Introduction:

General idea of phishing:

Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.

Early phishing attempts were crude, with telltale misspellings and poor grammar. Since then, however, phishing e-mails have become remarkably sophisticated. Phishers may pull language straight from official company correspondence and take pains to avoid typos. The fake sites may be near-replicas of the sites phishers are spoofing, containing the company's logo and other images and fake status bars that give the site the appearance of security. Phishers may register plausible-looking domains like aolaccountupdate.com, mycitibank.net or paypa1.com (using the number 1 instead of the letter L). They may even direct their victims to a well-known company's actual website and then collect their personal data through a faux pop-up window.

Spear phisihing

Phishing refers to malicious emails that are designed to trick the recipient into clicking on a malicious attachment or visiting a malicious web site. Spear-phishing is a more targeted form of phishing that appears to come from a trusted acquaintance.

Spear-phishing is a more targeted form of phishing. Whereas ordinary phishing involves malicious emails sent to any random email account, spear-phishing emails are designed to appear to come from someone the recipient knows and trusts—such as a colleague, business manager or human resources department—and can include a subject line or content that is specifically tailored to the victim's known interests or industry. For really valuable victims, attackers may study their Facebook, LinkedIn and other social networking accounts to gain intelligence about a victim and choose the names of trusted people in their circle to impersonate or a topic of interest to lure the victim and gain their trust.

typical attack

Email from a "Friend"

The spear phisher thrives on familiarity. He knows your name, your email address, and at least a little about you. The salutation on the email message is likely to be personalized: "Hi Bob" instead of "Dear Sir." The email may make reference to a "mutual friend." Or to a recent online purchase you've made. Because the email seems to come from someone you know, you may be less vigilant and give them the information they ask for. And when it's a company you know asking for urgent action, you may be tempted to act before thinking.

Famous attack

One of the most famous examples of a spear-phishing attack that succeeded despite its suspicious nature targeted the RSA Security firm in 2011.

The attackers sent two different targeted phishing emails to four workers at RSA’s parent company EMC. The emails contained a malicious attachment with the file name “2011 Recruitment plan.xls,” which contained a zero-day exploit.

When one of the four recipients clicked on the attachment, the exploit attacked a vulnerability in Adobe Flash to install a backdoor onto the victim’s computer.

“The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached excel file,” RSA wrote in a blog post about the attack.

The backdoor gave the attackers a foothold from which to conduct reconnaissance and map a way to more valuable systems on the company’s network. They eventually succeeded in stealing information related to the company’s SecurID two-factor authentication products. The attack was surprising because everyone assumed that a top security firm like RSA would have trained employees who know better than to open suspicious emails. Yet one of its employees not only opened one of the suspicious emails but retrieved it from his junk folder—after his email filter had deemed it suspicious—in order to open it.

Another surprising victim of a spear-phishing attack was the Oak Ridge National Laboratory in Tennessee. The lab, also hacked in 2011, got hit with a phishing email that appeared to come from the human resources department and included a link to a web page where malware downloaded to victims’ machines. The attackers sent the email to 530 of the lab’s 5,000 workers, and fifty seven people clicked on the malicious link in the email. Only two machines got infected with the malware, but this was enough to get the attackers onto the network. They were discovered only after administrators noticed megabytes of data being siphoned from the lab’s network.

The hack was so surprising because the high-security federal lab conducts classified energy and national security work for the government, including work on nuclear nonproliferation and isotope production. But the lab, ironically, also does cybersecurity research—work that focuses on, among other things, researching phishing attacks.

Vulnerabilities

Using Your Web Presence Against You

How do you become a target of a spear phisher? From the information you put on the Internet from your PC or smartphone. For example, they might scan social networking sites, find your page, your email address, your friends list, and a recent post by you telling friends about the cool new camera you bought at an online retail site. Using that information, a spear phisher could pose as a friend, send you an email, and ask you for a password to your photo page. If you respond with the password, they'll try that password and variations to try to access your account on that online retail site you mentioned. If they find the right one, they'll use it to run up a nice tab for you. Or the spear phisher might use the same information to pose as somebody from the online retailer and ask you to reset your password, or re-verify your credit card number. If you do, he'll do you financial harm.

Keep Your Secrets Secret

How safe you and your information remain depends in part on you being careful. Take a look at your online presence. How much information is out there about you that could be pieced together to scam you? Your name? Email address? Friends' names? Their email addresses? Are you on, for example, any of the popular social networking sites? Take a look at your posts. Anything there you don't want a scammer to know? Or have you posted something on a friend's page that might reveal too much?

