How do criminals get in ? The art of phishing

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.

==========

https://usa.kaspersky.com/internet-security-center/definitions/spear-phishing#.WMWezH9SFw_

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.

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.

==========

https://uk.norton.com/spear-phishing-scam-not-sport/article

Introduction

The latest twist on phishing is spear phishing. No, it's not a sport, it's a scam and you're the target. Spear phishing is an email that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC. Learn how to protect yourself.

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.

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?

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.

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.

And always remember: Don't give up too much personal information online, because you never know who might use it against you. Or how.

==========

https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html

The Real Dangers of Spear-Phishing Attacks

Spear-phishing attacks are delivered via a standard approach: email. They appear as ordinary emails. The body of the email may contain a link or an attachment. The immediate objective: to get you give up a little bit about yourself—your personally identifiable information (PII).

Spear phishing is targeted. The attackers did their research, usually through social engineering. They might already know your name or your hometown, your bank, or your place of employment—information easily accessed via social media profiles and postings. That bit of personalized information adds a lot of credibility to the email.

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.

Spear Phishing: 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.

How to Stop Spear-Phishing Attacks

To stop spear-phishing attacks security teams must first train users to recognize, avoid and report suspicious emails—it is important for every employee to recognize that their roles grant them access to different data, the currency of the information economy. Second, security teams must implement, maintain and update security technology and processes to prevent, detect and respond to ever-evolving spear-phishing threats. Finally, security teams must strive to stay ahead of attackers by investing in actively updated threat intelligence and expertise to meet their needs.

One thing is clear: You cannot discover a new spear-phishing attack by looking at it in isolation. This is how conventional point products such as antivirus and anti-spam software operate. While they can detect some known threats, they will fail to detect unknown threats and spear-phishing attacks.

Working with FireEye, you can develop fully integrated security solutions that cover multiple threat vectors. A spear-phishing attempt is often part of a blended attack that uses a combination of email, internet browsing and file shares. FireEye can help connect the dots to discover it in real time. Using a combination of industry-leading technology, threat intelligence and security expertise, FireEye can help identify:

```
Which attack groups are likely to use spear phishing
How attackers choose and approach their targets
What their ultimate goals are
What specific steps you can take to prevent or block malicious attacks resulting
from spear-phishing emails
```

To stop spear-phishing attacks and protect your organization’s assets with an integrated security posture, see the FireEye Email Security products.

==========

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

Your I.T. department has no doubt warned you not to click on suspicious links in e-mails, even when the missive promises a hilarious video or comes from a seemingly trustworthy source. If the link looks suspect: Do. Not. Click.

That’s because these emails are often phishing scams designed to trick you into clicking on a malicious attachment or visiting a malicious web site. In the latter case, the web site may appear to be a legitimate bank site or email site designed to trick the user into disclosing sensitive

information—such as a username and password or bank account information—or may simply surreptitiously download malware onto the victim's computer.

Just ask the White House employee who apparently clicked on a phishing email purporting to come from the State Department and allowed hackers into several government networks.

TL;DR: 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.

An estimated 91-percent of hacking attacks begin with a phishing or spear-phishing email. Although firewalls and other security products on the perimeter of a company's network may help prevent other kinds of malicious traffic from entering the network—for example through vulnerable ports—email is generally considered legitimate and trusted traffic and is therefore allowed into the network. Email filtering systems can catch some phishing attempts, but they don't catch all of them. Phishing attacks are so successful because employees click on them at an alarming rate, even when emails are obviously suspicious.

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.

==========

http://www.explorehacking.com/2011/01/phishing-basics.html

What is phishing ? Phishing is a technique of obtaining sensitive data such username,password,credit card details etc by an attacker by claiming to be a trusted or genuine organisation/company. The most common type of phishing is Fake Login Pages. The basic methodology of this attack is written below

1.Suppose an attacker wants to hack gmail/yahoo/facebook/bank account of the victim. Attacker creates a fake login page of that website . This fake login page looks exactly like real/genuine login page.

