When we talk about technology, everyone would agree that it is getting advanced by the day and more information is easily accessible to us now than it was ten years ago. But along with the multitude of benefits, it has also brought with itself many drawbacks. The easier it is to access information, the harder it has become to protect it. Malicious users are constantly looking for new ways to intrude into systems and steal valuable information. Even an otherwise secure system can easily fall prey at the hands of these constantly evolving intrusion methods.

In an effort to improve the security of our systems and to keep our critical information safe, we are constantly relying upon technology to do everything for us. But when it comes to cyber security, we cannot ignore the human factor which is still the weakest link for hackers all over the world to easily exploit. This is where the term “phishing” is worth mentioning, which is a means to obtain private information like passwords or credit card details by impersonating as a trustworthy source. While general phishing attacks normally fail to achieve the desired results, spear phishing turns out to be comparatively successful many a times.

Let’s have a look at what exactly spear phishing is, what is the reason for success of spear phishing attacks and how can we implement a successful spear phishing defense.

**Spear Phishing Definition**

First and foremost, a definition. A clear and complete definition will help our readers better understand the concept of spear phishing easily as they read further on.

“Spear Phishing is a targeted email that focuses on a specific organization, an individual of the organization, or a group of people to gain access to their confidential information, and falsely appears to be from a trustworthy source within that organization or group of people.”

**What is Spear Phishing?**

So what exactly is spear phishing? Why is it different from simple phishing? Phishing vs. Spear Phishing? Now that spear phishing has been defined, it is important to explain what it is and what the motive behind spear phishing attacks usually is. The content of spear phishing emails seems so legitimate and genuine that receivers are usually tricked into sharing their sensitive information such as username, passwords, credit card details, etc. In another type of spear phishing email you will be asked to click a link, which when once clicked, will deploy spyware in your system and steal your data.

Spear phishing combines phishing tactics such as email personalization, victim segmentation, sender impersonation and techniques for bypassing email filters to trick its target to open an attachment or click a link. Once an attachment is opened or link is clicked, it allows spear phishers to carry out advanced targeted attacks known otherwise as Advanced Persistent Threat (APT) attacks. Advanced and sophisticated cybercriminals are now able to gain long term access to sensitive networks of organizations with the help of APT attacks.

Typically, the difference between phishing vs spear phishing is that phishing attacks can be from random hackers whereas spear phishing attacks are usually from competitors or other perpetrators that seek trade secrets or personal financial gains. Phishing emails usually appear to come from largely well-known companies such as Ebay or Facebook. While in spear phishing attacks the apparent email source is someone within the company and mostly a position of authority. It is often as simple as looking up names of key individuals in a company from its website and then sending an email from his name to email accounts on corporate domain.

**Why is Spear Phishing Successful?**

General Phishing attacks are not always successful because with time and experience, people have become more conscious of responding to requests seeking private information unless they trust the source. Success of spear phishing depends upon three things. Firstly, the source should appear to be known and trusted. Secondly, the information in the mail should back its validity. Lastly, request made by the source should seem logical.

Hence, the reason why spear phishing attacks are mostly successful is because of the presence of above mentioned factors. Very few people actually suspect that an email would be lying about the source’s identity. Again, very few people would suspect that an email specifically mentioning their last name in the email would be a hoax. When simple phishing is combined with other techniques such as asking to click a link, it raises the natural curiosity and desire to do so, focusing more on what matters and filtering out on unimportant information such as complete email address of the source.

As a consequence, employees who fall prey to spear phishing attacks put their entire organization at risk. Malicious links in these emails allow hackers to plant malware in their machines and steal critical information from there.

**Some Characteristics and Real Life Examples**

Here we describe some key characteristics and examples of advanced spear phishing attacks:

**Multi-Vector Threat:** Uses a combination of zero-day application exploits, email spoofing, dynamic URLs, drive-by download, etc. This allows the hackers to bypass traditional means of spear phishing defense.

**Zero-Day Vulnerability Leverage:** Advance Spear Phishing Attacks leverage the zero-day vulnerabilities in desktop applications, plugins and browsers and compromise systems.

**Multi-Staged Attack:** In the first stage the system is initially exploited and then further stages involve malware outbound communication, binary download and data exfiltration.

**Lack of Spam Characteristics:** Personalized messages do not seem suspicious in contrast to high volume spam broadcasted to masses at one time. Reputation filters fail to flag them and minimize the likelihood of being caught by spam filters.

These characteristics indicate that scammers usually make use of simple as well as advanced phishing techniques to successfully trick people into believing them. The following real life examples show how dangerous consequences a seemingly simple email can have on the victims of spear phishing attacks.

