthcare organization's brand.

Healthcare organizations have responded by implementing rigorous risk mitigation strategies. As threats evolve, however, healthcare security managers must continuously revamp their policies and toolsets to stay ahead. In particular, phishing and its more potent variant, spear phishing, present a new type of security challenge. Phishing uses deceptive emails and fake web URLs to trick employees into disclosing login credentials or downloading malware. Spear phishing targets specific individuals by impersonating friends and coworkers.

Phishing and spear phishing create outsized security problems because traditional security measures won't stop them. Anti-spam filters are ineffective at preventing employees from getting these malicious emails. Anti-virus solutions aren't triggered when employees respond to the messages. Web-filtering tools are helpless to prevent either employees disclosing credentials or prevent drive-by infections from one-off websites. **An estimated ninety-one percent of hacking attacks**[1] include a phishing attack This is partly because many spear phishing email messages do not even contain the basic elements that are typically perceived as a potential threat, such as links, attachments or any other spam-like element.

Email and the employees who receive it are the vulnerable underbelly of your IT security.

1 http://www.wired.com/2015/04/hacker-lexicon-spear-phishing/

How Phishing and Spear Phishing Work

Phishing is a hacking technique that "fishes" for victims by sending them deceptive emails. (The "ph" replaced the "f" in homage to the first hackers, the "phone phreaks" of the 1960s and '70s.) Virtually everyone on the Internet has seen a phishing attack. In their crudest form, they are mass emails that request personal information under fairly obvious false pretenses or purport to offer the recipient prizes in exchange for entering personal information at suspicious-looking websites.

A surprisingly high **23% of recipients open** phishing messages, and **11% click on links** in phishing emails, according to security industry research.[2] It seems that even savvy – but busy – people can fall for convincingly faked websites, such as the form for Discover cards that was spoofed in figure 1. When the email recipient clicks on a link in an email and sees a site that looks identical to the legitimate site, he or she could easily be duped into disclosing personal information to the hacker. If you were in a hurry, would you notice the only tip-off…the slight difference between the URLs?

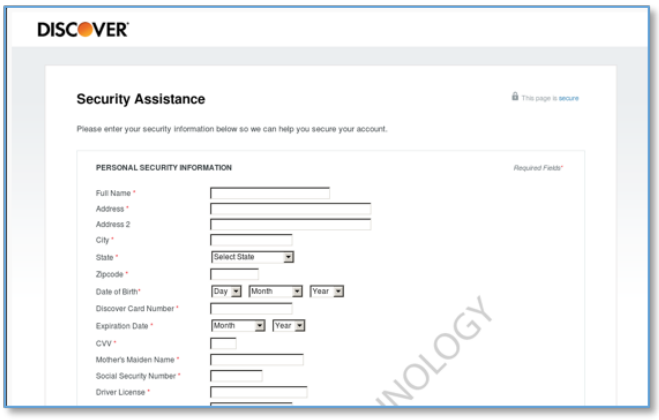


Figure 1 – Fake web sites can be startlingly realistic.

Spear phishing is an enhanced version of phishing that takes aim at specific employees of a targeted organization. The goal is usually to gain unauthorized access to networks, data and applications. In contrast to the rapid, mass email approach of phishing, which might see hundreds of thousands of attack messages go out within the space of a few hours, spear phishing is methodical, deliberate and narrowly focused.

To show how the spear phishing process works, let's explore an attack on a hypothetical hospital chain called Health Systems, which has 10,000 employees spread out over five campuses in different cities. The company employs more than 500 doctors. Hackers are interested in getting access to Health Systems' database of hundreds of thousands of electronic health records (EHRs). They can harvest the patients' personally identifying information (PII) and Social Security numbers and sell them on the black market to identity thieves. While they are at it, they will look for embarrassing information in the personal health information (PHI) of well-known patients in the Health Systems system.

