Multi-stage Targeted Twin Phishing Attack
A Small International Trading Company Case Study

Qingxiong Ma
University of Central Missouri

Mustafa Kamal
University of Central Missouri

Abstract

Only the email phishing process and characteristics are fully understand, can the effective counter-measures be taken to improve employees ability in the decision making process. This study attempts to explore the process and features of email phishing in small international businesses. Recent email phishing attacks show they are more of targeted twin phishing with specific domain knowledge launched by distributed global team rather than mass phishing. The attacks are characterized with multiple stages including target searching, twin phishing, spoofing, clone phishing, controlling, and manipulating. Through the analysis of a business case with an international small trading company, the discussion was supported and justified. The result from this study and the enclosed business email phishing case can be used as email security training or education materials.

Keywords: email phishing, multi-stage, case study, small international business, targeted twin phishing

1. Introduction

Realizing the business value of technology, more and more business are using technology to reduce the transaction cost and exploring new business opportunities. The growth and advancement of technology has not only benefitted honest Internet users, but has provided criminals new powerful tools of fraudulence. Email phishing attack is one of the biggest threats to business users.

Phishing is a form of social engineering in which a criminal, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion (Markus, 2007). Phishing emails always ask victims to click a link that will guide the victim to a forged website where personal information is requested. According to the Anti-Phishing Working Group, 25,000 phishing campaigns are launched per month. For general consumers' email attack, the purpose of phishing is to get personal identity, credit card number or authentication information such as user name and password. Unfortunately, people tend to use the same login information across several websites or systems.

Email phishers are not just targeting consumers. They are going after high profile targets to steal proprietary information such as intellectual properties, business secrets, even national security (Hong 2012). Phishing is a hazard to E-business (Richard and Hintau). The damage caused by phishing goes beyond monetary property. Delicate bonds of trust that organization build with their constituents are eroded. People loss faith in the reliability of e-business, companies loss their customer base, reputation, and credibility, which in turn causes significant economic loss, resources and time. However, the numbers of email phishing incidents reported for corporate and business is only very small portion of the actual number simply because victimized companies do not want to release any negative news to public so that their image can be damaged and the confidence of the investors may be undermined.

Special attention should be paid to email phishing in small-and mid-sized businesses (SMBs). SMBs are often targeted. The statistics shows the majority of data breaches were perpetrated against smaller firm (DBIR Verizon, 2012). Despite the fact, many SMBs perceive that they are too small to be targeted by email phishers. In addition, unlike their counterpart of large firms and corporates, SMBs often do not have effective email gateway solutions, security knowledge, or security policies as well as resources for controls regarding to information security. Thus, SMBs are more vulnerable and easier to be attacked by the email criminal groups.

Only people fully understand the email phishing process and characteristics, can the effective counter-measures be taken to improve employees ability in the decision making process. For this purpose, this study will explore the types of phishing, process and characteristics of phishing in SMBs. To support the discussion, a small international trading company case study was conducted.

2. Purpose of Targeting SMBs

Most business email phishing attacks are conducted by a group of professionals. The motivations and reasons of business email phishing include:

1) Employee personal identity information or download malware onto the computer
2) Innovative research or intellectual property (IP)
3) Business partner relationships
4) Direct monetary property by kidnapping the business transaction

3. Attack Classifications

Generally, business email phishing attacks fall into mass attacks and targeted attacks (DBIR). Mass attacks have been the basis of threats since the first days of distributed networks. Self-propagating worms, distributed denial of service (DDoS) attacks, and spam are some preferred methods for achieving financial gain or business disruption. The criminal creates a common payload and places it in locations that victims might access, often inadvertently. Examples include infecting websites, exploiting security vulnerabilities in file formats such as PDFs, sending emails to make a purchase, and mass phishing of banking credentials.

Targeted attacks are highly customized threats aimed at a specific user or group of users. These attacks are disguised by either known entities with unwitting compromised accounts or anonymity in specialized botnet distribution channels. Targeted phishing to a group of people with a commonality is also termed spear phishing. Spear phishing is a new class of phishing attack that is becoming popular. Spear phishing have many common features as earlier phishing scams, but they are more context specific and seem to have originated from an organization (Wang et al.). Notably, a recent server breach at the Internet marketing company Epsilon caused the names and email address of millions of people exposed. This breach is described as the worst of its kind (Information Week, 2011).

4. Characteristics and Process

Business email phishing is kind of spear phishing, in which phishers are professional, globally distributed, and team-worked. This type of phishing is characterized as targeted, well-planned, multi-staged, and difficult to protect against. They are financial transaction oriented, twin phishing along supply chain, and can the most potent negative impact to victims.

4.1 Targeted Twin Phishing

To make victims believe they are interacting with legitimate parties, phishing attackers need to have specific business domain knowledge, personal background information or business activities tailored to email receivers. The spear phishing email may appear to relate to some specific item of personal importance or a relevant business activity - for instance, discussing payroll discrepancies, a legal matter, or proposing new business opportunities. To collect the information, they may have a strategy starting with targeted geographical and economical location. Then, they select profitable industries, and followed by the selection of specific businesses.

Phishers understand businesses in developing countries are easy to attack. In these places, the history of computing is shorter, the level information security awareness is low, and the security controls are not always in place. They also understand the expectations of English writing level for business communication in the non-English speaking countries cannot be too high. Next, they may focused on some targeted industries such manufacturing and construction, where large volume of financial transactions generated frequently. Third, they understand companies advertising on many B-to-B websites are financially sound, large volume sales, and strongly interested in getting new sales order. These companies are listed in some famous

websites. They may also do some preliminary search and collect personal information about their target email receivers from social networks, press releases, and public company directory.