1. In January 2009, the CEO and Chairman of Rutberg & Company LLC Mr. Bryan Rutberg became a victim of a spear phishing attack when his Facebook account was hacked. According to him, he had responded to an email from a colleague asking him to click on a link to his Facebook account. Upon clicking, a fake Facebook page opened where he filled his actual username and password.

Upon getting the Facebook details of Rutberg, the hacker then took over his account and sent messages to his friends, telling them that he has been robbed and needs them to send money to a branch of Western Union in London. One of Rutberg’s friends actually sent the money and became an indirect victim of the phishing scam.

1. In early 2010, a California escrow company’s owner received a spear phishing email apparently sent by UPS. Once she clicked the attachment, the hackers were able to install a backdoor into her system and used it to steal $465,000 from the company’s bank account.
2. In February 2015, an Omaha company was tricked into sending 17.2 million dollars to a bank in China. The spear phishing emails were sent to company’s controller apparently from the CEO.

**Spear Phishing Training and Awareness**

According to a research by NSS labs, user training and education is the most effective spear phishing defense mechanism. Training and Education can be in the form of regular classroom style presentations, reminder emails, office memos, newsletters, or simulated phishing emails. Simulated phishing emails are specifically helpful as they can provide a real time scenario to employees, give soft reminders about best practices and also alert the management about which employees require more training.

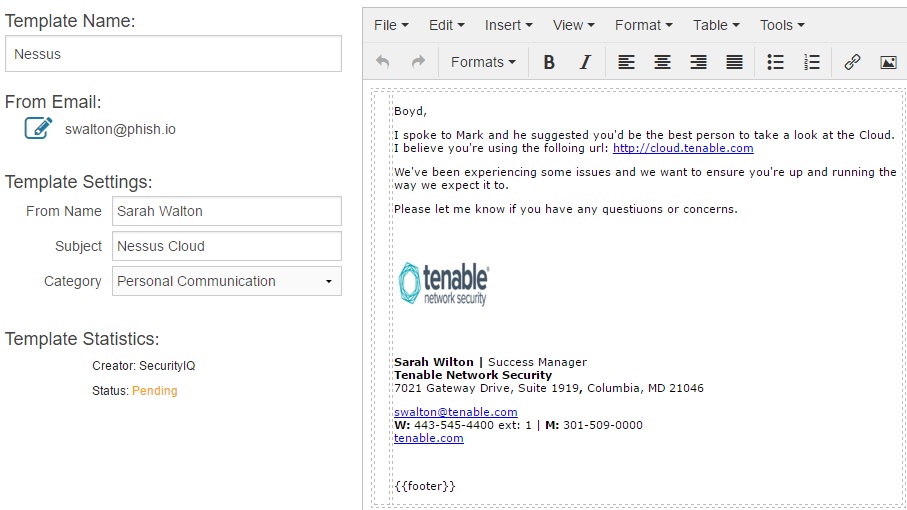
**How to Protect Yourself from Spear Phishing?**

Spam filters are one of the basic controls you can deploy to avoid receiving emails from uncommon sources. In addition to that, advanced malware detection software also helps identify attachments and links. This includes even those attachments and links that the antivirus has not known before. But then again, attackers are also getting more sophisticated and technology is never a complete solution to keep such malicious users away.

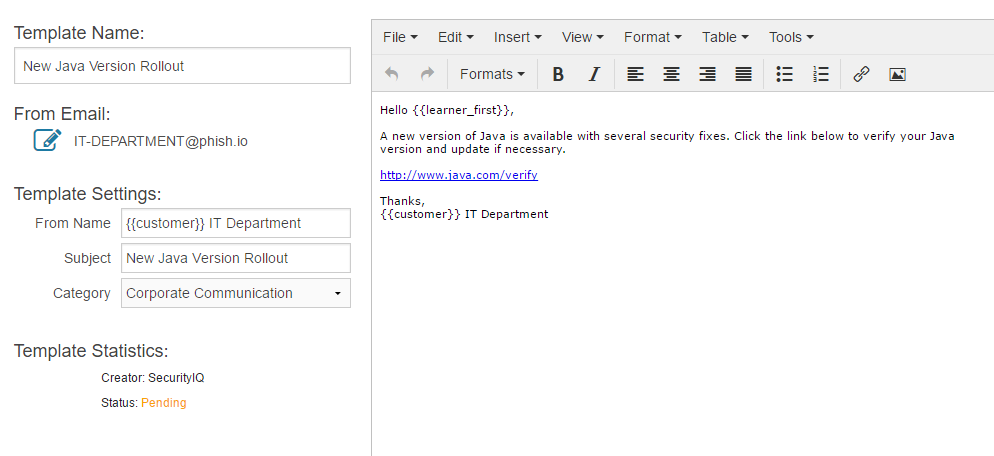
Secure mechanism in terms of technology requires the IT departments to keep all systems on their network updated as outdated systems are often the weak links exploited during an attack. Because human factor can still not be ignored in phishing attacks, even after all these measures, the most important of all is to educate and train the employees for spear phishing defense. The best way is to provide real life scenarios and examples with the help of a phishing simulator.