2.Attacker then sends the link of that fake login page to victim through an email or any other means.The sender's email Id is usually spoofed to give an authentic look to it. 3. Victim clicks on the link, fake login page appears in his browser and he enters his credentials in that page thinking that it is genuine. 4.The credentials that are username and password go to the attacker. Hence victim's account gets hacked. 5.Victim is then redirected to any webpage as chosen by attacker. Most probably the victim is redirected to genuine website or a page displaying an error.

I hope the idea is clear to you. This is the best method to hack anyone's gmail/yahoo/orkut/facebook/bank account.Creating a fake login page is very simple. Then it depends on attacker's smartness that how he manages to fool the victim to get his credentials entered in fake login page. Simply this attack depends on attacker's intelligence as well as victim's carelessness.

Countermeasuers : The obvious countermeasure is that just dont blindly enter your sensitive data in a webpage that exactly looks likea genuine/real page. Carefully check the URL .But URLs can also be spoofed. The protocol must be hopefully https(secure) instead of http. If you still have doubts, you should check the digital certificate of the website. Take care.

==========

https://ijnet.org/en/blog/basics-phishing-attacks-what-journalists-need-know-stay-safe

The basics of phishing attacks: What journalists need to know to stay safe TOPIC:

```
Journalists' Safety
```

Jorge Luis Sierra | October 26, 2016

Unless they cover technology, most journalists probably could not explain exactly how a cyberattack happens. Yet it's more important than ever, given recent global events, for journalists to understand how repressive governments or other groups are launching these attacks against them.

In order to defend themselves appropriately, journalists need to know how they can defeat attempts to infect their computers and mobile devices.

First, journalists need to have a basic understanding of what kind of digital weaponry governments are purchasing. Attackers are using powerful and expensive technology developed by private companies like Hacking Team, an Italian company that sells software that steals information from mobile phones, including contact lists, SMS messages, documents, photos, audio clips, videos and passwords. Some cyberattack software covertly records what keys are being struck on a keyboard and can extract data before it is encrypted.

Secondly, journalists need to understand how these hacking tools work. Although there are some differences between them, they basically follow the same pattern: the victim is deceived into clicking a link after receiving a message with a hidden spy program.

A cyberattack typically consists of the following phases:

```
Infection of the user's device by injecting malicious software. Attackers will try
to deceive journalists by sending a message carefully crafted to look legitimate,
trying to get the victim to click on a link or open a document that will actually
infect their device. There are three ways that an attacker may try to access a
journalist's laptop or phone; in information security lingo, these methods are
known as social engineering, exploits and spear phishing.
Once the malicious software is in the device, it gets to work immediately. If the
device is an iPhone, the software waits until the phone is connected and syncing
with a laptop. The cyberattack software will then override the phone's software
restrictions — a practice known as "jailbreaking" — allowing for the installation
of a malicious program that essentially infects the phone.
The malicious software may actually work best if the infected phone, while plugged
in and charging, is connected to a WiFi network controlled by the attacker. This
way, the victim won't detect any sudden battery drain that usually results from
malicious software at work.
```

This is how adversaries mounted an attack on Rafael Cabrera, an investigative reporter for Mexican

online news site Aristegui Noticias. Cabrera helped report on whether Mexico's president favored a major government contractor that built a mansion for the president's family. The so-called "Casa Blanca" scandal eventually became a major embarrassment for the government.

The first attempt against Cabrera was a phishing attack. Cabrera received an innocent-looking text message supposedly sent by UNOTV, a news service that delivers breaking stories via SMS to mobile subscribers. However, hidden in that message was a version of Pegasus, a powerful surveillance tool that can extract text messages, contact lists, calendar events, emails and instant messages from phones. Pegasus can also harness an infected phone's microphone to record sound and use its camera to take photos.

The messages were a classic example of spear phishing, because they were carefully crafted and personalized, meant to pique Cabrera's interest and get him to click on a link. "The president's office will sue those who published the 'Casa Blanca' story," read one. "Due to 'Casa Blanca' story, the president's office may put reporters in jail — see the names," read the second.

