# Cyber Security Centre of Excellence

## West Bengal

## Department of Information Technology & Electronics
## Government of West Bengal

## HOW TO COMBAT SPEAR PHISHING EMAIL ATTACKS

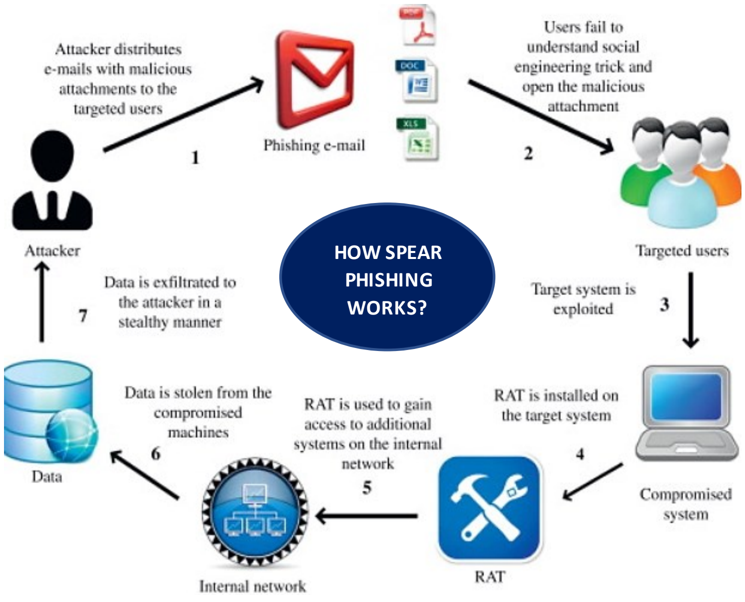
### Phishing:

Phishing is a type of cybercrime in which email, mobile or social channels are used for sending out communications designed for stealing sensitive information such as Bank account details, credit card details, personal details etc. This information is further used for a variety of purposes ranging from identity theft, fraudulently obtaining funds, crippling down computer system in order to secure trade secrets or subtle information relating to national security.

### Spear Phishing:

A spear phishing attack is an attempt to acquire sensitive information or access to a computer system by sending counterfeit messages that appear to be legitimate. **“Spear phishing”** is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents.

Like other social engineering attacks, spear phishing takes advantage of our most basic human traits, such as a desire to be helpful, provide a positive response to those in authority, a desire to respond positively to someone who shares similar tastes or views, or simple curiosity about contemporary news and events. These messages are delivered via e-mail and are designed to convince the user to open a malicious link or attachment, exposing the target to the threats.


HOW SPEAR PHISHING WORKS?
Attacker distributes e-mails with malicious attachments to the targeted users
1
Phishing e-mail
Users fail to understand social engineering trick and open the malicious attachment
2
Targeted users
Target system is exploited
3
Compromised system
RAT is installed on the target system
4
RAT
RAT is used to gain access to additional systems on the internal network
5
Internal network
Data is stolen from the compromised machines
6
Data
Data is exfiltrated to the attacker in a stealthy manner
7
Attacker

Source: malicious software. https://www.sciencedirect.com/topics/computer- science/spear-phishing-attack

## Difference between Phishing and Spear Phishing:

Phishing emails are exploratory attacks in which offenders attempt to obtain victim’s sensitive data, such as Network Access Credentials or Personally Identifiable Information (PII). In the year 1990s, Phishing started off as **Nigerian Prince scams** and has become a common outbreak ever since. These attacks open the door for further infiltration into any kind of network accessible by victim. The victims are deceived by means of social engineering and technical deception and are obligated to open attached files, click on embedded links and reveal sensitive information.

