

|  |  |
| --- | --- |
| Home | **Location:** Ground Floor, Unit 30a/3 Manton St, Darwin NT 0800 |

Peter O'Gorman

Rahul Shokeen

Yi (Angi) Yang

1st Dec. 2020

**Bsiness process in managing Spearphishing email**

**Table of Contents**

**1. Problems Overview in Spear Phishing1**

**2. Spear Phishing Situation Analysis5**

2.1 PESTAnalysis5

2.2 Target Person to be Targeted5

**3. Identify Potential Opportunities6**

3.1 As-is Diagram6

3.2 To-be Diagram6

**3.3 Algorithms7**

**3.4 The Benefit of This Product** **7**

**4. Measure the Effectiveness and Efficiency (KPI)8**

**5. Appendix10**

**1. Problems Overview in Spear Phishing**

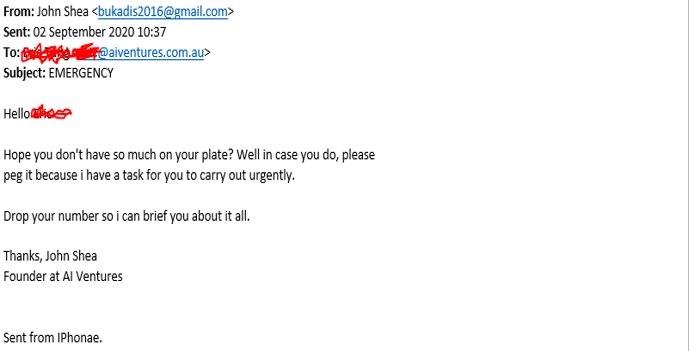
****

Figure 1 the person pretends as the company big boss

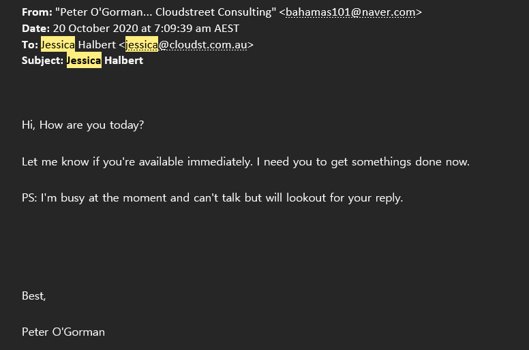
****

Figure 2 the person feigns himself as Peter O’Gorman to send email to his staff



Figure 3 the person disguises himself as a colleague to send email to the receiver

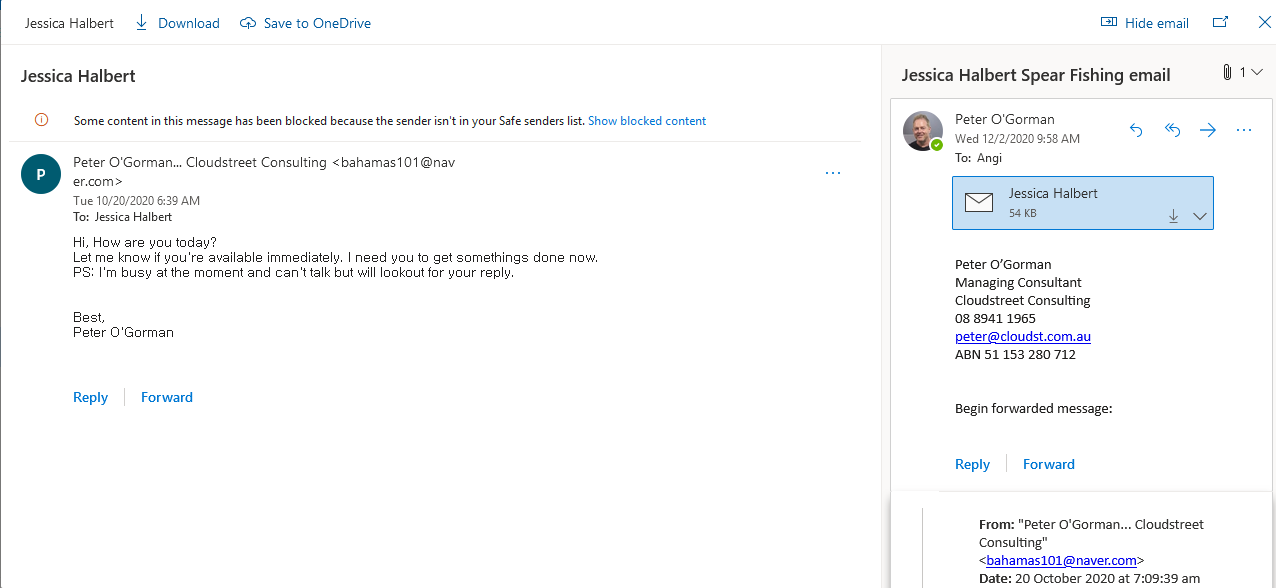


Figure 4 someone forwards the email contains the information from previous sender and receiver