2 Verizon 2015 Data Breaches Report

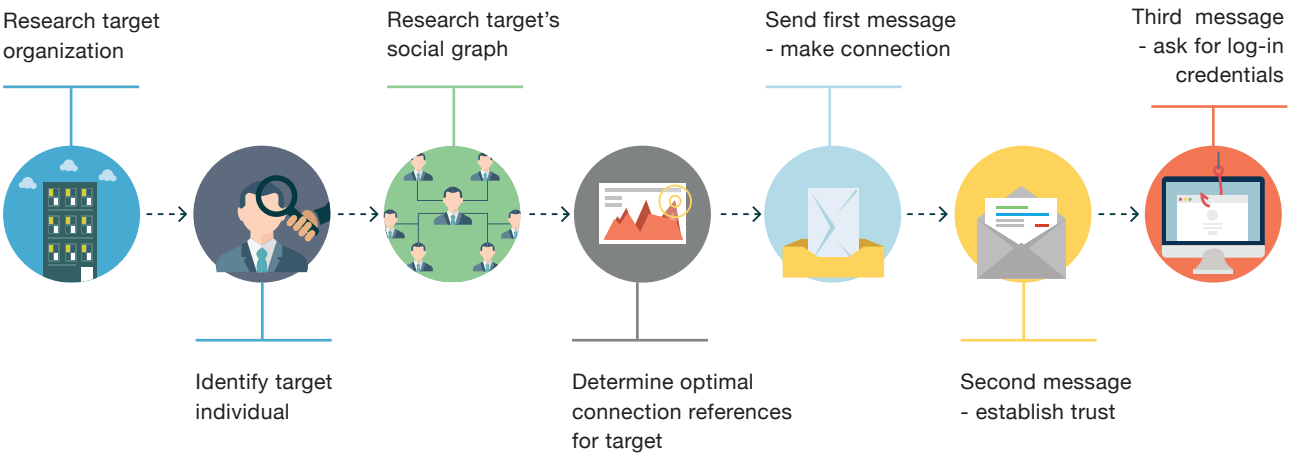


Figure 2 - The progression of a spear phishing attack, starting with research of the target organization and identification of a specific individual inside the organization, followed by a series of emails intended to build trust with the target

Figure 2 shows the progression of a spear phishing attack. The attacker's first step is to research Health Systems to get a sense of how they can best mount a successful spear phishing attack. After cataloguing the doctors in the "About Our Practitioners" section of the Health Systems website, the attackers create a cross-reference of social graphs, using fake Facebook and LinkedIn accounts to build lists of who knows whom inside Health Systems. Then, by crawling through sites like Yelp and HealthGrades.com, the attackers are able to assemble a list of patients who have seen specific doctors at Health Systems. With all of this information, the attackers are ready to go spear phishing.

The attackers find a radiologist at Health Systems named John Smith. Posing as Dr. Smith, the hackers target Smith's Facebook friend and colleague, Dr. Jeff Jones, a family practitioner at Health Systems. To build trust in the faked email address, the hacker posing as Dr. Smith sends his "friend," Dr. Jones, a note asking if he's planning on attending an upcoming medical conference. If Dr. Jones responds, the hacker is off to a good start. He's successfully impersonating another Health Systems doctor and starting to build trust with his target. Dr. Jones replies and says he is going to the conference. The two agree to share travel information about the conference.

How can the attacker get away with this? Doesn't Dr. Smith have a unique, domain-specific email through Health Systems? Yes, he does. However, due to Health Systems' "Bring Your Own Device" (BYOD) policy, doctors are able to use personal mobile devices to send messages to one another as long as the message doesn't contain any actual personally identifiable health information (PHI) about a patient. In this case, the attacker knows from LinkedIn that Dr. Smith's personal email address is johnsmithmd1@gmail.com. The attacker creates a gmail account for johnsmithmd.1@gmail.com. Dr. Jones doesn't notice the difference, and the stage is set for the real attack.

The hackers know from Yelp that Jane Doe is a patient of Dr. Jones. The hacker posing as Dr. Smith sends to Dr. Jones an image file of an "X-ray I want you to look at" that actually contains key logging malware. If Dr. Jones opens the file, his device is instantly infected and the network is breached.