Amongst different varieties of phishing threats, the most challenging one to stop are the spear-phishing attacks. These are relatively more sophisticated, well-researched, and exceedingly targeted operations. The tactics for spear-phishing used by cyber offenders include segmentation of their victims, personalizing e-mails, impersonating specific senders and other related techniques for bypassing old-style e-mail defenses. Though it seems that there is a similarity between phishing and spear-phishing, but both are quite a bit different. The phishing attacks are non-specific and comprises of untargeted low-tech attack vector. Phishing operations are used by attackers to run after low-yield victims while the high-yield victims are targeted under spear-phishing operations.

## Reasons why phishing attacks are one of the top cybersecurity crimes:

- These variety of attacks have solid success rates in the cybercrime industry.
- They demand low cost and deliver an easy return on investment (ROI).
- Cyber offenders can perform these operations with minimal hardware or technological knowledge.

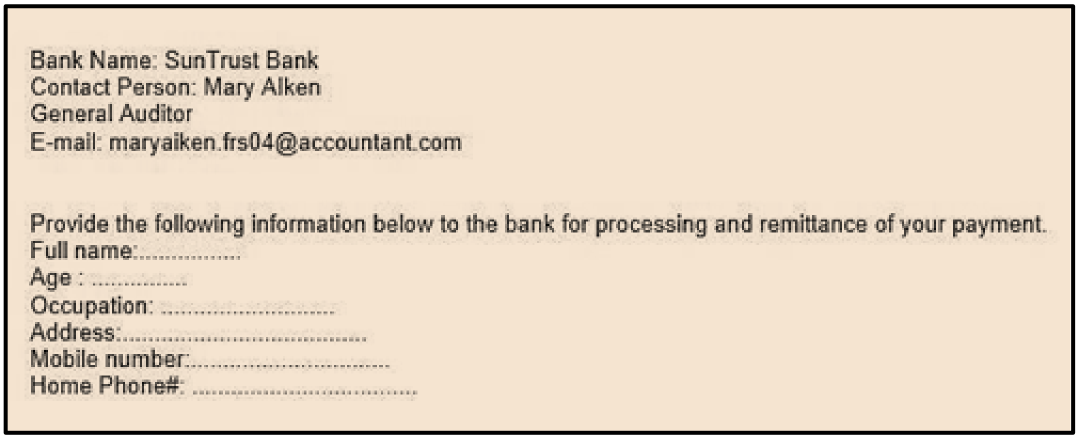
## Characteristics of Spear-Phishing attacks:

- **Blended or multi-vector threat:** In case of spear-phishing, a blend of email spoofing, dynamic URL’s and drive-by downloads for bypassing traditional defenses are used.
- **Zero-day Vulnerabilities:** Advanced level of spear-phishing attacks influence zero-day vulnerabilities in browsers, plug-ins and desktop applications in order to hit systems.
- **Multi-stage attacks:** The primary exploitation of systems is the first stage of an APT attack which further include more stages of malware specific outbound communications, binary downloads and data exfiltration.

- **Well-crafted email forgeries:** Spear Phishing email threats are target-specific hence they don’t bear similarity to the high-frequency spams broadcasted via internet.

## Commonly used tactics in Spear-Phishing attacks:

- The goal is same as phishing which is to trick the targets into clicking a link or opening an attachment.
- The phishing operation may blanket complete database of email addresses but in case of spear phishing specific individuals from organizations are targeted with a definite mission.
- The attackers are able to write emails with utmost accuracy by mining social networks for personal information about targets.
- Once the links or attachments are accessed by the target, a foothold is established by the attacker in the network which empower the culprit in completing their illicit mission.
- For **Advanced Persistent threat (APT) attacks**, spear-phishing is the most prevalent delivery method. Today these APT attacks are launched by cyber offenders and government with sophisticated malware and sustainable multi-vector and multi-stage operations for achieving a specific goal. They explicitly intent to gain long term access to an organization’s sensitive data, network and assets.
- The success of spear-phishing is down to a number of factors. First, it takes advantage of basic human psychology. When taking into account that the email is likely to appear to be from a known, trusted source, such as a bank, work colleague or friend, it is perhaps inevitable that there will be some individuals who will respond, no matter how aware they are of the danger of security threats.