Phishers, as a group of financial fraudulent criminals, understand they have to control the business transaction to make money. To fully control transactions, the control and manipulate the communication on both ends of business partners is imperative. Therefore, email accounts for both business partners have to be phished. Since businesses are related or networked to each other, when one business email system is phished successfully, it is easy to find out other partners. If the first phished account happens to be an upper level supplier, they will get the customers information down the supply chain, and vice versa. Therefore, the email phishing attack to businesses is not only targeted, but also paired alone the supply chain.

4.2 Well crafted

Generally, phishing emails have multiple domain names in the email header and contains links in the content part. Salem et al. categorized the features of phishing emails into source code and content. The former includes IP-based URLs and Non-matching URLs, contain scripts, and number of domains. The latter includes generic salutation, security promise with a link and links to https website. The hyperlinks usually are located in the emails and can appear as any one of the 5 categories (Jain and Richariya):

1) The actual link and the visual link in the email are different i.e., the hyperlink in the email does not point to the same location as the apparent hyperlink displayed to the users
2) The DNS name in the hyperlink is substituted by the quad-tuple IP address
3) DNS names used are manipulated to look similar to the genuine DNS name the phishers are trying to forge
4) The hyperlink is encoded so that it becomes very difficult to read for example, unusually long hyperlinks
5) When visiting the phishing hyperlink, it usually asks the user for various personal details like username, password, account number, SSN, etc.

Business spear phishing attacks are typically well planned and designed. From the email message content, format, writing style, layout till the forged website design, they are well planned, designed, and integrated. Technically, phishers use a blend of email spoofing, zero-day application exploits, dynamic URLs, and drive-by downloads to get around traditional defenses.

4.3 Serialized Multi-stage

The process of email phishing is generally divided into three phases. The first is targeted victims receiving an initial phishing message; the second is the victim taking the suggested action in the message by clicking a link to a fake website, where the sensitive information such as username and password can be collected if victim reply, or download a malware for outbound communications and data exfiltration; the third is the criminal monetizing the stolen information (Hong,; FireEye). However, the process of business spear phishing attacks is much more complicated and difficulty. Generally, they containers the following stages:

1) Target-searching and Phishing Email Crafting

The initial phishing email is tailored to the receiver in such a way that the phisher does not have to mimick or use some big names, financial, trustworthy or public organization as they did in some other types of email phishing. This indicated that the selection of the target businesses requires business domain knowledge, email receivers' personal information or specific business activities.

2) Set up Camouflaged website to collect credential login information
   To collect the victim's credential or confidential information, the phishers usually set up fraudulent websites, which are usually hosted on comprised servers under a subdomain. They can also register a new domain with similar spelling or the same domain in different countries such as foshan.com, fushan.com, foshan.com.cn, foshan.com.uk. Then the phisher created this page and wrote a script file using PHP or JSP. This script file will collect the data and save the information into a database or send to an email when the button is clicked.
3) Configure the email setting for long-term access
   Nowadays all the popular email system such as Gmail has many powerful and useful functions, which the phisher can take advantages over. For example, both offline function and the email forward function using either POP3 or IMAP in Gamil allow users to have a copy of the emails records very soon. Besides stealing the email records for customer relationship, company innovation documents in the attachment, phishers also can change the setting for long-term access.
4) Twin phishing along the business supply chain
5) Clone phishing. It is a type of attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email (Rajkumar). The attachment or Link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. Nowadays the popular web email system including hotmail, yahoo, and gmail allows users to specify a Reply-To address. This function makes it possible that the users send a message from one account (Hotmail for example), but receive replies at another email address. The phisher configured the email setting put his email address in the Reply-To part. As a result, when a user send email, the message will be replied to the phisher instead of the user-self. Then, the phisher cloned the reply and send to the user.
6) Controlling communications and Manipulation information. Popular email systems not only allow users to specify the Reply-To a different address, they also lets users send messages with another of email addresses listed as the sender. This feature helps users manage multiple accounts from one interface. In Gmail, to use one of the alternate sender addresses, click the FROM link when you compose a new message. After clicking FROM, you'll see a drop-down menu next to your address, where you can select the email address you'd like to send from. That means, the email can be configured and send from any address as long as that address is validated. In this way, the receiver will see that the message comes from the real business partner's email address.
7) Intervening business transactions for monetary purpose

This is the most risky stage. In order to fraud successfully and get the money out of customer's pocket as soon as possible, the phisher can make any promise at any price to satisfy the customer.

Although the process of business email phishing is complicated and expensive, it is usually very effective and has high probability of success and the rate of return (Figure 1, Appendix). According to a white paper (FirEye), spear phishing emails had an open rate of 70%, compared with 3% of open rate for mass phishing. Further, 50% of recipients who open the emails also click on the enclosed links, which is 10 times the rate of mass mailings.

4.4 Globally Distributed Teamwork

The business phishing is a team work because the phishing process requires several roles and each should be conducted by different person. Email is an information technology product, to bypass the security huddles and attack emails, phishers need someone who is strong technical skills. They need person who are good at writing and business person knowing negotiation. They need people help to create a fake business and set up business bank account. They need people understand the international fund transfer process.

With today's technology enabled globalization, it is very easy to set up such a team, and the cost is very low. The examples of popular websites for outsourcing are: oDesk, Elance, Guru, RentACoder, GetAFreelancer. After you post the job, you will receive applications very soon from all over the world. Many virtual assistant only ask for a few dollars per hour. Since these team members may not know each other, it is very difficult to be detected, discovered, and punished.