Alternatively, the fake Dr. Smith could send a note that says, "Hey, Jeff – I'm on the golf course, but I need to call an insurance company about Jane Doe's X-ray. I can't remember the log-in for the EHR system – can you help me out?" If Dr. Jones shares his log-in for the EHR system, the hacker is inside. Either way, the phisher can collect Dr. Smith's login credentials – a free pass to invade the hospital's private networks. Any PHI and other HIPAA-regulated data is at risk of being improperly accessed.

Phishing Has Already Infected Healthcare Employees

Phishing and spear phishing are not theoretical threats for healthcare organizations. Sixty-four percent of respondents to the 2015 Healthcare Information and Management Systems Society Survey indicated that they had experienced a security incident caused by an external actor such as an online scam or social engineering. Employees of the Massachusetts-based Partners HealthCare System fell prey to a phishing attack in late 2014 that led to 3,300 patient records being compromised.[3] Information compromised included names, addresses, dates of birth, telephone numbers and, in some cases, Social Security numbers.

Around the same time, the Seton Family of Hospitals reported that a phishing attack had potentially compromised the private information of 39,000 patients. Other examples of phishing in healthcare include an attack on the St. Vincent Medical Group, which affected 760 patient records, and the potential exposure of 8,300 patient records in Washington's Franciscan Health System. In the Franciscan case, about 20 Franciscan Health employees had responded to emails they thought had been sent by Franciscan's parent company, Catholic Health Initiatives.[4] The company reported that recipients of the attack emails had been directed to a third-party website that asked employees for their user names and passwords, giving the attackers access to patient data. At the University of Vermont Medical Center, CISO Heather Roszkowski told Information Security Media Group in 2015 that the Center had experienced a six-month spike in phishing attempts, including those "laced with malware in an attempt to steal credentials." [5]

3 Snell, Elizabeth – "Why Healthcare Phishing Scams Are a Key Issue" – HealthItSecurity.com – October, 2015

4 Snell, Elizabeth – "Why Healthcare Phishing Scams Are a Key Issue" – HealthItSecurity.com – October, 2015

5 Kolbasuk, McGee Marianne – "Phishing Leads to Healthcare Breach: Experts Say More Employees Are Being Targeted" HealthInfoSec – April 23, 2015

Organizational Factors That Increase Phishing Exposure in Healthcare

Every industry is vulnerable to phishing attacks, but the healthcare industry has distinctive factors that create a high level of exposure to the threat. For instance, the very large, distributed nature of many healthcare organizations can mask hackers who are impersonating individuals who work in an extended system. If you work for a healthcare provider with 20 hospitals, who's to say that there isn't someone named, say, "Dr. Joel Schwartz" at another facility when he reaches out to you by email? **Are you going to check the staff directory every time you get an email?**

Healthcare also involves many interdependent but administratively separate entities working together. Health insurance companies, lab services, pharmacies and so forth all must share patient information in order to conduct business. The human connections between these entities also provides rich cover for phishing attackers.

The hierarchical nature of most healthcare organizations can also contribute to spear phishing risk. Though the "ranks" of various people may not be official, there is usually a very clear order of importance and authority for doctors, nurses, maintenance people and so forth in a medical organization. Orders often flow from the top down, with little questioning tolerated. This kind of operating environment enables hackers to pose as senior staff members and get access to information with less friction than would occur amongst equals. When combined with some of the unique hardware strictures in healthcare IT, the potential for spear phishing becomes all the more significant.

Healthcare organizations frequently provision specialized hardware for departmental workloads. An OB-GYN delivery room, for example, might contain a dedicated terminal that contains a department-specific EHR application. This, combined with the urgency of some medical issues, means that if a hacker posing as a doctor sends a huffy email to an underling complaining that he cannot log onto the terminal and asking the underling to please give him the log-in credentials he may well get those credentials unchallenged. With those credentials and network access, the hacker can then probe the system as an insider.