Countermeasures

Traditional security often doesn't stop these attacks because they are so cleverly customized. As a result, they're becoming more difficult to detect. One employee mistake can have serious consequences for businesses, governments and even nonprofit organizations. With stolen data, fraudsters can reveal commercially sensitive information, manipulate stock prices or commit various acts of espionage. In addition, spear phishing attacks can deploy malware to hijack computers, organizing them into enormous networks called botnets that can be used for denial of service attacks.

To fight spear phishing scams, employees need to be aware of the threats, such as the possibility of bogus emails landing in their inbox. Besides education, technology that focuses on email security is necessary.

How to Protect Yourself

Traditional security often doesn't stop these attacks because they are so cleverly customized. As a result, they're becoming more difficult to detect. One employee mistake can have serious consequences for businesses, governments and even nonprofit organizations. With stolen data, fraudsters can reveal commercially sensitive information, manipulate stock prices or commit various acts of espionage. In addition, spear phishing attacks can deploy malware to hijack computers, organizing them into enormous networks called botnets that can be used for denial of service attacks.

To fight spear phishing scams, employees need to be aware of the threats, such as the possibility of bogus emails landing in their inbox. Besides education, technology that focuses on email security is necessary.

Be suspicious of any email with urgent requests for personal financial information Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately. They typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc. Phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are. Don't use the links in an email to get to any web page, if you suspect the message might not be authentic. Instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser. Avoid filling out forms in email messages that ask for personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone. Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser. to make sure you're on a secure Web server, check the beginning of the Web address in your browser's address bar - it should be "https://" rather than just "http://". Regularly log into your online accounts. don't leave it for as long as a month before you check each account Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate If anything is suspicious, contact your bank and all card issuers. Ensure that your browser is up to date and security patches have been applied.

Patches, Updates, and Security Software

When you get notices from software vendors to update your software, do it. Most operating system and browser updates include security patches. Your name and email address may be all it takes for a hacker to slip through a security hole into your system. And it almost goes without saying, you should be protected by Internet security software, and it should always be up to date.

Can we prevent phishing attacks?

Companies can reduce the odds of being targeted, and they can reduce the damage that phishers can do (more details on how below). But they can't really prevent it. One reason phishing e-mails are so convincing is that most of them have forged "from" lines, so that the message looks like it's from the spoofed company. There's no way for an organization to keep someone from spoofing a "from" line and making it seem as if an e-mail came from the organization.

A technology known as sender authentication does hold some promise for limiting phishing attacks, though. The idea is that if e-mail gateways could verify that messages purporting to be from, say, Citibank did in fact originate from a legitimate Citibank server, messages from spoofed addresses could be automatically tagged as fraudulent and thus weeded out. (Before delivering a message, an ISP would compare the IP address of the server sending the message to a list of valid addresses for the sending domain, much the same way an ISP looks up the IP address of a domain to send a message. It would be sort of an Internet version of caller ID and call blocking.)

Although the concept is straightforward, implementation has been slow because the major Internet players have different ideas about how to tackle the problem. It may be years before different groups iron out the details and implement a standard. Even then, there's no way of guaranteeing that phishers won't find ways around the system (just as some fraudsters can fake the numbers that appear in caller IDs). That's why, in the meantime, so many organizations—and a growing marketplace of service providers—have taken matters into their own hands.

Be Smart

If a "friend" emails and asks for a password or other information, call or email (in a separate email) that friend to verify that they were really who contacted you. The same goes for banks and businesses. First of all, legitimate businesses won't email you asking for passwords or account numbers. If you think the email might be real, call the bank or business and ask. Or visit the official website. Most banks have an email address to which you can forward suspicious emails for verification.

This is how it works: An email arrives, apparently from a trustworthy source, but instead it leads the unknowing recipient to a bogus website full of malware. These emails often use clever tactics to get victims' attention. For example, the FBI has warned of spear phishing scams where the emails appeared to be from the National Center for Missing and Exploited Children.

Many times, government-sponsored hackers and hacktivists are behind these attacks. Cybercriminals do the same with the intention to resell confidential data to governments and private companies. These cybercriminals employ individually designed approaches and social engineering techniques to effectively personalize messages and websites. As a result, even high-ranking targets within organizations, like top executives, can find themselves opening emails they thought were safe. That slip-up enables cybercriminals to steal the data they need in order to attack their networks.