5. MOHO: A Case of Small International Manufacturing and Trading Company

MOHO is a manufacturer of construction chemicals in China. The company produces over 70 products, including coatings, glues, water-proofing materials, high range water reducer, set accelerators, set retarders, anti-freezing products, etc.. These products are widely used in industrial and civil engineering, public infrastructure, hydraulic electricity engineering and concrete ready-mix products. In addition, MUHU provides professional services of technology know-how transfer, including process, design, manufacturing, application, and management know how. Their customers are mainly businesses instead of general consumers.

In order to expand to international market, the company developed their business website, actively posted the company and products information in many B-to-B Internet marketplaces such as Made-in-China, Alibaba, and ECplaza. They also paid for the clicks for Google ads. As many SMBs, they adopted popular Gmail for the business because it is free and functionally powerful. Email is the major communication tool for the international sales. Sometimes, they also use instant message tools such as MSN, Skype, Gtalk and telephony to communicate with customers overseas. The content of email communication covers almost every aspects of sales, including new product or new price information, order negotiation, confirmation, proforma invoice (PI), sales contract, payment information, and product shipping information. PI includes information for the order, payment and shipping. The minimum order quantity is one 20 feet shipping container, which is usually worth 30,000USD. The preferable payment method is telegram wire

transfer (T/T) because it is faster and cheaper than letter of credit (L/C). The payment process usually starts with issuing a PI based on many-turns of talk and discussion. Then the payment is made by customers based on the instructions on the PI. Once the fund is credited to the bank account, the vessel is booked and container is loaded. They had shipped the products to every corner of the world.

The employees and management of MOHO are not aware of email phishing until recently the company email account was targeted and phished. The attack is advanced, complicated, and the assault is devastating and incredible. The analysis of this incident case will display a typical picture of the way targeted phishing in SBMs. Please keep in mind this analysis is conducted after the incident. Do not assume the employees had any email security experience or knowledge.

Stage 1 – Targeting and Spoofing

As a routine work, the company's salespersons will check new emails and reply to them promptly. As usual, one of the salespersons opened the email as in Figure 2 (Appendix).

After reading the email, the salesperson first checked the records and found that this is a new customer inquiring technology transfer and was replied a week ago. The salesperson hoped this would be a promising customer. With English as a second language and limited computer knowledge, it will be impossible for the salesperson to consider this message as a fraud. The link? What about the link? The company sometimes also enclosed product brochure link in the email.

To write such an email, the phisher has to know the specific business domain knowledge. They targeted economic developing countries such as China and India. China is the world "supply center" and grows fast in manufacturing and exporting. As of June 30, 2012, one of China's business-to-business marketplaces named Alibaba had 29.4 million registered users from more than 240 countries and showcased 2.5 million supplier storefronts. After get the targeted companies, the phisher crafted this email with fake contact information and a LINK, started the initial phishing attempt.

Stage 2- Set up Forged Website to Collect Credential Information

Nothing unusual, the salesperson clicked the link and was taken to a website asking for user name and password (Figure 3, Appendix). Without a second thought, the salesperson input the emails account's login information on this neat page with beautiful pictures. The salesperson did not pay attention to the long subdomain name and the inconsistent company information between the domain name, page tile and page footer. The salesperson even only found that after typed in user name and password, nothing happened. So the salesperson replied the phisher and reported this technical issue.

Stage 3 - Configure the Email Setting for Long-term Access

The salesperson is still patiently waiting and expecting to see the reply from the phishing for the product requirements or specification. The salesperson did not know the phisher had login the email account and was busy for transferring out all email records including all customer information and transaction records and all attachments. Of course, the salesperson did not understanding the consequence of phisher had done on the email setting. They configured the email setting and open the back door for long-term access.

Stage 4 – Twin Phishing

In this case analysis, it is assumed the supplier's email account is phished successfully first. They may search the customers that had or having financial transactions by using keyword such as Invoice, Orders, T/T etc. With this target list, repeated step 1-3 above. If any one of targeted customers is phished, they can start the next step to start the transaction clone phishing and manipulation.

Stage 5 – Set up New Email Accounts for Clone Phishing

Figure 4 (Appendix) shows the communication schema between email phisher and the two business parties.

For the company (Party A), they have one customer (Party B) who had started business relationship two years ago. Recently, they have discussed an important order (more than100,000usd value) over a month. It is time to finalize the contract. The communication between the two parties is direct and normal (in green color). Unfortunately, this customer became one of the victims. After phished, the communication between the two parties becomes indirect and torqued. Their messages were cloned and spoofed without knowing.

As usual, the salesperson received an email on July 14. The customer indicated the contract price is accepted and asking for PI. The salesperson is happy and enjoy the success of new sales order. Thus, the salesperson clicked the reply button as usual and drafted the email. Before the send button clicked, the PI is attached. A regular PI includes customer contacts, order information, payment terms and method as well shipping inforlation. The saleperson expected the customer will receive the PI and make the payment accordingly, but never realized that this email is cloned by phisher and the communication with phishers is just started.

Now the phisher communicated with both parties and play a role as a middleman. However, this middleman would not merely clone the messages back and forth. He may delay and manipulate the message.

What happened is the phisher created two fake emails addresses. One is for Party A and one is for Party B (Table 1, Appendix). Then the phisher will configure the fake address for Party A in the Reply_to section for messages send out from Party A; and configure the fake address for Party B in the Reply_to section for messages send out from Party B. In this way, the actual receiver is the phisher, not the business partner.