**a. The hacker is normally pretending himself as a company funder and asking contact number from the receiver (**Figure 1**).**

**b. The hacker feigns himself as a company manager and only communicates by email (**Figure 2**).**

**c. The hacker disguises himself as a colleague of recipient to ask contact number (**Figure 3**).**

**d. The previous sender and receiver’s information have been leaked by forwarding email (**Figure 4**).**

The examples are all a kind of email attack by Spear Phishing that is the act of sending and emails to specific and well-researched targets while purporting to be a trusted sender. The aim is to either infect devices with [malware](https://www.csoonline.com/article/3295877/malware/what-is-malware-viruses-worms-trojans-and-beyond.html) or convince victims to hand over information or money.

Spear phishing is a campaign that was purposefully built by a threat actor with a goal of penetrating one organization, and where they will **really research names and roles within a company**. A highly targeted form of phishing, involves bespoke emails being sent to well-researched victims. It is hard to spot without close inspection and difficult to stop with technical controls alone.

It’s quite obviously that the spam did harmfully to the recipients especially to the non-IT staffs. Let’s assume that a person pretends as your big boss or higher manager and asks you for a contact number, key information of your company or doing something for him. Although we won’t acknowledge, it’s true that we were under pressure and willing to have an effective performance so that we were easily to be cheated at that time.

However, the hacker would also feign himself as a close friend or relative of you in spam so that you could easily lay down the guard and do something for the hacker as his expectation without a double-checking on his real identity.

The even more damaging is the computer virus, Trojan horse virus or ransomware contained by the spam that might be links, pictures, or the spam itself when you start to read while click on it. The results could be computer damage, economic loss, loss control of your account and computer. You cannot do anything on it before you find a specialist for help.

**2. Spear Phishing Situation Analysis**

**2.1 We use PEST analysis to show the issues under below:**

Figure 5 PEST Analysis on Spear Phishing Attacks

After the PEST analysis (Figure 5) we do realise that Spear Phishing Attacks are more complicated, and the loss and risky is even hard to be measured. Phishing Attacks happened as email service started. They were mainly multifarious advertisements bombarded the clients’ email inbox. On record of [phishing](https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html) attacks began as [Nigerian prince scams](https://www.csoonline.com/article/3249484/west-african-criminals-moving-nigerian-prince-scams-duping-business.html) in the mid-1990s, today they have morphed into well-researched and targeted campaigns that are both highly effective and incredibly difficult to stop.

**2.2 How a target person has been targeted?**

Some targeted campaigns involve documents containing malware or links to credential stealing sites to steal sensitive information or valuable intellectual property, or to simply compromise payment systems. Others avoid malicious payloads and instead use social engineering to hijack processes for a small number of large payouts via a single or series of bank transfers.

Another way could be subjective that the person registered at some websites, published his personal information in the social media such as Facebook (It happened several times that hacker finds someone’s friend circle and pretend as a friend to hack successfully.), WeChat and you name them, handout business name cards and CVs, and etc..

Well, from the situation analysis, we have get to known that Spear Phishing has already caused plenty problems and will be continued. Therefore, is there any solutions fitting on it?

**3. Identify Potential Opportunities**

**3.1 As-is Diagram**

Spear Phishing working by as-is diagram.

