International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.247-256
http://dx.doi.org/10.14257/ijsia.2016.10.1.23

Phishing Attacks and Defenses

Junaid Ahsenali Chaudhry [1], Shafique Ahmad Chaudhry[2], Robert G. Rittenhouse[3*]

[1] *Department of Computer Science, Innopolis University, Kazan, Russia*
[2] *Department of Computer Science, Dhofar University, Oman*
[3] *Department of Computer Engineering, Keimyung University, Daegu, Republic of Korea (corresponding author)*
[1]*j.chaudhry@innopolis.ru*, [2]*shafique@du.edu.om*, [3]*rrittenhouse@acm.org*

Abstract

A phishing attack is a method of tricking users into unknowingly providing personal and financial information or sending funds to attackers. The most common phishing attacks use some form of electronic messaging such as email to provide a link to what appears to be a legitimate site but is actually a malicious site controlled by the attacker. Phishing is a hybrid attack combining both social engineering and technological aspects and combatting phishing attacks requires dealing with both aspects

Keywords: *Phishing, cyber security, community computing, cybercrime*

1. Introduction

This paper is a revised and expanded version of a paper entitled "Phishing: Classification and Countermeasures" presented at The 7th International Conference on Multimedia, Computer Graphics and Broadcasting, Jeju Korea, November 25, 2015 [1].

Phishing is a form of cybercrime that aims to deceive users into providing personal and/or financial information or to send money directly to the attacker. A phishing attack is generally initiated via some form of message which includes a link to a deceptive domain name which appears to be a legitimate site but is actually controlled by the attacker. The term phishing was first used in 1996 and phishing has continued to grow and evolve since then as shown in Figure 1 [2].

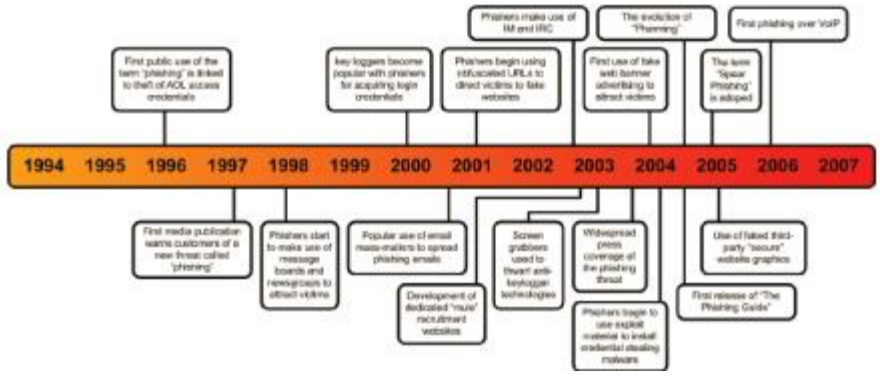

Figure 1. The Evolution of Phishing [2]

[*] Corresponding Author

ISSN: 1738-9976 IJSIA

Phishing began in the early 1990s as a way for hackers to obtain America Online (AOL) accounts. In the early 1990s AOL would create an account whenever a valid looking credit card number was entered. In the middle of the decade AOL began to verify the credit card information entered so hackers began to steal existing AOL accounts by posing as AOL employees and tricking the victim into divulging their username and password information [3].

Phishing is no longer limited to email to but may also be carried out through voice messaging, SMS, instant messaging, social networking sites, and even multiplayer games [4]. The aim is to deceive the victim into visiting the spoofed site, which appears identical to the original one, and make the user feel comfortable entering a username and password or other personal information. A phishing site is generally created to acquire personal information such as credit card numbers; personal identification numbers (PINs), social security numbers, banking numbers, passwords, *etc*. or to install malware on the victims computer Phishing began as email. It has since spread to include SMS and instant messaging, message boards, banner ads on websites, voice messaging, social media sites such as Facebook, and even multiplayer games. Figure 2 illustrates some of the different communication media, potential payloads and purposes of Phishing [2]