The employee may also noticed that the two different emails address in the From and Reply section in Figure 5 (Appendix), but so what? They had got used to the different emails in the multiple forward and CC section.

Stage 6 – Controlling and Manipulating

During this stage, the salesperson keeps sending email to the customers asking for the bank slip for the payment, but almost no response. In a period of 5 weeks, the salesperson sent 5 such emails, it is not surprised for no response from the customer if that salesperson knew all the messages sent was received by the phisher, not the real customer. On the other hand, from the customer perspective, they kept receiving from the partner's email address and they never noticed the different reply address either. What the customer received is spoofed or forged one. Of course, they did not know their messages never reached to the real business partner.

Actually, the company's email communication with the customer was completely controlled by and under disposal of the phisher (Figure 6, Appenidx).

The phisher had configured the Send-Email address so that the phisher can select any email address (including the business partner's email address) to the receiver. Figure 7 (Appendix) shows how to configure the settings (A) and how to use the function to send message (B).

Stage 7 – Intervening business transactions and Create bank account.

By manipulating the transaction, the attack will not end until the phisher see the money. Considering the confidentiality, complexity, and large quantity of the communication, the detailed records are not presented here. Following are two excepts (Figure 8 A and B, Appendix) from the emails received by the customer asking them to change the bank information of fund transfer. However, to do this, the phisher has to set up a temporary business bank account first, which usually takes longer time and more documents to apply. This requires expertise and not everyone is familiar with the process of international telegram transfer.

From the last email message (Figure 9, Appendix), we can see the whole phishing process is successful. Now they are happy and excited because of the successful plot and schema. Once they get the money, they will run away and leave the rest of the world crying, blaming and figuring out the process.

After this incident, all the phishing emails were analyzed carefully for forensic purpose, special attentions was paid to the email headers. The detailed email header data are in plain text format. This data shows the routing information on the email's path. The data is presented in reverse chronological order, meaning the info at the top is the most recent event. Examining the headers of this email we can see several things, including the sender's email software name, IP address and timestamp, destination server name, IP address and timestamp. Each hop shows detail about the IP address and respective reverse DNS name.

The result from this analysis shows that the phisher sometimes sent emails from a country in Africa, and then routed to Chicago, and then sent back to China. Sometimes, the email was launched from Russia, routed to Mexico, then to Singapore, finally to China. Apparently, the email routing path is not fixed; it can be relayed from anywhere in the world. This uncertain routing path also increases the attack detection difficulties.

6. Summary

From previous discussion, a scenario of targeted email phishing for small business can be described as below.

Phishers pretend potential customers and offer the opportunity for new orders. They get the business email login information by asking them click some links in the email. The link will guide victims to a counterfeited web site for signing in. Upon collected the login information, the phishers will get into the server or email account to get all customers information. What's worse, several online services or accounts may be compromised because people tend to use the same password across different systems. Then they can play the roles to both the company and their customers by manipulating transaction information, including the bank account information. Thus email phishing is very difficult to prevent and the cost can be very high. Generally, the cost

can be the directly financial loss from transactions, it will cost more on the damage to the relationship and trust with customers.

7. Conclusion

This study explored the process and characteristics of email phishing in SMBs. Our discussion is supported by an analysis of case of small international trading company. We found that the new trend of email phishing in SMBs is characterized as targeted, multi-staged, cross country team work. Understanding of the phishing process and these characteristics is very important to develop effective counter-measures to protect the information asset of SMBs from attack. The result from this study and the enclosed business email phishing case can be used as email security training or education materials.

As any exploratory case study, the limitation with this study is the sample size. Because of it is an emerging topic, more studies are necessary. Future studies will focus on following areas.

1. Design anti-measures and strategy in the multi-stage process.

Studies show that well designed user security education can be effective (Kumaraguru et al.). Web-based training materials, contextual training, and embedded training have all been shown to improve users' ability to avoid phishing attacks (Sheng et al.). Thus for the training and education purpose, online multi-stage, context-based training strategy should be investigated.

2. Understand why employees fall for the victim of email phishing by studying from the perspective of social, psychological and behavioral theories. Specific characteristics including age, gender, education, knowledge of phishing or online habits were analyzed to determine their impact on the participant's ability to identify legitimate or fraudulent email messages (Martin). Also there are some studies have tried to identifying the factors influencing a user's ability to categorize email, but very few of answer and explain why and what are the reasons that induce the users fail to make a wise decision.
3. Understand the different impact or victimization of email phishing by cross culture, language and industry.

References

DBIR, Cisco . Data Breach Investigations Report (DBIR) *, 2011,* Email Attacks: This Time It - Cisco at http://*www.cisco.com/en/US/prod/collateral/.../targeted_attacks.pdf*

Downs, Julie S. ; Holbrook, Mandy ; and Cranor, Lorrie F., "Behavioral response to phishing risk" (2007). Institute for software research. Paper 35. http://repository.cmu.edu/isr/35.

FireEye, Spear Phishing Attacks: Why They are Successful and How to Stop Them http://www2.fireeye.com/wp_spearphishing.html?x=FE_HP_SB, 2012

Hong, Jason (01/2012). "The state of phishing attacks". *Communications of the ACM(0001-0782)*, 55(1), p.74.

InformationWeek (2011). Epsilon fell to spear-phishing attack. online. April, 2011.