Consequences of Phishing in Healthcare

The business impacts from a phishing attack can be sizeable in any industry, but in healthcare, their effects are amplified by regulatory penalties. A data breach, a typical result of phishing, can result in loss of reputation, high costs to remediate and loss of intellectual property. Healthcare records are prized by identity thieves because they contain valuable personal data such as Social Security numbers, physical addresses, phone numbers, birth dates and credit card data. Costs to contain a breach include legal liability, identity theft victim compensation, identity protection services and outright financial theft from the healthcare organization itself. In addition, healthcare organizations face civil fines mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA **violation penalties range from $100 to $50,000 per patient record**. The table below, published by the law firm of McGuire Woods, shows that civil money penalties (CMPs) from HIPAA depend on the type of violation and level of culpability.[6] There is a difference between an unknowing violation, whose penalty can be as low as $100 per violation, and one with "reasonable cause," "willful neglect – corrected" and "willful neglect – not corrected," which range from $1,000 to $50,000 minimum penalties, respectively. Penalties are capped at **$1.5 million** per identical violation and **$10 million** for a single set of incidents.

Violation Category	Each Violation	Total CMP for Violations of an Identical Provision in a Calendar Year
Unknowing	$100 – $50,000	$1,500,000
Reasonable Cause	$1,000 – $50,000	$1,500,000
Willful Neglect – Corrected	$10,000 – $50,000	$1,500,000
Willful Neglect – Not Corrected	At least $50,000	$1,500,000

6 https://www.mcguirewoods.com/Client-Resources/Alerts/2013/2/HIPAA-Omnibus-Final-Rule-Implements-Tiered-Penalty-Structure-HIPAA-Violations.aspx

Average security breach costs for a healthcare organization were $363 per patient record in 2014, according to the Ponemone Institute's 2015 Cost of Data Breach Study: Global Analysis. **This is the highest per capita cost for a security incident of any industry**. As an example of how costly this can get, New York-Presbyterian Hospital and Columbia University Medical Center paid $4.8 million in settlement of alleged HIPAA violations from the leak of 6,800 patients' information. According to a study by the Ponemone Institute, the average HIPAA fine cost $2 million in 2014.[7] The average overall cost for a security incident among the 350 corporations surveyed by Ponemone was **$3.79 million**.

One important question that arises is "What is willful neglect?" Willful neglect is defined as deliberately not adhering to the defined HIPAA security standards.[8] Health and Human Services (HHS) has some leeway in determining fines and is increasingly looking at the overall holistic security measures put in place to prevent a breach. This can result in fines for operations that are technically in compliance for each individual component of their IT security, but which still leave security holes that can be exploited. Taking active anti-phishing steps can significantly decrease both overall risk of being breached and of HIPAA fines.

7 http://www.healthcareitnews.com/news/group-slapped-record-hipaa-fine

8 http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php

Mitigating the Phishing Threat

It should not be a surprise that 96% of users want better protection against phishing attacks, according to Gartner.[9] The key word here is "better." Many controls and countermeasures are already in place. There is huge room for improvement, though, as evidence of increasingly high-impact attacks mounts.

HIPAA-Compliant Email Is Not Enough

Generally speaking, "HIPAA-compliant email" means that the email has been encrypted so that it is not easily intercepted and exploited when in transit. However, the act of encryption does not offer protection for employees who use outside email. Standard anti-spam and HIPAA email compliance vendors such as Google and Microsoft will not prevent all phishing and spear phishing email from getting through to employees.

Consider the Anthem breach, which exposed 80,000,000 patient records to hackers[10] – the worst healthcare data breach to date. According to the law firm of Nelson Hardiman, which specializes in healthcare compliance and researched the Anthem case, Anthem experienced a sophisticated external cyberattack "where hackers stole log-in keys and passwords from more than one administrator, most likely with a phishing campaign that used malware attachments or took advantage of a browser exploit." [11] Anthem was HIPAA compliant, but the breach will still allegedly cost Anthem more than $100,000,000 to remediate.[12] Health Technology Management commented on the breach, saying, "Being HIPAA compliant will not shield Anthem from negative fallout, as it's a healthcare entity that leaked enough personally identifiable information to commit a large amount of medical identity fraud and other crimes." [13]

How does this happen? The issue has to do with email messages that evade anti-spam filters because they aren't "spammy." They might not contain any malware or suspicious links at all. They may simply be establishing a trust relationship with the recipient. Or the messages feature URLs that appear harmless when being examined by standard email filtering software. After passing the filter, the phishing email waits in the recipients' in-box. Within a short time, perhaps an hour, the hacker will redirect that link to a malicious site. When the recipient opens the email, the link it contains becomes toxic and leads, for example, to a phishing site that is stealing user credentials.