Fortunately, when Cabrera saw these on his cellphone screen, he immediately started worrying that the messages were an attempted cyberattack. He did not click on the links leading to the false news stories.

Editor Carmen Aristegui and reporter Irving Huerta, who both worked on the investigation, also received text messages reading, "My dad died last night, we are devastated, click here to see the funeral home address."

Thanks to their experience and awareness of the risks involved, neither of them clicked on the links contained in the malicious messages.

To learn more on what to do to prevent these attacks — and what to do if you become a victim of spear phishing — click through the slideshow below:

==========

http://www.spamlaws.com/phishing-basics.htmlThe Basics of Phishing

Phishing is one of the most common threats on the internet. Every single time you open up an email on your computer you might be targeted by a phishing attack. Phishing scams are very dangerous and if you're not careful then you could end up having your identity stolen.

Although phishing is very common, not that many people actually know anything about it. There are some important things that you can do to protect yourself from this crime. What Is Phishing?

Phishing is where criminals try to get hold of your personal information. This is commonly done on the internet, however it can also be done over the phone. Normally a phishing email will be sent which looks authentic. Phishing is dangerous because it can result in identity theft.

These emails usually appear to come from your bank account, PayPal, eBay or social networking

site. As you have no reason to doubt them they are often trusted. They will urge you to follow a link in order to update your personal information.

They are commonly very persuasive and make people feel they really need to click the link to update the account. This could be because additional information is needed for security purposes. It could also be because your PayPal account has been limited.

Either way you need to be very careful when clicking on links in your email. When you click on the links you will often be taken to a very official looking website. You will then be instructed to enter security information and to update your personal information. The emails normally give a sense of urgency to complete this by assuring people that this must be completed quickly. Spotting Phishing Emails

Phishing emails look like the real deal; however they are not. There are some things that you need to look out for. The first would be the language. Many phishing scams are started in foreign countries and this means that if the email has poor English or doesn't make sense then it could be a phishing scam.

Emails from your bank and PayPal should always look and sound professional. PayPal will also always call you by your username or real name.

Phishing only works because the phisher sends the same email out to hundreds of people. They don't know who has what bank account and so they will bombard everyone. If you happen to have an account with that name then you might click on the link. If it seems too generic then never follow any links.

Also look at the link itself; it should be the actual domain name of the company. Also right click on it and click properties. This will tell you where the link is really directing you to.

It's a good idea not to click on any links in your emails and instead input the domain names directly into your browser. You can't be too careful on the internet, stay safe!

==========

https://www.meriwest.com/?Cabinet=Main&Drawer=Home&Folder=Security&SubFolder=Basics+of+Phishing

Basics of Phishing Home / Home / Security / Basics of Phishing

Meriwest is very proactive when it comes to our member security. With this latest installment on Phishing, we have outlined additional useful information and tools that will help you protect your security. What is Phishing?

Phishing is a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking

the trusted brands of well-known banks, online retailers and credit card companies, data suggests that phishers are able to convince recipients to respond to them. As a result of these scams, an increasing number of consumers are suffering credit card fraud, identity theft, and financial loss.
How To Identify Phishing

Phishing email messages, websites, and phone calls are designed to steal money. Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your computer. Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. They might email you, call you on the phone, or convince you to download something off of a website.

How would you rate your ability to identify phishers? Find out more about recognizing phishing email messages. How To Avoid Phishing Scams

The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While online banking and e-commerce is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. The Anti-Phishing Working Group has compiled a list of recommendations below that you can use to avoid becoming a victim of these scams.

```
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.
```

Other useful links:

```
File a report with the Internet Crime Complaint Center
Anti Phishing Work Group
Federal Trade Commission information on ID theft
```

Please note that you will NEVER receive an email from Meriwest asking you to verify your account information. And if you do, please report it to us immediately by calling 1-877-MERIWEST or send an email to contact_center@meriwest.com.

==========

http://www.csoonline.com/article/2117843/identity-theft-prevention/phishing--the-basics.html

Q: What is phishing?