Numbers

Spear-phishing emails work because they’re believable. People open 3% of their spam and 70% of spear-phishing attempts. And 50% of those who open the spear-phishing emails click on the links within the email—compared to 5% for mass mailings—and they click on those links within an hour of receipt. A campaign of 10 emails has a 90% chance of snaring its target.

If you do not recognize a spear-phishing attack, you may not realize you are losing data until it’s too late. By focusing on a particular person, cyber attackers can eventually gain direct or indirect access to critical data, including bank accounts, computer system passwords, work credentials and security clearances. Spear phishing is a precursor to a far more dangerous advanced attack.

According to studies from the email marketing site DMR Digital Stats and Gadgets, worldwide some 205 billion emails are sent daily by 4.3 billion users. Office workers receive on average 121 emails per day with 42 percent of emails opened on mobile devices and 55.2 percent opened on desktop computers. But not every email message is safe; the site also reports that 2.3 percent of emails include malicious attachments. So of those 121 emails each office worker gets per day, 2.8 of those emails will carry a malicious payload. These statistics show clearly that despite the rise in the use of social media, email continues to be the core communications tool for businesses.

The Who and the Why

Anyone can be the target of a spear-phishing attack, whether they accidentally click on an unsolicited survey response or get bamboozled by a fake alert from their bank. While an attacker may not be interested in you specifically, you can be their foothold into a secure computer system that may contain the PII of customers, executives and other personnel as well as critical data, such as intellectual property and financials. In that sense, we are all critical to the safety of our own PII and the business systems we are part of. If you're in finance, you have access to critical company data. If you're in sales, you have access to lists of customers and prospects. If you're in facilities, you may have access to onsite service-call schedules. Everyone has value.

Spear-phishing attacks are not trivial or conducted by random hackers. They are targeted at a specific person, often times by a specific group. Many publicly documented advanced persistent threat (APT) attack groups, including Operation Aurora and the recently publicized FIN4 group, used spear-phishing attacks to achieve their goals.

The state of spear phishing today:

Right now people are getting more aware of the situation and the usual mail phishing still works but is a lot less efficient because it is been around for a long time and countermeasures are pretty easy. But they are getting more and more smart as well(project proposition, impersonation, ...)

It is still very powerfull with the available tools online to retrieve information about companies, institutions directly from their website and then using social networks to

Predictions for the fututre of spear phishing:

Factors that will influence spear phishing:

Today, the majority of organizations have experienced malware infiltrating their networks through phishing. Two-thirds of decision makers report malware infiltrations through email in the last year. Additionally:

45% believe phishing is a serious or very serious concern 44% fear employees will click on phishing links leading to malware attacks 39% worry about phishing attacks leading to customer data breaches 37% are concerned that data breaches will leak sensitive internal data

The bottom line is that phishing as a method of network penetration is continuing to rise.

Companies are getting more and more aware of the power of those attacks and those companies will start to implement effective defenses to counter them.

Consequences of those factors to spear phising

Assess your risk: Where does your sensitive data reside? Who has access? Take inventory of these things and know how changes (i.e. upcoming new regulations) will affect them. It also helps to know which phishing tactics your users are most susceptible to. Use this combined intelligence to craft a strategy — a combination of people, process, and technology.

Train users: Your employees are your last line of defense against phishing and malware, yet 78% of organizations do not properly train employees to detect and deal with phishing threats. Providing internal security training can boost the overall effectiveness of your security systems.

Select the right security: Finally, keep your organization safe from phishing attempts with a quality security solution, especially when moving email infrastructure to cloud applications such as Office 365 or Hybrid Exchange.

Email security applications, such as PineApp's Mail-SeCure Solution Modules, can provide advanced email security appropriate to small- to mid-sized businesses, enterprises, managed services providers and telcos. Multilayer anti-spam modules, combined with perimeter-level security provide high levels of detection rates for malicious email – even before it enters the corporate network. While email-borne attacks have improved, email security applications also are much more sophisticated and continuously evolving, while also providing functionality for such business requirements as large file transfer, encryption, archiving and the like. Customers now have a single, point solution and are not spread thin amongst many different applications and vendors. PineApp's latest release is recognition that the pressure on businesses across geography and different applications makes them vulnerable but there are solutions to address that vulnerability.

Advanced management and auditing with smart and efficient policy enforcements help the IT department identify potential malicious email and allow the emails to be stopped before they arrive at the target mailbox. The goal of advanced email security is to stop malicious emails before they arrive at the targeted victim. A user cannot click on a malicious link if the email never reaches them.