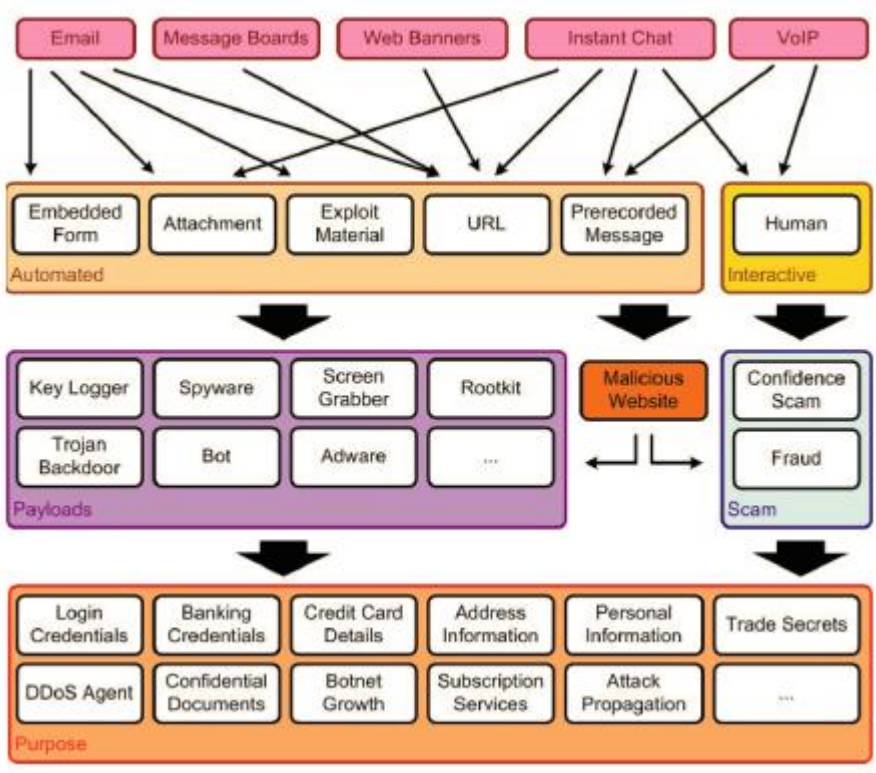

Figure 2. The Methods Used in Phishing

According to the Anti-Phishing Working Group (APWG) phishing activity trends report 2014 [5], during the 4th quarter of 2014, a record number of malware variants were detected – an average of 255,000 new threats each day. It is also reported that 197,252 unique phishing reports were submitted to APWG during that time showing an increase of 18 percent from the third quarter of the same year. Gartner estimated 57 million adults in the United States received phishing attacks in 2004 and approximately 19 percent followed a link contained in a phish email with 3 percent giving the phisher sensitive financial or personal information [6].

A 2006 study [7] found:

- Phishing websites may fool up to 90% of visitors
- Existing anti-phishing browsing cues are often ineffective. Twenty-three percent of those studied did not look at security indicators displayed
- Warnings about fraudulent certificates were also ineffective: The majority of participants in the study proceeded without hesitation when presented with warnings.

The procedures and techniques used in phishing constantly evolve. The attackers, often rich in technical understanding of computer communications and well versed with the target system procedures, protocols, and common casual habits of its users, develop new methods of bypassing security protocols and evading detection in order to increase the chances of a successful attack. In addition to user inability to detect phishing attacks, the frequency of attack and diversity in attack methods also helps improve the chances of successful attacks. Technological advances and newly found vulnerabilities also play a major role in assisting the success of phishing attacks. It is not surprising that even well trained end users failed to detect 29% of phishing attacks [8]. Untrained users can be expected to detect even fewer attacks.

Early phishing emails and sites were crafted by the attacker and often easily detectable. Phishing websites today are created with toolkits that let a phisher specify what legitimate page to copy and where to direct stolen data, then generate all needed content [4]. One interesting finding of this research is that these phishing kits often hide backdoors through which the phished information is sent to recipients other than or as well as the intended ones. Phishing today is an industry. Phishing toolkits and associated malware are available for free or purchase. There is also a ready market for information obtained from victims [3].