A: Phishing is a method of trying to gather personal information using deceptive e-mails and websites. Typically, a phisher sends an e-mail disguised as a legitimate business request. For example, the phisher may pass himself off as a real bank asking its customers to verify financial data. (So phishing is a form of "social engineering".) The e-mail is often forged so that it appears to come from a real e-mail address used for legitimate company business, and it usually includes a link to a website that looks exactly like the bank's website. However, the site is bogus, and when the victim types in passwords or other sensitive information, that data is captured by the phisher. The information may be used to commit various forms of fraud and identity theft, ranging from compromising a single existing bank account to setting up multiple new ones.

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.

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.

What can my company do to reduce our chances of being targeted by phishing attacks?

In part, the answer has to do with NOT doing silly or thoughtless things that can increase your vulnerability. Now that phishing has become a fact of life, companies need to be careful about how they use e-mail to communicate with customers. For example, in May 2004, Wachovia's phones started ringing off the hook after the bank sent customers an e-mail instructing them to update their online banking user names and passwords by clicking on a link. Although the e-mail was legitimate (the bank had to migrate customers to a new system following a merger), a quarter of the recipients questioned it.

As Wachovia learned, companies need to clearly think through their customer communication protocols. Best practices include giving all e-mails and webpages a consistent look and feel, greeting customers by first and last name in e-mails, and never asking for personal or account data through e-mail. If any time-sensitive personal information is sent through e-mail, it has to be encrypted. Marketers may wring their hands at the prospect of not sending customers links that would take them directly to targeted offers, but instructing customers to bookmark key pages or linking to special offers from the homepage is a lot more secure. That way, companies are training their customers not to be duped.

It also makes sense to revisit what customers are allowed to do on your website. They should not be able to open a new account, sign up for a credit card or change their address online with just a password. At a minimum, companies should acknowledge every online transaction through e-mail and one other method of the customer's choosing (such as calling the phone number on record) so that customers are aware of all online activity on their accounts. And to make it more difficult for phishers to copy online data-capture forms, organizations should avoid putting them on the website for all to see. Instead, organizations should require secured log-in to access e-commerce forms.

At the end of the day, though, better authentication is the best way to decrease the likelihood that phishers will target your organization. Banks are beginning to experiment with technologies like RSA tokens, biometrics, one-time-use passwords and smart cards, all of which make their customers' personal information less valuable for phishers.

One midsized bank was able to cut its phishing-related ATM card losses by changing its

authentication process. Every ATM card has data encoded on its magnetic strip that the customer can't see but that most ATM machines can read. The bank worked with its network provider to use that hidden information to authenticate ATM transactions—an important step that, according to Gartner, only about half of U.S. banks had taken by mid-2005. "Since the number isn't printed on the back of the card, customers can't accidentally disclose it," the bank's CISO explained. The information was already in the cards, so the bank didn't have to go through an expensive process of reissuing cards. "It was a very economical solution, and it's been very effective," said the CISO.

What plans should my company have in place before a phishing incident occurs?

Before your organization becomes a target, establish a cross-functional anti-phishing team and develop a response plan so that you're ready to deal with any attack. Ideally, the team should include representatives from IT, internal audit, communications, PR, marketing, the Web group, customer service and legal services.

This team will have to answer some hard questions, such as:

- Where should the public send suspicious e-mails involving your brand? Set up a dedicated e-mail account, such as fraud@domainname.com, and monitor it closely.
- What should call center staff do if they hear a report of a phishing attack? Make sure that employees are trained to recognize the signs of a phishing attack and know what to tell and ask a customer who may have fallen for a scam.
- How and when will your organization notify customers that an attack has occurred? You might opt to post news of new phishing e-mails targeting your company on your website, reiterating that they are not from you and that you didn't and won't ask for such information.
- Who will take down a phishing site? Larger companies often keep this activity in-house; smaller companies may want to outsource.If you keep the shut-down service in-house, a good response plan should outline whom to contact at the various ISPs to get a phisher site shut down as quickly as possible. Also, identifying law enforcement contacts at the FBI and the Secret Service ahead of time will improve your chances of bringing the perpetrator to justice. If a vendor is used, decide what the vendor can do on your behalf. You may want to authorize representatives to send e-mails and make phone calls, but have your legal department handle any correspondence involving legal action.
- When will the company take action against a phishing site, such as feeding it inaccurate information or exploiting vulnerabilities in its coding? Talk out the many pros and cons beforehand.
- How far will you go to protect customers? Decide how much information about identity theft you'll give to customers who fall for a scam, and how this information will be delivered. You should also talk through scenarios in which you will monitor or close and re-open affected accounts.
- Are you inadvertently training your customers to fall for phishing scams? Educate the sales and marketing teams about characteristics of phishing e-mails. Then, make sure legitimate e-mails don't set off any alarms.