Bank Name: SunTrust Bank
Contact Person: Mary Alken
General Auditor
E-mail: maryaiken.frs04@accountant.com

Provide the following information below to the bank for processing and remittance of your payment.
Full name:................
Age : ...............
Occupation: ..........................
Address:.......................................
Mobile number:...............................
Home Phone#: ................................

An example of spear-phishing email

## Major types of Spear-Phishing attacks:

Researchers lately analyzed **more than 1.5 million spear-phishing emails** and classified them into four major domains:

- **Brand Impersonation:**

Under this domain, emails are designed to imitate renowned companies and commonly used business applications, which makes up around half of all the attacks. Here, the attackers plan to harvest credentials and takeover the account. These kinds of operations are used to steal personally recognizable information, like credit card and social security numbers. In around **56% of these types of spear-phishing attacks**, Microsoft is impersonated.

- **Business Email Compromise:**

These variety of frauds include whaling, wire-transfer fraud and business email compromises which are also known as CEO fraud. Though they cover a small percentage of spear-phishing attacks but has caused loss of **more than $26 billion** in the last few years as per the reports issued by FBI. These predominantly targeted attacks are quite difficult to identify but they rarely include a URL or malicious attachment.

- **Scamming:**

In these attacks, offenders trick victims into revealing the information and use it to deceive them, snip their individuality or both. Attacks are implemented through diversity of hooks like unclaimed packages, lottery winnings, donation solicitations etc.

## Blackmail:

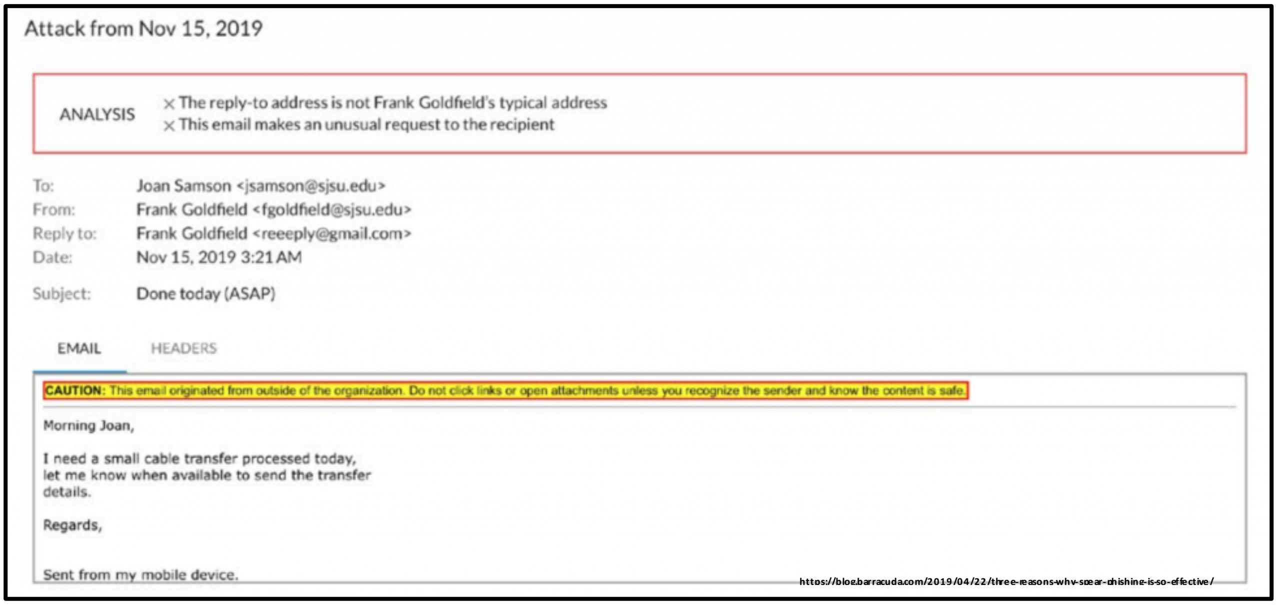
Most of the blackmail scams include sextortion attacks. Attackers claim to have video, images or other suspicious content which has been allegedly recorded on victim's system and threaten to share the personal information of the accused with their email contacts unless they are being paid. Employees are correspondingly targeted through blackmailing scams and corporate email compromise attacks.