Phishing is not only a technological problem. It is also a social engineering attack that aims at exploiting vulnerabilities in the overall system and is facilitated by users. These vulnerabilities can be used by the attackers to construct more convincing scams. It is therefore essential to counter phishing at both the technical and social aspects.

The remainder of this report is organized as follows: in section 2, we discuss the formal threat landscape. We discuss related work in section 3 and in section 4 we propose countermeasures to mitigate the phishing problems.

2. Problem Description

Phishing relies on a masquerade where attackers disguise themselves as someone else and, based on the reputation and human level relationships with the target, try to uncover information. Some argue that phishing is a social science problem because the attacker uses social engineering tools to exploit the victim. Others would counter this argument by noting that it requires technical knowledge of the system that victim is using, bypassing the security measures, and making your message look credible in order to gain victim's attention. For classifying the attack vector, we look at the problem through both social engineering as well as technical perspectives.

A typical phishing attack consists of three key components: lure, hook, and catch [3]:

- **The lure** is most commonly an email message that appears to be from a legitimate organization such as a bank or internet service provider the message contains a link to the hook. The hook is often hidden by obfuscating the URL.
- **The hook** is a website that mimics the site of the legitimate institution which the victim or phish is willing to divulge confidential information to.
- **The catch** involves the phisher making use of the collected information.

Social engineers exploit curiosity, fear, and empathy factors plus traditional phishing techniques to trick the users into becoming phishing victims [9].

- **Curiosity** is the desire to stay informed. It can be exploited by sending an e-mail that might contain a link to watch a video about the latest news stories. The destination link will then lead the user to a malicious site.
- The **Fear** tactic is used to persuade the users to act in a certain way by instilling fear. For example, an email purportedly from the bank telling user to validate his/her information because his/her account might have been breached could cause the user to enter personal information in a malicious site. Similarly a user might be asked to verify a nonexistent charge to an account or that attempts had been made to log in to the account [3]
- To exploit **Empathy** towards others, hackers generally impersonate a friend or relative, claiming a dire need for money or exploit a tragedy such as. the earthquake and tsunami in Japan.

A phishing attack typically employs a number of technical tricks to make it more convincing [3]. These include:

- Using trademarks, logos and images associated with the organization the phisher wants the victim to believe is the originator of the message. Many victims do not realize how easily these can be copied
- In some cases the phishing email has actually included the advice that users should not click on email links. This does make the message look more authentic and clearly many users will click on embedded links anyway.
- Email spoofing to change the apparent sender of the message. Most victims do not realize how trivial it is to spoof an email address.
- URL hiding and encoding
- It is even more convincing if the message originates from someone the user knows [10].

Phishing attacks cover a diverse range of techniques. One troubling development is the increase in **Spear phishing,** email targeted at particular individuals or groups, rather than spamming random users. Spear phishing is generally preceded by the attacker researching the potential victims and setting. The attacker can then send a message appearing to be from a legitimate source. Spear-phishing is also being used against high-level targets, such as corporate executives or government officials, in a type of attack called "**whaling**" Social media may be used for research on victims. In one study 72 percent of users responded to a forged phishing email appearing to be from friends [10].

In **clone phishing** a previously delivered legitimate email is used to clone a malicious email. The malicious email will typically contain a link to the phisher's website. Such links are often obfuscated by either by substituting similar characters such as 0 (zero) for O (capital o) or by using Unicode UTF-8 characters encoded as escape sequences [2, 11].

Malware-Based phishing refers to attacks that result in installing and running malicious software on users' computers. Generally malware is introduced as an email attachment which is downloadable. Malware commonly installed in phishing attacks includes key loggers and screen grabbers, spyware that captures and logs keyboard input or screen displays and sends information to the phisher. In other cases control of the victim's computer is the goal of the attack. The computer can then be used for further phishing attacks particularly on the victim's acquaintances, to send spam or participate in a denial of service attack.

Malware can also be used for **Session Hijacking** where a user's online activities are monitored until an authenticated session with a particular account is established. Once the connection is established, the malicious software takes over and can perform unauthorized actions, such as transferring funds, without the user's knowledge.