How can we quickly find out if a phishing attack has been launched using our company's name?

Sometimes a new phish announces itself violently, as an organization's e-mail servers get pummeled with phishing e-mails that are bouncing back to their apparent originator. There are other ways to learn about an attack, though—either before or after it occurs.

a) Monitor for fraudulent domain name registrations.

Phishers often set up the fake sites several days before sending out phishing e-mails. One way to stop them from swindling your customers is to find and shut down these phishing sites before phishers launch their e-mail campaigns. You can outsource the search to a fraud alert service. These services use technologies that scour the Web looking for unauthorized uses of your logo or newly registered domains that contain your company's name, either of which might be an indication of an impending phishing attack. This will give your company time to counteract the strike (more on that later).

b) Set up a central inbox.CSO. To do this, organizations typically set up one e-mail address where all suspected phishing e-mails are directed, with an address such as fraud@domainname.com or phish@domainname.com. Ideally, this central inbox should be monitored 24/7.

The easiest and most effective way to find out if your organization is being targeted by phishers is simply by giving the general public a way to report phishing attacks. "It's your customers and noncustomers who are going to be the ones that tell you that the phish is out there," said one security manager interviewed for a case study published in

c) Watch your Web traffic.Internet Storm Center recommends that by examining Web traffic logs and looking for spikes in referrals from specific, heretofore unknown IP addresses, CSOs may be able to zero in on sites used for large-scale phishing attacks.

After gathering victims' information, many phishing sites then redirect the victim to a log-in page on the real website the phisher is spoofing. SANS's

d) Hire a firm to help.Brandimensions hosts a vast, interconnected network of domain names and e-mail addresses intended solely to attract phishing e-mails and other spam. They're called honeypots. Entire websites are built to publish e-mail addresses, point to one another, and thereby attract the attention of automated Web crawlers that compile spam lists. The company then uses "relevancy detection software" to flag the e-mails that could be most damaging to its customers.

The same companies that scan the Internet for unauthorized uses of your logo can also monitor for active phishing sites. For example, Toronto-based

How can we help our customers avoid falling for phishing?

People who know about phishing stand a better chance of resisting the bait. "The best defense is that a consumer has heard of phishing and is unlikely to respond," says Patricia Poss, an attorney with the Bureau of Consumer Protection at the Federal Trade Commission. Must be trained to think twice about replying to any e-mail or pop-up that requests personal information.

Teach employees how to recognize spoofed e-mail. Similarly, warn your customers about the dangers of phishing, and let them know you'll never ask for their account number, password, Social Security number or any other personal information via e-mail. Train them to avoid clicking on e-mail links to reach you and instead to type your company's URL directly into a new browser window.

The oft-targeted PayPal, for instance, has a Security Center on its website that includes an e-commerce safety guide, fraud protection tips for buyers and sellers, a link to let users report spoof e-mails and a prominent reminder to log in to PayPal by opening a new browser window and typing in the URL. Some companies also do physical mailings to customers.

However, there's only so much that customer education can do. The onus is also on the organization to limit the damage by shutting down the phishing site.

If an attack does happen, how should we respond?

Once a phishing attack occurs, the goal for the organization is to get the phishing site shut down as quickly as possible. This limits the window of opportunity in which the phisher can collect personal information. With any phishing attack, organizations should take three steps (or hire a firm to take these steps for them).