## Carefully timed attacks (Business Email Compromise -BEC Tactic):

Through the researches, it has been analyzed that **91% of BEC attacks take place on weekdays** unlike malicious emails which can arrive any day of the week. For making these mails convincing and trustworthy attackers particularly try to impersonate business behavior, repeatedly sending emails during the working hours of compromised account. Businesses are the typical targets in this context, hence it is not surprising that **weekends cover less than 10% of the attacks.** Cyber attackers also use seasonal events/ holidays to upgrade their efforts and feat security weaknesses with other potential vulnerabilities.

## Targeted attacks from trusted sources (BEC tactic):

Though this category of attacks constitutes low volume but are highly targeted. The number of employees according to an **average attack target are not more than 6 in number.** Email-domain and display-name spoofing techniques are used to imitate any employee or supervisor, demanding a lead transfer or personally identifiable information from finance department employees in order to gather sensitive data. Hackers use popular web-based email services, like yahoo and Gmail for launching outbreaks. According to the researches, **reply-to email** has been found different from the **sender's email** in **around 4% of all BEC (Business Email Compromise) attacks.**



Attack from Nov 15, 2019

ANALYSIS

× The reply-to address is not Frank Goldfield's typical address
× This email makes an unusual request to the recipient

| | |
|---|---|
| To: | Joan Samson <jsamson@sjsu.edu> |
| From: | Frank Goldfield <fgoldfield@sjsu.edu> |
| Reply to: | Frank Goldfield <reeeply@gmail.com> |
| Date: | Nov 15, 2019 3:21 AM |
| Subject: | Done today (ASAP) |

**CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Morning Joan,

I need a small cable transfer processed today,
let me know when available to send the transfer
details.

Regards,

Sent from my mobile device.

https://blog.barracuda.com/2019/04/22/three-reasons-why-spear-phishing-is-so-effective/

Example of email-domain and display-name spoofing

### Short and urgent messages (BEC Tactics)

The maximum emails sent as a part of business email compromise attacks are urgent requests which demands prompt response. Mostly, the requests appear to originate from a senior level officer or trustworthy colleague. In few exceptional cases, **1% of BEC attacks email** are casted either with the name of any individual or organization in the subject line. The two most common approaches are to request help or ask about availability. URL or attachments are observed in only 3% of the BEC attacks.

### Examples of BEC attacks:

- **Urgent requests: Around 85% of the Business Email Compromise (BEC) attacks**

  a. **More than half of the attacks – 59% (Ask for help)**

  b. **More than 1/4th of the attacks- 26%- (Ask if the person is available)**

c. **Around 38% of the attacks request urgent help**

- **Payroll and direct-deposit Scams (Around 8% of all BEC attacks)**
- **Gift-card Scams**

## Impact of Spear-Phishing attacks:

- **Only 1 out of 10 spear-phishing emails successfully tricks a user into clicking**
- **Report says around 66% of those surveyed claims that attacks have had a direct monetary cost for their organization in the last year.**
- **The average amount lost per organization due to spear-phishing in the last 12 months has been reported to be around $270,000. A latest business email compromise scam cost a media corporation around $29 million.**

## Major practices for combating spear phishing:

In order to avoid spear phishing attacks, a combination of technology and user security training is deployed. As reported, here are the major practices businesses should consider for protecting individuals from spear phishing attacks.

- **Artificial Intelligence (AI):** Researchers should find a solution for detecting and blocking spear phishing attacks having BEC and brand impersonation which may include malicious links or attachments. The vulnerabilities and suspicious communication patterns which may be a sign of threat can be analyzed by Machine learning tools.