Jain, A; Richariya,V. Implementing a web browser with phishing detection techniques, World Comput Sci Inf Technol J. 1(7):28–291 (2011)

Kumaraguru, Ponnurangam (05/2010). "Teaching Johnny not to fall for phish". ACM transactions on Internet technology(1533-5399), 10(2), p.1.

Martin, Tim. "Phishing for answers: Factors influencing a participant's ability to categorize email." Comput. Changing World, Portland, OR (2009).

Markus Jakobsson and Steven Myers. Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons, Inc., 2007.

Milne, Andrew. Size Isn't Everything: Frequency of SMB Targeted Attacks Growing. http://www.secureworks.com/media/blog/general/frequency-of-smb-targeted-attacks-growing/, 2012.

Richard,C.O.; Hintau, A.J. Phishing as a Hazard to E-Business, International Journal of Computer and Internet Security, Vol4, No. 2, 2012, pp. 59-63

Salem, O; A Hossain, M Kamala, Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks, The 10th IEEE International Conference on Computer and Information Technology, Bradford, West Yorkshire, UK, 2010

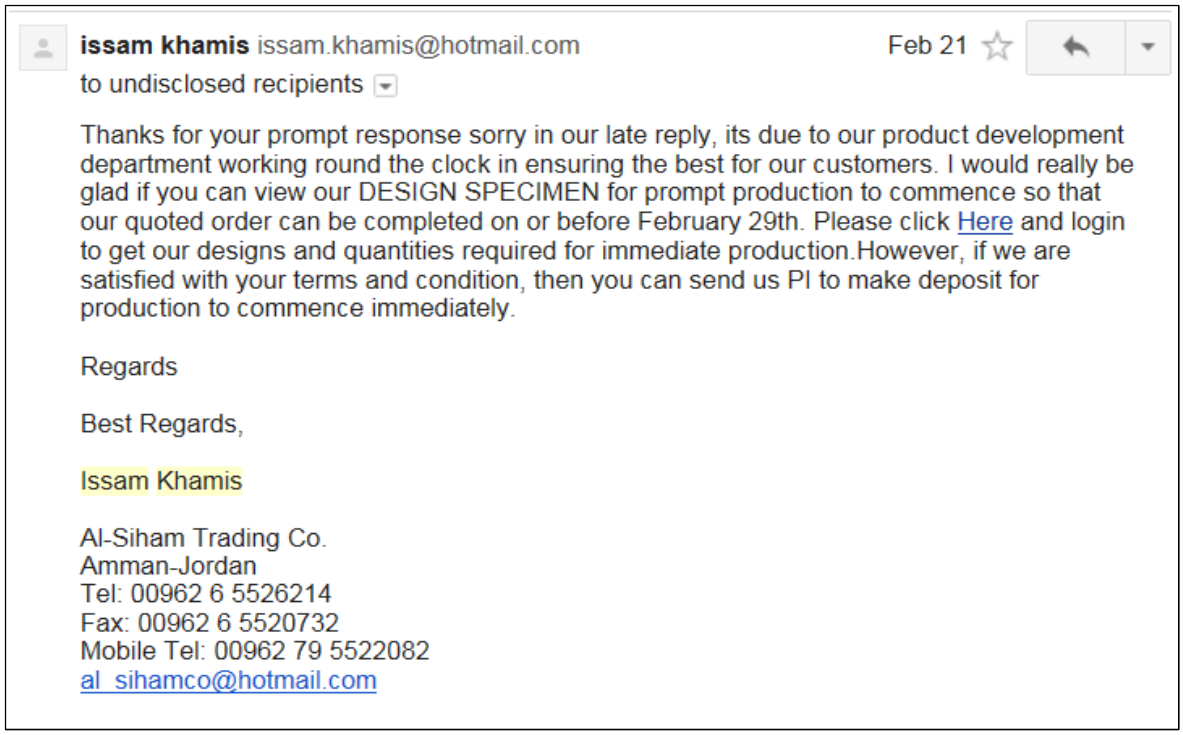
S Sheng, B Magnien, P Kumaraguru Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish- Proceedings of the 3rd …, 2007

Wang, J., R. Chen, T. Herath, A. Vishwanath, H. R. Rao. Forthcoming. "Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email." IEEE Transactions on Professional Communication.

Appendix

Example of a Typical Campaign	Mass Phishing Attack (Single Campaign)	Spearphishing Attack (Single Campaign)
(A) Total Messages Sent in Campaign	1,000,000	1,000
(B) Block Rate	99%	99%
(C) Open Rate	3%	70%
(D) Click Through Rate	5%	50%
(E) Conversion Rate	50%	50%
Victims	**8**	**2**
Value per Victim	$2,000	$80,000
Total Value from Campaign	**$16,000**	**$160,000**
Total Cost for Campaign	$2,000	$10,000
Total Profit from Campaign	**$14,000**	**$150,000**

Figure 1 Economics of Mass Phishing vs. Spearphishing Attacks
(Adopted from Cisco Report, 2011)



issam khamis issam.khamis@hotmail.com Feb 21

to undisclosed recipients

Thanks for your prompt response sorry in our late reply, its due to our product development department working round the clock in ensuring the best for our customers. I would really be glad if you can view our DESIGN SPECIMEN for prompt production to commence so that our quoted order can be completed on or before February 29th. Please click Here and login to get our designs and quantities required for immediate production.However, if we are satisfied with your terms and condition, then you can send us PI to make deposit for production to commence immediately.