Step 1) Gather basic information about the attack. This should include screen shots of the website plus the URL.

Step 2) Contact the ISP (or whoever is hosting the website). Explain the situation and ask that the site be shut down. Many phishing sites are launched on hacked computers, so in a best-case scenario, taking down the site is simply a matter of contacting a website's owners, pointing them to the URL of the webpage, and asking them to remove the offending content (and patch their Web servers). "You say, Hey, did you know there's a URL on your website that's a phishing attack?" says Hugh Hyndman, CTO of Brandimensions. "They look at it and go, Oh my God, and they remove that website."

How well an ISP is likely to respond depends on both the ISP and an organization's relationship with it. "If you have good relationship with the ISP, you can get the site down in a matter of hours," says Dave Jevans, chairman of the Anti-Phishing Working Group. "Sometimes." Other times you won't be so lucky. Seventy percent of phishing sites are hosted outside of the United States, so you may need a translator. You also may need to do some delicate negotiations to convince the ISP to throw the switch on a paying customer. If the representative hems and haws and says that policing the Internet is not his job, Jevans says, "rattle a few sabers" and threaten to call law enforcement.

In the most difficult scenario, a phishing site is domain-based. Hyndman has seen phishing websites set up to automatically change their IP addresses as often as every three minutes, hopping from one hacked computer to another in a complex game of cat and mouse played out across the globe.

Step 3) Contact law enforcement. Although this is an important step, be warned that it isn't

necessarily the most effective way to get the site shut down quickly. The FBI and Secret Service are more concerned with patterns and big busts than individual ones, and until a customer has fallen for a scam and suffered damages, there may have been no law broken. Nevertheless, agents may be able to intervene on your behalf—and who knows, your case may be part of the bigger picture investigation needed to shut down a given fraudster. (This has happened. In May 2005, a 20-year-old Texas man was sentenced to almost four years in prison for phishing.)

By establishing a relationship with law enforcement, you'll come to understand when agents want information about what kinds of attacks. For instance, the bank in the aforementioned CSOcase study gets a compact disc from its vendor with information about each phish, and a copy of that CD is then passed on to the FBI, which looks for patterns or anomalies in the attacks.

Does all this sound like too much for your company? Then pay someone else to do it for you. The marketplace is brimming right now with companies that will do the dirty work. Brandimensions, Cyota, MarkMonitor and others offer anti-phishing services.

Responders at a good service provider will have expertise in working their way up the network stream seeking someone who can and will shut down the site. They try to work with the ISP or Web hosting company, and then if necessary contact the domain name registrar that's directing the URL to a given IP address. They'll send e-mails and faxes; they'll make phone calls. If necessary, they'll send notices threatening legal action. Often, when the site is hosted outside the United States, they'll seek help from local groups of first responders organized by CERT/CC at Carnegie Mellon. The end result? The phishing website might be up for hours instead of days.

Any legal/regulatory requirements we should be aware of?

Regulatory requirements depend on your organization and industry, but the financial services industry in general is being pushed to action. Two examples:

- The Treasury Department's Office of the Comptroller of the Currency issued a bulletin in July 2005 that outlined the steps banks should take to mitigate the risks of phishing. Among other things, national banks were told they must file suspicious activity reports, or SARs, if they are the target of a spoofing incident.
- In December 2004, the Federal Deposit Insurance Corp. issued guidelines for how financial institutions can mitigate phishing risks. The document warns that "the financial service industry's current reliance on passwords for remote access to banking applications offers an insufficient level of security" and describes better options, such as two-factor authentication. (View the table of contents for "Putting an End to Account-Hijacking Identity Theft.")

What action can we take against the phishers themselves?

Takedown, which essentially just relocates the problem, may be the only aggressive form of defense that the targeted company has. Prosecutions of phishers have been rare, due to the difficulty of tracing how personal information has been captured, sold and exploited.

However, when a site proves to be particularly vexing to shut down, the vendor may offer to try a

controversial practice sometimes known as dilution. This involves feeding fake information into a phishing site—the goal being to "dilute" the real information, making the phisher's haul less valuable.