9 Gartner - Magic Quadrant for Secure Email Gateways – June 2015

10 http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/

11 http://www.nelsonhardiman.com/hipaa-security-breaches-raise-bar-for-hipaa-compliance/

12 http://www.zdnet.com/article/anthem-data-breach-cost-likely-to-smash-100-million-barrier/

13 http://www.healthmgttech.com/beyond-compliance-hipaa-after-anthem.php

Web-filtering software is not typically able to block these URLs because phishing sites are generally not online long enough to get blacklisted. Anti-virus systems won't help, as there is often no virus involved. The site is brand new, so it also would not appear on any blacklists and therefore would not trigger standard web filters. Standard security measures are helpless in this case. A specific anti-phishing solution is needed.

Vade Secure's Anti-Phishing/Spear Phishing Solution

Vade Secure's anti-phishing solution is focused on the specific problem of phishing, including specific Content Filtering. Features such as looking at credential requests and Identity Match™ that are tailored to fighting spear-phishing attacks.

Content email filtering. This artificial intelligence has been trained by monitoring hundreds of millions of email boxes for 10 years looking for phishing threats. It heuristically evaluates email content, requests for credentials, phone numbers, DNS reputation, any linked website content and much more. Unlike other pattern-recognition technologies, our filter looks at the characteristic of each email and is therefore much more reliable for low-volume email scams and spear phishing attempts. It can catch the first phishing email that comes into your organization… even if there is only one.

Attachment management. All attachments are thoroughly investigated in a remote sandboxed environment to eliminate possible malware. The attachments are analyzed, taking into account the environment where they originate. Vade Secure's unique attachment analysis algorithm examines the proprieties of both emails and attachments. This gives Vade Secure the ability to predict the advent of a "0-day" attack from previously unknown vectors. It is also possible to add the Dr. Web anti-virus add-on.

Webpage exploration at the Time-of-Click. Every URL that is included in any email is safely explored in a remote sandboxed environment to see if it contains any form requesting personal information, any malware, honeypots or any other malicious code. What makes our solution unique and superior to other tools is that this exploration is done at the time an employee clicks on it. Competing solutions examine URLs at the time the email is received by the network. This is important because sophisticated hackers will now send emails that include URLs that initially lead to innocent websites, then wait to redirect those URLs an hour or two later, thus bypassing most filtering systems unless the site is examined at the time of click.

Identity Match™ advanced spoofing detection. This patented set of spoofing protections identifies every incoming email that attempts to spoof trusted company domain names, display names and even similar but different email addresses that are close to real ones. Identity Match looks at both technical and style indicators of every email and compares them to previous communication habits. The solution identifies similarities between new senders and all your previous contacts in order to identify if there is a spoofing attempt targeting your company. This unique feature helps to identify and isolate even highly sophisticated one-off spear-phishing attempts.

Education and remediation. Vade Secure provides educational banners to users who receive phishing emails informing them of the threat posed and how they can avoid it. These impossible to ignore integrated banners alert users to the possibility of a phishing attempt right in the message itself. We also alert administrators if users have ignored phishing warnings on either email links or URLs and have thereby potentially created a breach of security.

Vade Secure is available as a plugin that can layered on top of existing anti-spam solutions or as part of a global email filtering solution located either in the cloud or an on-site virtual appliance.

Give us a call at 415-745-3630 if you want to discuss how you can quickly add anti-phishing measures to your current email setup.

About Vade Secure

Vade Secure is the global leader in anti-phishing software, offering a full set of security features against phishing, malware and spam. The company is entrusted to protect hundreds of millions mailboxes worldwide. This breadth of deployment has given Vade Secure unique insights into the nature of malicious emails. The resulting proprietary knowledge enables Vade Secure to provide comprehensive solutions against all email threats, ensuring a zero-day protection even on small waves of email. Vade Secure is also a leader in more general email filtering providing a comprehensive set of productivity-enhancing tools to manage commercial emails known as grey-mail. The company's solutions are tailored for ISPs, OEMs, hosting companies and the enterprise.