Regards

Best Regards,

Issam Khamis

Al-Siham Trading Co.
Amman-Jordan
Tel: 00962 6 5526214
Fax: 00962 6 5520732
Mobile Tel: 00962 79 5522082
al_sihamco@hotmail.com

Figure 2 Sample of Initial Email Phishing Attempt

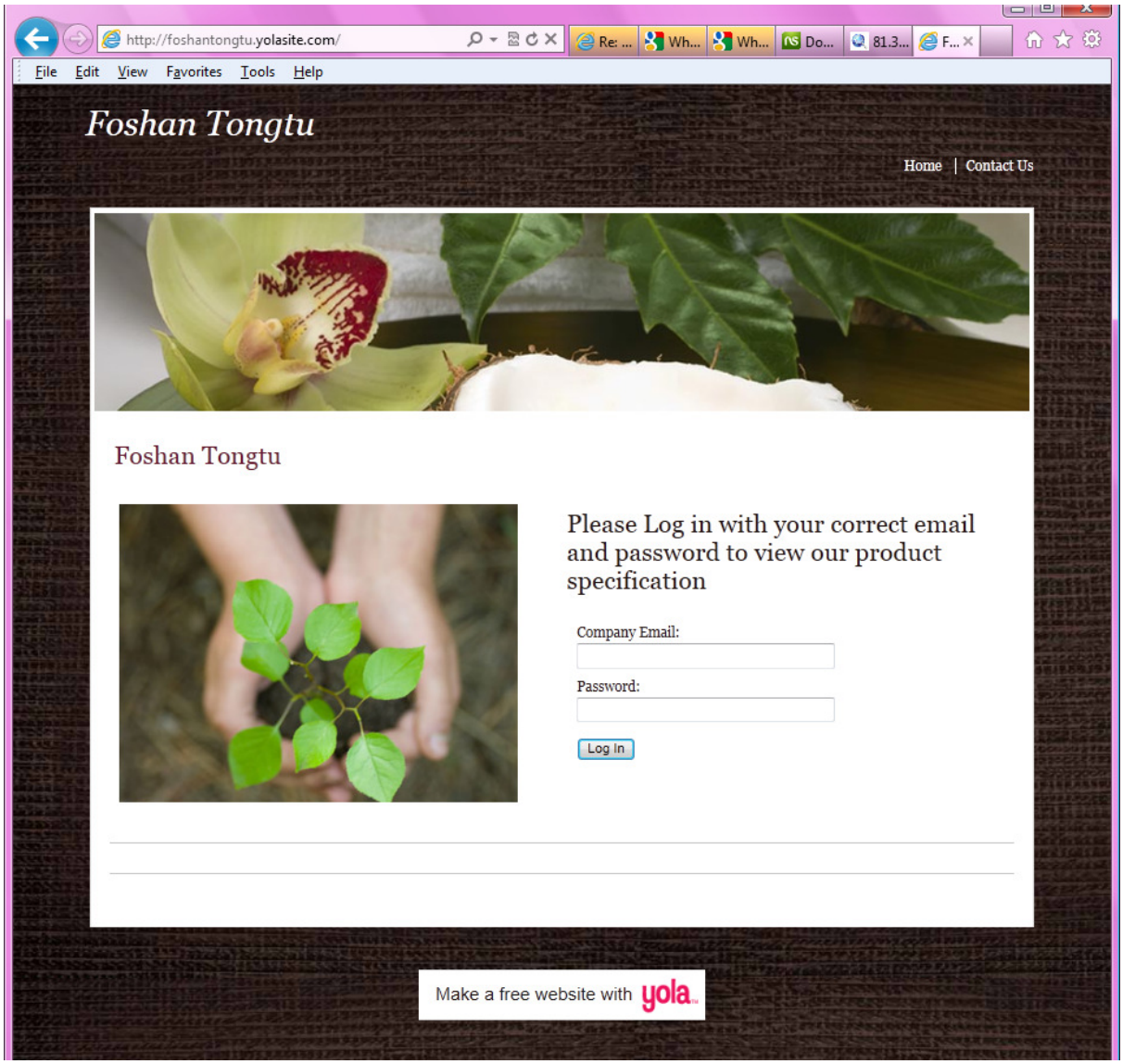


Figure 3 Sample of Forged Website Design for Colleting Credential Information

Table 1 Sample of Spoofed Email Address for the Parties Involved

	Actual address	Fake address
Party A	intl@mohoindia.com	mohoindiaintl@gmail.com
Party B	export@rtc-co.com	Export-rtc-co@hotmail.com