Dilution is tricky for many reasons. Opinions differ on how best to generate the fake information. Also, patterns (where the traffic is coming from or how often) can tip off phishers that the information is bogus, possibly prompting them to retaliate against the targeted company. There are also legal concerns. High-volume dilution can amount to denial of service—an attack in which so much bogus traffic floods a website that it collapses. Jevans, of the Anti-Phishing Working Group, laughs when asked about dilution. "That's the polite term," he says. "Denial of service"—the impolite term—"is illegal. Which is why you find not everybody is using dilution."

Vendors may counter that dilution is significantly different from a denial-of-service attack because the Web traffic is supposed to at a reasonable enough rate to look like actual users. Still, most companies are leery of the practice. The bank profiled in CSO, for example, decided that dilution was worth the risk only if the situation became critical, with a large number of people responding to the phish and causing the bank "significant" losses.

How might phishing attacks evolve in the near future?

As phishing e-mails and websites have grown more sophisticated, phishers also have changed the kinds of companies they are spoofing. Early phishing e-mails usually targeted large banks, credit card companies, online payment services, ISPs and large online retailers. As those large companies put defense mechanisms in place to limit the damages, phishers have moved on to smaller companies that may be less prepared to defend themselves.

At the same time, phishers have also grown more sophisticated in their use of e-mail address lists. A phishing e-mail targeting a regional credit union, for example, may be sent only to customers who use ISPs located in that same area. The latest and perhaps ultimate personalization? A technique known as "spear phishing," in which e-mails are customized for particular users. One scam targeted just executives at certain kinds of companies. Security analyst Steve Hunt reports another spear-phishing scam in which he received a text message from a "bank" directing him to call a telephone number; the number yielded a recorded voice asking for his debit card number and PIN.

Meanwhile, as customers become more savvy about the risks of divulging personal information, fraudsters are looking for ways to gather information without the victims' knowledge. This is often done with a method known as pharming. Like phishing, pharming aims to collect personal information from unsuspecting victims. The difference is that pharming doesn't rely on e-mail solicitation to ensnare its victims. Instead, this attack method essentially tinkers with the road maps that computers use to navigate the Web, such that large numbers of users can wind up giving personal data to a bogus site even if they've typed in a legitimate URL.

Pharming combines a mix of mainstream threats such as viruses and spyware, plus more esoteric stuff such as domain spoofing and DNS poisoning. In one scenario, a user receives some kind of

malware (virus, worm, Trojan horse or spyware) that rewrites local host files, which convert URLs into the number strings that computers use to find and access websites. Then, for example, when the user types a legitimate bank's URL into the browser window, the computer is misdirected to a bogus but authentic-looking website of the same sort that might be used in a phishing attack. In another scenario, a hacker poisons a more public DNS directory cache (at an ISP, for instance), again leading unsuspecting Internet users to phony sites.

In either case, potentially large numbers of users are drawn to the fraudulent sites or proxy servers (a computer that sits between the user and the real server and captures information as it passes through), where criminals can track activity and gather credit card data and personal identification numbers.

Pharming is technically harder to accomplish than phishing. To execute a phishing attack, a hacker needs to be able to create a plausible URL, a decent webpage and an e-mail message. This is not hard. Pharming, on the other hand, requires knowledge of how to manipulate DNS caches or gain access to someone's computer files or servers to change settings. But it can also be more damaging, because even savvy computer users may have no idea that their information has been compromised.

How can we guard against pharming attacks?

Just as pharming is more technically difficult to pull off than phishing, it's more technically complicated to protect against. Here are some basics.

a) Deploy technologies such as intrusion prevention and antivirus software, desktop firewalls with filters to look for spyware, and logging software to look for particular events such as spikes in DNS traffic or spikes in e-mail traffic from a single user.

b) Make incident response teams aware of the threat, and teach employees and customers how to avoid pharming incidents. Also ramp up education efforts aimed at business partners, especially for smaller companies that might need help to deal with the pharming threat.

c) Place controls on DNS servers, such as host-based intrusion detection systems, to prevent visitors or customers to websites from inadvertently participating in a pharming attack. There are also some vendors that focus on DNS security, such as UltraDNS.

d) Be prepared to have Internet service providers quickly shut down malicious sites that are set up for pharming. Consider moving ahead with plans for stronger authentication technologies that control access to systems that could be targets of pharmers.

e) Follow developments such as the progress of the DNSSEC standards, and ensure that your company's ISPs have the proper controls on their DNS directories and servers.