At PhishSim, we have designed several simulated phishing emails that will allow employees to learn how to spot a spear phishing scam before they respond.

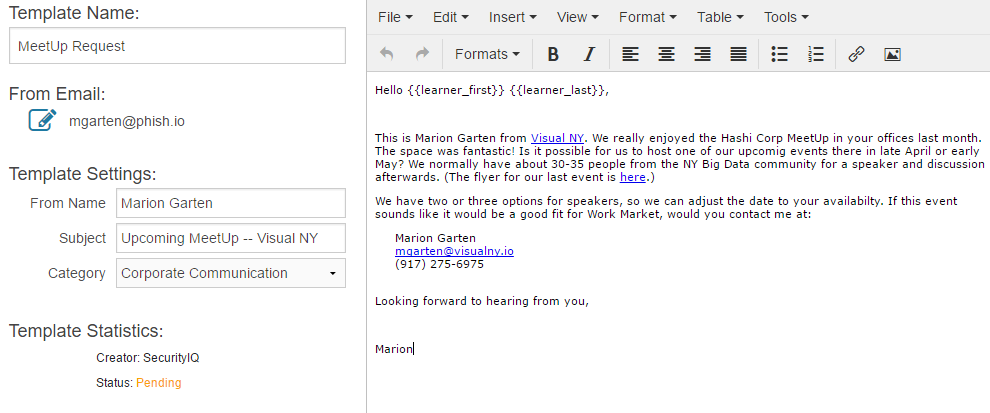
Below are some of the spear phishing email templates from PhishSim. These can be used to check employee awareness regarding phishing scam and realize the need for employee training by testing how many employees actual fall prey to them.



Here, the sender has directly addressed the employee and the email content seems like a routine office communication. In reality, the link sent by the user actually leads to malware installation in your system.



In this Template, the email appears to have been sent by the IT Department, asking all the users to update Java on their systems.



In this email, the sender is referring to a past event that actually took place and addressing the receiver by their name. The request seems legitimate and can easily trick the receiver into clicking the link.

These are only few of the examples our PhishSim simulator provides to its clients. These simulated emails help organizations and their employees understand the nature and level of spear phishing email they can receive and prepare them for a more “phishing-conscious” approach when reading and responding to electronic messages.

**What are Some of the Best Practices When Responding to Emails?**

Here we give you a list of best practices to adopt spear phishing defense and help yourself and your coworkers avoid such attacks

* **Use common email sense.** Never trust an email message, even if you think it is from a trusted source. Take out some time to examine its authenticity, especially if the message asks you to provide confidential information or to click a link.
* **Be extra vigilant about emails that refer to current events.** For example, an email apparently coming from your colleague asking you to open a link to pictures of a recent event that took place in your organization, live broadcasting of a sporting event, or pictures of a recent natural disaster are likely to be malware links.
* **Do not assume that emails sent by colleagues or friends have secure attachments or links.** Information such as email addresses can be easily attained by hackers from company’s official website or social networking websites. If the contents of the message seem suspicious, a safe approach is to call your friend from whom you have received the mail and verify if they actually sent it or not, especially if you were not expecting a message from them.
* **Analyze the URL in case of a web link inside the message to trace its actual origin.** Since it is very easy to spoof a hyperlink’s text, take your cursor over the URL without clicking and check the complete address of the link. If it sounds unfamiliar, do not click it.
* **Dig out further on emails requesting immediate action.** Check the company website by searching the company name in Google and get their contact number. Call them to verify if you have received a valid message or not. Do not call on any number provided in the message as it will lead you directly to the malicious user.
* **Do not post too much personal information on social networks.** Putting information such as birthdays, names and ages of your spouse or kids and anniversary dates can be used against you by tricking you into a phishing scam.
* **Always be extra cautious about unexpected messages on mobile phones through SMS or social messengers.** People are more likely to respond to “smishing” attacks on smartphones. Social messengers even create a thread where a link clicked by one user is automatically sent to all other users in their contact list. A smartphone connected to its company’s network is an easy target to compromise.