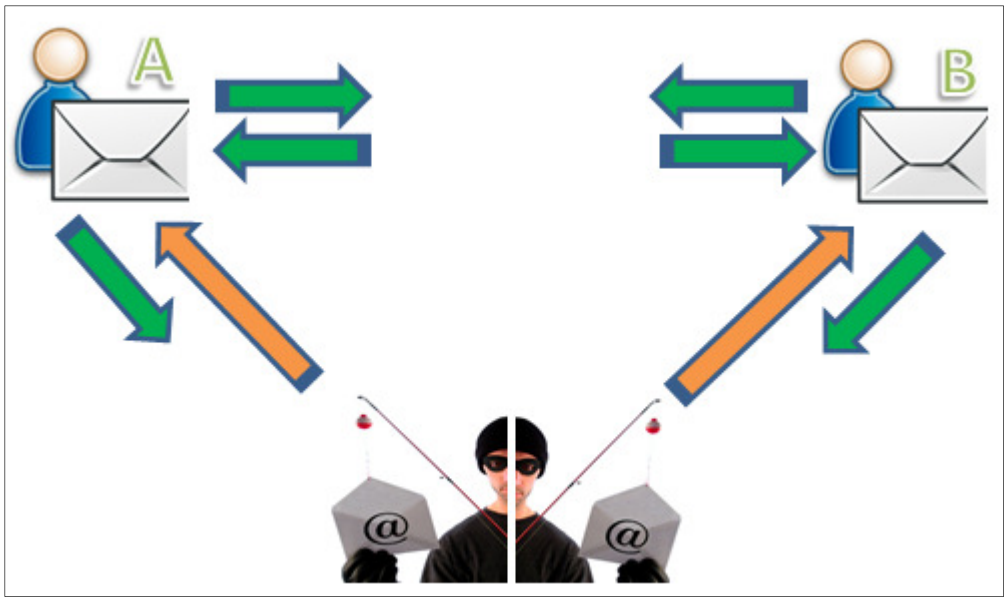


Figure 4 Communication schema for Clone Phishing

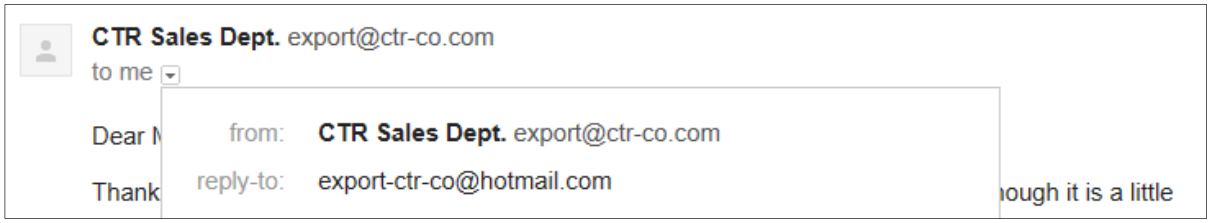


Figure 5 Sample Spoofed Email Heading

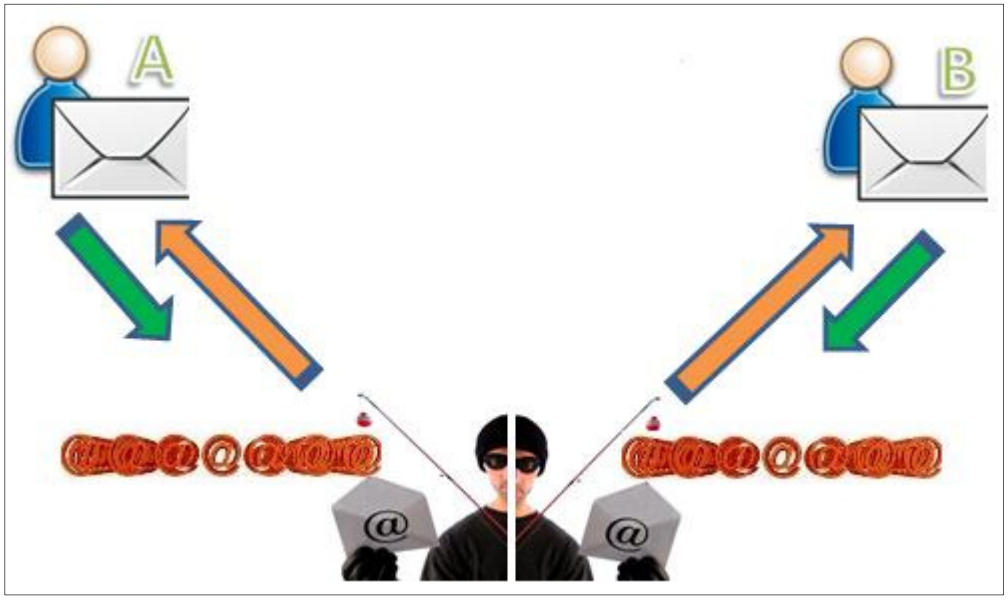


Figure 6 Communication Controlled by Phisher

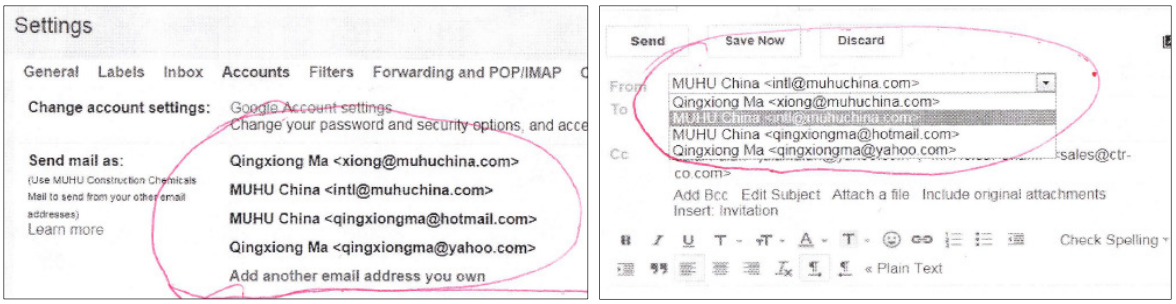
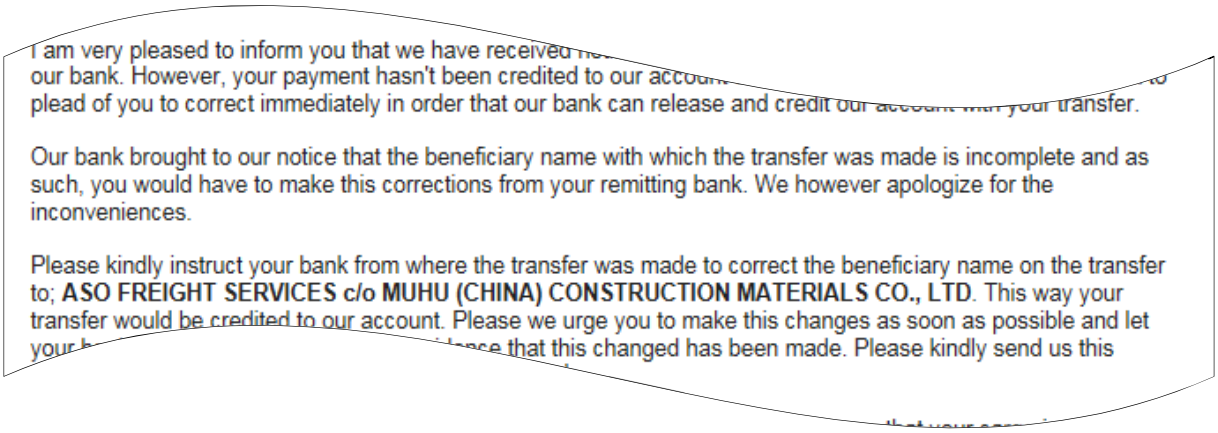