==========

https://securingtomorrow.mcafee.com/business/security-connected/past-present-and-future-of-phi

shing/

In the Digital Age, email is second nature. It's a commonly accepted method of communication, and a convenient one, at that. With convenience, however, comes danger – especially if you're not even alerted to the bait!

This email 'bait' I'm referring to comes in the form of phishing scams, which are becoming increasingly abundant as hackers see high ROI on their efforts. In fact, up to 95% of hacks start with a phishing email. Obviously, this is a problem for you, your team, and your business. Like with any problem, the best way to understand it and seek a solution is by examining where it came from.

So, let's take a look at the history of phishing scams, and see what we can glean from these evasive digital threats to educate our future paths.

Past

Since there has been email, there have been phishers. From the great "Nigerian Prince" scam of the late 90s to more complex spear phishing techniques used today — phishing via email has been the single greatest threat to any organization because of the potential to expose corporate data, pertinent financials, banking details, and private employee information. While email is a tool that all businesses rely on to run daily operations, it can also put everyone at risk.

In recent years, organizations both large and small have become increasingly threatened by phishing. It's not just high-profile enterprises that are phishing targets, but also SMBs with a lot to lose. Recently, a small San Diego lawyer unintentionally clicked on a phishing email that he believed was sent by the US Postal Service. The click triggered a malware installation that transferred nearly $300,000 out of his firm's bank account to a bank in China. The moral of the story? From family-owned shops to SMBs and large enterprises, phishing has the potential to affect your organization.

Present

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. But, there are preventative measures organizations of all sizes can take to decrease the probability of infiltration.

Future

```
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.


================================================================================
==

https://www.scmagazineuk.com/the-future-of-email-security/article/531895/

There was a time 20 or so years ago that email security was fairly straightforward
- make sure you have anti-virus software running and remind your users to not click
links they don't recognise. While that remains good advice, email has become a
mission-critical application and remains a major target for spear phishers, social
engineering and the introduction of malware. It's often the first line of attack
for those trying to breach a network.
```

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.

Today's email attackers have very sophisticated tools at their disposal. Using various social media sites, attackers today can identify high-value targets and calculate if those targets or their direct managers are traveling or involved in a project of interest to the attacker.

Unfortunately, according to Verizon's “2015 Data Breach Investigations Report,” users still haven't learned their lessons about opening potentially malicious emails. The study says 23 percent of recipients now open phishing messages and 11 percent click on the attachments. This is not good news, but it also is not necessarily surprising.

Using spoofed return email addresses or information gleaned from social media sites, it is relatively easy for attackers to create authentic-looking messages that could cause an employee to disclose confidential data or click on an infected link. For example, what CFO would decline to open a spreadsheet from the CEO titled Merger Financials? And would an HR manager ignore an email apparently from the corporate counsel that asks for personal data about an employee who is

“under investigation?”

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.

While some of today's email attacks target users with sophisticated intrusions, another important aspect of next-generation email security is identifying and stopping the less sophisticated attacks, such as simply confusing the potential recipient. For example, consider the sales manager who uses Salesforce.com as their sales force automation and customer resource management application. Let's assume this sales manager gets an email recommending that they update their software from a domain called salesforce.update. Might the sales manager be tricked into believing that this is a valid update and not a spear phishing attack designed to download malware onto their server? They might.

==========

https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/

http://www.information-age.com/11-trends-will-dominate-cyber-security-2016-123460617/

https://www.darktrace.com/blog/5-cyber-security-predictions-for-2017/

https://en.wikipedia.org/wiki/Phishing#Spear_phishing