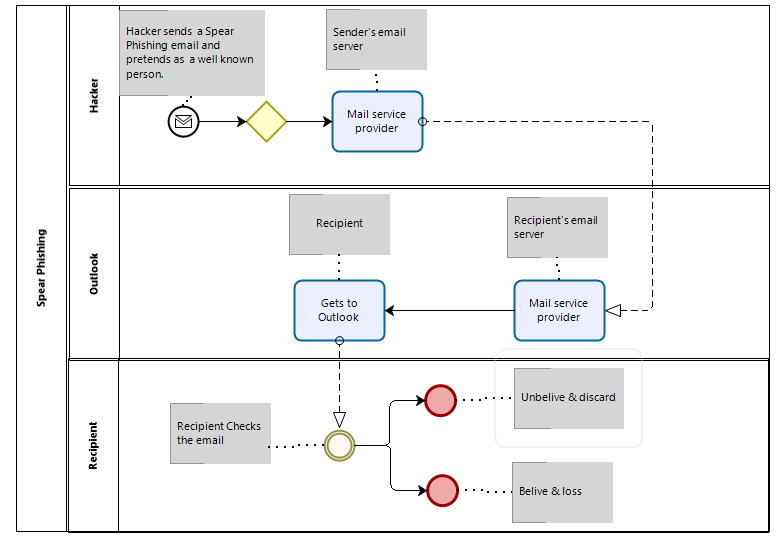


Figure 6 as-is diagram shows the situation of Spear Phishing

We can see from the diagram (Figure 6) that anyone could become the hacker as long as the one got the target email address and knew the manager’s or other staffs’ full name in a company as well. Then just simply edit an email pretending to be that person and finish with his full name signature, and send. The recipient normally needs 15 seconds to 30 seconds to recognise that is a Spear Phishing Attack, or he won’t and become a victim from that.

**3.2 To-be Diagram**

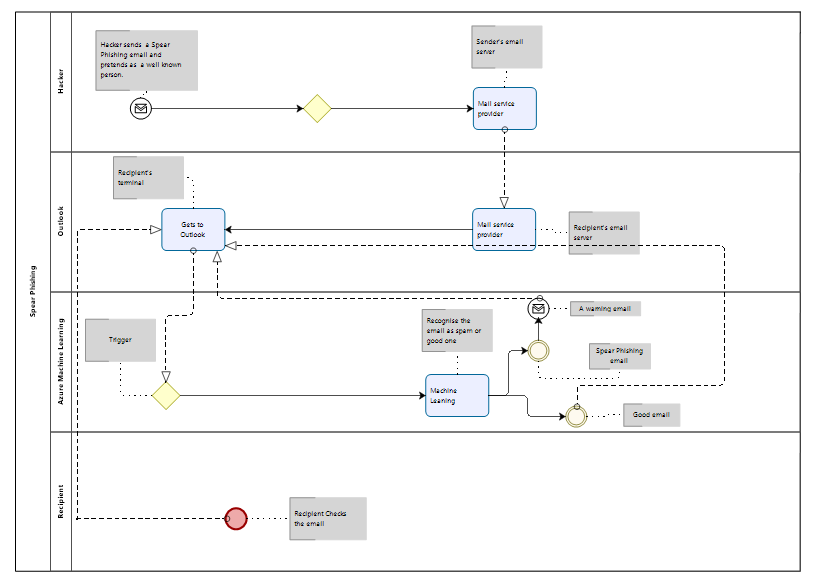


Figure 7 to-be diagram shows machine-learning blocks Spear Phishing and warns recipient by email

To change this condition, we need the support from Azure Machine Leaning (Figure 7). Checking the email content by programming, the machine could recognise the similar content of spear phishing email and block them. Then send a warning email to the recipient in which including the spam attached in the attachment. The to-be diagram shows the process using Machine Learning management.

**3.3 Algorithms**

**a. One of the most common spear-phishing traits involves exploiting a sense of urgency.**

**b. the most obvious warning sign is an incorrect email address or one that looks similar to one you expect but is slightly different.**

**c. by machine learning, the content of Spear Phishing email could be easily recognised, then block them.**

**3.4 The Benefit of This Product**

There are several solutions around Spear Phishing Attacks by doing research from Internet. They are:

1. Training company staffs in recognising the spear phishing email;

2. Setting the email filter in blocking the spear phishing email and report to server;

3. Comparing the sender’s using name with email address;

4. Remove email address from hacker’s list as same as unsubscribe function;

5. Build an email folder especially for the company staffs (for example: Cloudstreet), once receive email form a colleague, and find it in this specific folder.

Whereas, our software using machine learning algorithm to recognise the content of spear phishing email then block the similar content ones.

1. The company does not need to train the staffs to save the time and money.

2. It’s hard to share the email filter setting between companies, and it’s easy to generate new email address using for hacking.

3. Here has more or less people using irrelevant personal information in their email addresses so comparing user name with email address couldn’t be a perfect solution.

4. Removing email address from hacker list like unsubscribe function would be realized in the future and need technical support in both hardware and software, but not now.

5. Building a specific email folder is similar as the second suggestion that is hard to spread between companies.

Therefore, the software is easy to accept and spread between companies as long as the company is using Microsoft service especially Azure platform. Then they can access the service at anywhere by any time. The only work we should do is making the algorithm more and more efficient.

**4. Measure the Effectiveness and Efficiency (KPI)**

Need data then continue...?

**5. Appendix**