Figure 7 Alternate Sending Email Address (A) Alternate Sending Email Address (B)

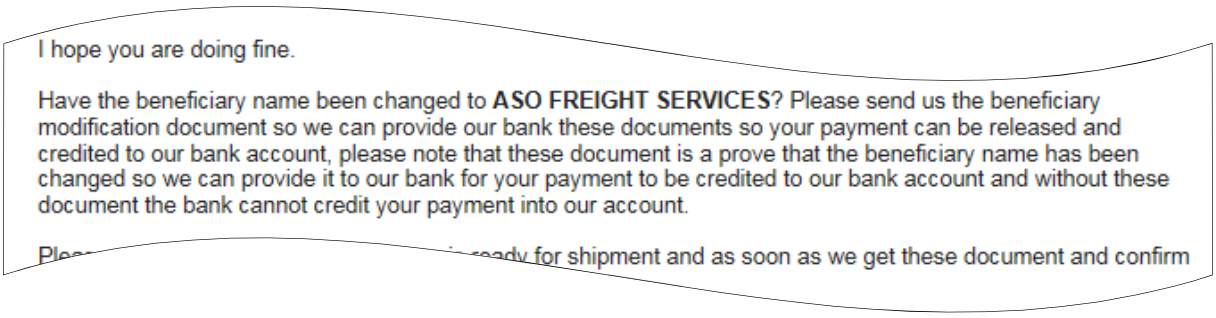


I am very pleased to inform you that we have received
our bank. However, your payment hasn't been credited to our
plead of you to correct immediately in order that our bank can release and credit
transfer.

Our bank brought to our notice that the beneficiary name with which the transfer was made is incomplete and as such, you would have to make this corrections from your remitting bank. We however apologize for the inconveniences.

Please kindly instruct your bank from where the transfer was made to correct the beneficiary name on the transfer to; **ASO FREIGHT SERVICES c/o MUHU (CHINA) CONSTRUCTION MATERIALS CO., LTD**. This way your transfer would be credited to our account. Please we urge you to make this changes as soon as possible and let your
that this changed has been made. Please kindly send us this

Figure 8 Examples of Intervene the Business Transaction (A)

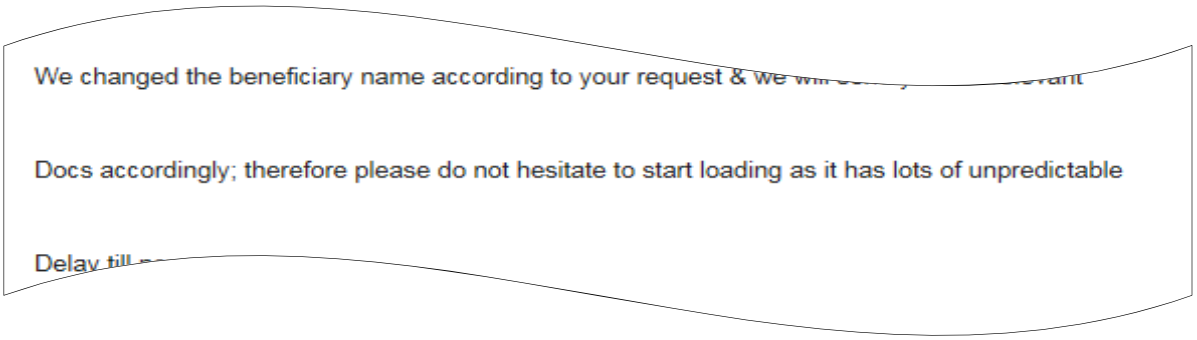


I hope you are doing fine.

Have the beneficiary name been changed to **ASO FREIGHT SERVICES**? Please send us the beneficiary modification document so we can provide our bank these documents so your payment can be released and credited to our bank account, please note that these document is a prove that the beneficiary name has been changed so we can provide it to our bank for your payment to be credited to our bank account and without these document the bank cannot credit your payment into our account.

Ple
ready for shipment and as soon as we get these document and confirm

Figure 8 Examples of Intervene the Business Transaction (B)



We changed the beneficiary name according to your request & we

Docs accordingly; therefore please do not hesitate to start loading as it has lots of unpredictable

Delay till

Figure 9 Examples of Message showing the Phishing Succeeded