- **One should not rely solely on traditional security:** The traditional email security methods which uses blacklists or DND for spear phishing and brand impersonation may not have protection against zero-day links spotted in many attacks.

- **Account take-over protection should be deployed:** Tools based on Artificial Intelligence should be taken into consideration specifically for the accounts which may have been compromised, so that the spear phishing attacks originating from those accounts may be avoided.

- **Implement DMARC authentication and reporting:** For helping prevent domain spoofing and brand hijacking which are the common impersonation techniques, DMARC authentication may prove to be of great importance.

- **Use Multi-factor authentication:** With the implementation of multi-factor authentication, another layer of security over a simple username and password is added which is an effective security measure.

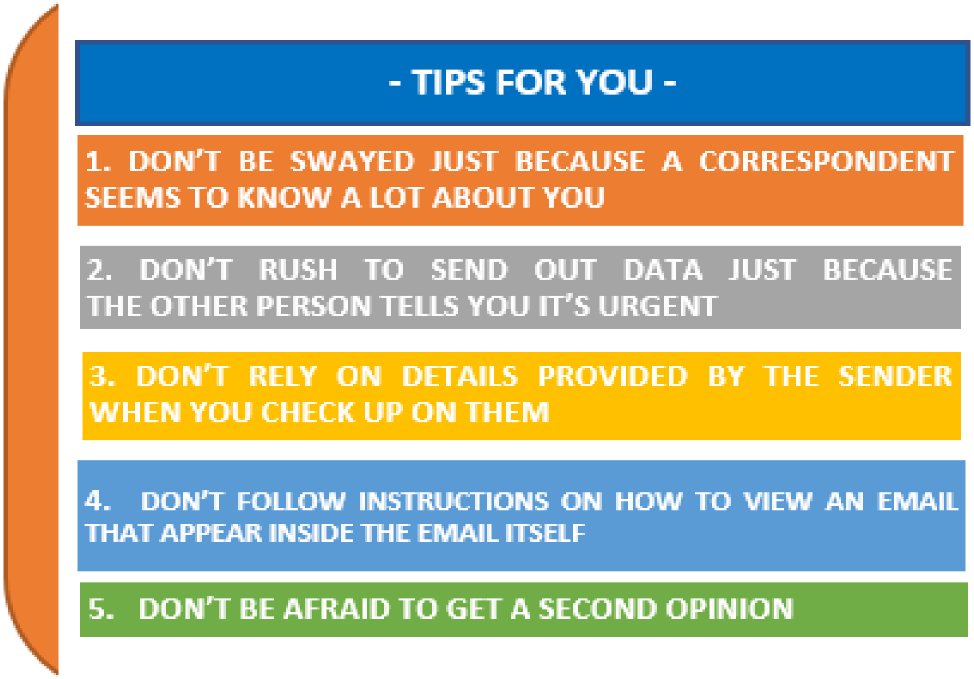
- **Staff should be trained to recognize and report attacks:**
  Reporting and identifying spear phishing attacks should be a part of every security awareness training. Phishing simulations for emails, voicemails, and text messages can be used commercially for training users so that they may recognize them as well. Businesses should establish procedures in system for confirming about any monetary request reaching via e-mail.

- **Pro-active Investigations:**
  Due to personalized behavior of spear-phishing attacks, they may not be always recognizable by the employees. Therefore, organizations should conduct regular scrutiny's for detecting emails with malicious content known amongst common hackers, including the subject in relation to password variations.

