Phishing & Spear Phishing attacks are similar - key differences:

• **Phishing** campaign - *very broad and automated, think 'spray & pray’*

• Doesn't take a lot of skill to execute a massive Phishing campaign

• Most Phishing attempts are after things - *credit card data, usernames and passwords, etc.*, and are usually a one-and-done attack
What is Spear Phishing? - Definition
Spear Phishing is a Highly Targeted Scam

- **Specific** individuals/employee, organization or business
- Advanced hacking techniques & research on targets
- More valuable data - confidential information, business secrets, etc.
- **Who has the information** they seek, & go after that person
- Spear Phishing **email** or **electronic communication** is just the beginning to get larger network access
- Cybercriminals may also install malware on a **user’s computer**
ANATOMY OF A SPEAR PHISHING ATTACK

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

6. The email is opened because they 'know' the sender.

7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/smartphone/network.

9. The hacker uses the backdoor to steal information.
Who do you Trust?

- **Spear Phishing** messages appear to come from a **trusted** source
  - Phishing messages - from a large & well-known business, organization, or website with a broad membership base: Google, PayPal, ASSP, LinkedIn

- Apparent **source** of email/ electronic communication - an individual **within** the recipient's own organization (business) often, someone in a position of authority
  - or from someone the (you) know personally
Spear Phishing Scenario – Social Engineering Users

• Haven’t had high-quality security awareness training - you are easy

• Attacker researches who they regularly communicate with

• Attacker sends a personalized email to the that uses one or more of the 22 Social Engineering Red Flags to make the click on a link or open an attachment

Just imagine you get an email from the email address of your significant other that has in the Subject line:

”Honey, I had a little accident with the car, and in the body: I took some pictures with my smart phone, do you think this is going to be very expensive?”
Social Engineering Red Flags

FROM
- I don’t recognize the sender’s email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it’s not related to my job responsibilities.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- Is the sender’s email address from a suspicious domain (like microsoft-support.com)?
- I don’t know the sender personally and they were not vouched for by someone I trust.
- I don’t have a business relationship nor any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven’t communicated with recently.

TO
- I was cc’d on an email sent to one or more people, but I don’t personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS
- I hover my mouse over a hyperlink that’s displayed in the email message, but the link-to address is for a different website. (This is a big red flag.)
- I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank.
- I received an email with a hyperlink that is a misspelling of a known web site. For instance, www.bankofamerica.com — the “m” is really two characters — “y” and “n.”

DATE
- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?
- Did I get an email with a subject line that is irrelevant or does not match the message context?
- Is the email message a reply to something I never sent or requested?

SUBJECT
- Hi, I’m on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes directly into my account and I can buy a ticket home.
- http://www.bankofamerica.com
- Thanks so much! This really helps me out!
- Your CEO

ATTACHMENTS
- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn’t ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.

CONTENT
- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open up an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender’s request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.
Greetings Steve,

What is the current balance in the account? I need you to make a payment to a vendor and get back to me with the best form to process the payment and your availability to get it processed.

I anticipate your swift response.

Regards

James
Greetings Steve,

What is the current balance in the account? I need you to make a payment to a vendor and get back to me with the best form to process the payment and your availability to get it processed.

I anticipate your swift response.

Regards
James

Email address extension after name is not shown on iPhone & iPad
Always “verify” that it is a known user name address
Text Messages – Open a Link and ?

(732) 377-4569

Text Message
Today 10:11 AM

ggfQLW.Fargo Our site is under maintenance! Please update your device.
www.wfauthinf.cf/0paZh/4252381032.devs

(908) 516-0552

Text Message
Friday 8:39 PM

vfkBM#O-N-L-I-N-E#4252381032#WFargo# Security update! www.infowellsfwnells.gaf/zUatK/4252381032.devs
How to Protect Yourself?

• Traditional security often doesn't stop these attacks because they are so cleverly customized
• Becoming more difficult to detect
• To combat these attacks, companies are turning to anti-phishing software to detect and flag incoming attacks
• Anti-spam and anti-malware tools are no-brainers for any company hoping to protect business data

• Note: “Companies such as IronScales are taking it a step further by layering in machine learning (ML) tools to proactively scan for & flag sketchy phishing emails. ML lets the tools compile or remember scam data; software learns and improves with every scan."
How to Protect Yourself?

• To fight *Spear Phishing* scams, you *(employees, employers, & family)* need to be aware of the threats, such as the possibility of *bogus* emails landing in your inbox, & electronic communications *(Text messages)*

• Besides Education, *Technology* that focuses on *email security* is necessary
How to Stay Safe
Ways to ensure you/ your company don't get scammed

• **Company emails** are labeled "INTERNAL" or "EXTERNAL" in “Subject” line

• Verify suspicious or risky requests by phone
  ➢ *Example: Your CEO emails you and asks you to send someone's personal health data*
  ➢ *Then give him or her a call or send a chat message to verify the request*

• A company asks you to **change** your **password**
  ➢ *Don't use the link in the email notification*
  ➢ *Go directly to the company's website instead; change your password from there*

• Never, under any circumstances – send to someone **in the body of an email**
  your password, social security number, or credit card information, etc

• Don't **click on links in emails** that **contain no other text or information**
PROTECT YOUR CHAPTER FROM SPEAR-PHISHING ATTACKS

ASSP Chapter Leader Training
I need you to process an outgoing payment, can we process via wire transfer or check today? Let me know the details you need.

Thanks,
Arielle
• Mark can check the return email address
• While a spammer can spoof Arielle’s name in the email text field, they cannot spoof her actual email address
• Mark can look at the email address listed – or hit “reply” to show the email address if it does not already appear
• It’s not Arielle’s email address
  ➢ Though it’s made to look like it could be if you just glance at it.
  ➢ A closer look reveals a spelling error (chapters) and an incorrect domain name
ASSP Best Practices

• Verify email address

  ➢ Utilize chapter emails from ASSP
    ex. president@chapter.assp.org

• Contact the “sender” directly
Remember, we are ⚗ – Stay Alert

Thank you
Steven Conklé, PE, CSP
ASSP ROC 1 – ARVP Finance