- **Prevent Data-loss:**

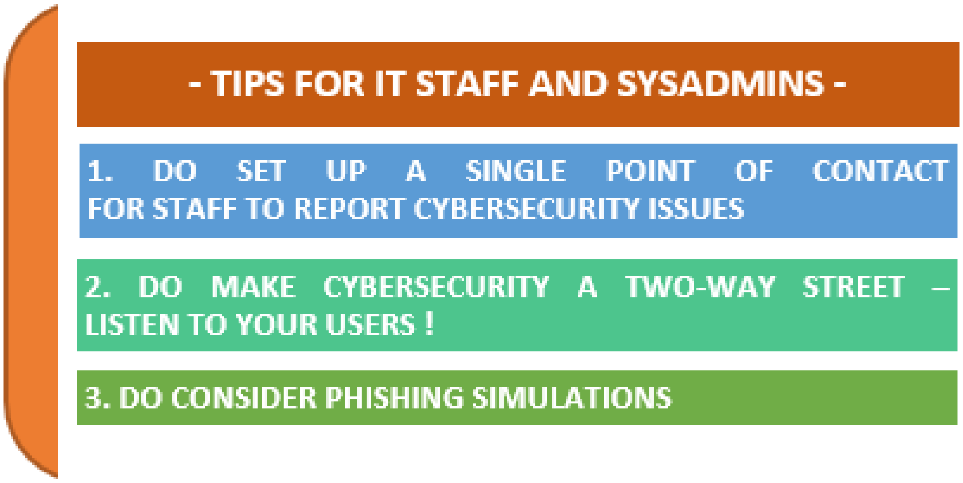
  For maintaining the confidentiality of emails or protecting sensitive information, combination of technical solutions and business policies should be incorporated.

**AWARENESS TIPS:**



- TIPS FOR YOU -

1. DON'T BE SWAYED JUST BECAUSE A CORRESPONDENT SEEMS TO KNOW A LOT ABOUT YOU
2. DON'T RUSH TO SEND OUT DATA JUST BECAUSE THE OTHER PERSON TELLS YOU IT'S URGENT
3. DON'T RELY ON DETAILS PROVIDED BY THE SENDER WHEN YOU CHECK UP ON THEM
4. DON'T FOLLOW INSTRUCTIONS ON HOW TO VIEW AN EMAIL THAT APPEAR INSIDE THE EMAIL ITSELF
5. DON'T BE AFRAID TO GET A SECOND OPINION



- TIPS FOR IT STAFF AND SYSADMINS -

1. DO SET UP A SINGLE POINT OF CONTACT FOR STAFF TO REPORT CYBERSECURITY ISSUES
2. DO MAKE CYBERSECURITY A TWO-WAY STREET – LISTEN TO YOUR USERS !
3. DO CONSIDER PHISHING SIMULATIONS

## Spear Phishing attempts:

### Targeting businesses:

a. Epsilon (2011)

b. Ubiquiti Networks Inc (2015) – Hong Kong

c. Electronic Frontier Foundation (2015)

d. Security firm RSA (2011)

e. Alcoa

### Targeting Individuals:

a. PayPal

b. Amazon (2015)

### Other common spear phishing scam examples:

a. An email from an online store about a recent purchase. It might include a link to a login page where the scammer simply harvests your credentials.

b. An automated phone call or text message from your bank stating that your account may have been breached. It tells you to call a number or follow a link and provide information to confirm that you are the real account holder.

c. An email stating that your account has been deactivated or is about to expire and you need to click a link and provide credentials. Cases involving Apple and Netflix were recent sophisticated examples of this type of scam.

d. An email that requests donations to a religious group or charity associated with something in your personal life.

References:

- https://www.comparitech.com/blog/information-security/spear-phishing/#Examples_of_spear_phishing
- https://www.phishprotection.com/content/phishing-prevention/#spear-phishing-attacks
- https://www.lmgsecurity.com/phishing-attacks-and-spear-phishing-what-they-are-why-they-are-effective-and-how-to-prevent-them/
- https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf
- https://gbhackers.com/spear-phishing-attack/
- https://ascensiongt.com/2019/12/29/spear-phishing/
- https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf
- https://www.sciencedirect.com/topics/computer-science/spear-phishing-attack
- https://blog.barracuda.com/2019/04/22/three-reasons-why-spear-phishing-is-so-effective/
- https://www.slinternational.com/resources/report-spear-phishing-vol-3/