Phishing attacks often direct users towards **Web Trojans** or clone websites which operate when users are trying to login. These Trojans can capture credentials and send

them to the phisher. The sites may will typically include copied graphics and may even include realistic appearing SSL padlocks and third party verification services [2].

In **Search Engine Phishing** hackers create bogus websites and get search engines to index them. A search through a search engine guides victims to these bogus sites where they might end up giving personal information while believing they are accessing the genuine site. There are black hat search engine optimization kits available that can quickly enable a bogus site to rise in search engine rankings. Nonetheless, given the time lag between when a website is created and when it is accessed this is typically employed to direct users at malicious sites [12].

Several types of attacks are directed at the user's computer or internet connection rather than the user. These include system reconfiguration attacks and pharming. These are purely technological attacks that don't involve social engineering and it is questionable whether they should really be considered phishing.

System Reconfiguration Attacks modify settings on a user's PC for malicious purposes. For example: URLs in a favorites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "bankofabc.com" to "bancofabc.com" which might be authenticated by a new root certificate installed on the user's computer.

DNS-Based Phishing ("**Pharming**") modifies host files, which are used to subvert the Domain Name System (DNS). In this scheme the host files on a victim's computer or DNS used for searches are tampered with. As a result requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site. As a result users can enter potentially confidential information to bogus sites.

2.1 Defenses

We believe the problem of phishing has to be tackled by following a heuristic approach, which includes User Education, Technological enhancements and Process Engineering.

User Education: Since the user's capability and analytical skills while using the electronic communication channels hold a pivotal position in phishing attack recognition, a strong emphasis is given to user training and education. It is worth noting that phishing attacks normally are at the peak of their effectiveness during the initial few hours of the attack. Since phishing attacks normally target multiple users from the same or different organizations, sharing knowledge in alerting others of the phishing attacks becomes as important of a matter as attack recognition itself.

Software/technological enhancement: Various anti spamming software is sold in the market that claim high success rates of filtering spam messages. In reality, they might be successful in filtering out the infamous "Nigeria Prince Scams" but yield to more sophisticated phish-craft. Firewalls and filters are effective in fixed source spam communication which may be handled by blocking sources and maintaining blacklists but the modern day phishing environment is more complex

Process Engineering: The knowledge learnt from phishing can help fine tune business processes and eliminate authentication loopholes in procedures. The business processes should be engineered in a way that appropriate checks and balances are kept in place and user's informed judgment is backed up by the process level support, multiple checks in a distributed chain of command, online and offline verification, preemptive and post-emptive supply chain is enforced *etc*.

3. Related Work

Phishing victims often do not realize that they have been tricked. The first phase in combating phishing problem is the detection of a phishing attack. We classify these detection methods in two categories: human detection and machine detection.

3.1 Human Detection

All technology users are not the same. Some are more knowledgeable about security issues and some think longer before they click on a suspicious link. Users may receive training at work but otherwise most internet users are not particularly knowledgeable. Within an organizational setting common operational procedure, knowledge sharing, and double verification processes can reduce problems. Most technology workers are not familiar with the user interaction model of the information systems that they use. Hence it becomes easier for the phishing attackers to mimic the web interface of some familiar webpage and lure the user to enter their private information that is then transmitted to the attackers

An overview of phishing education is presented in [13]. This work focuses on context aware attacks and introduces a strategy for educating users by combining phishing IQ tests and class discussions. However not all potential victims have the advantage of formal classroom training and simply presenting the information in an email or a webpage is of limited effectiveness [14]

To explore the effectiveness of embedded training, researchers conducted a large-scale experiment that tracked workers' reactions to a series of carefully crafted spear phishing emails and a variety of immediate training and awareness activities [15]. Based on behavioral science findings, the experiment included four different training conditions, each of which used a different type of message framing. The results from three trials showed that framing had no significant effect on the likelihood that a participant would click a subsequent spear phishing email and that many participants either clicked all links or none regardless of whether they received training. The study was unable to determine whether the embedded training materials created framing changes on susceptibility to spear phishing attacks because employees failed to read the training materials.

Anti-Phishing Phil [16] is an online game that teaches users good habits to help avoid phishing attacks. It was designed according to learning science principles. During a study participants who played the game were better able to identify fraudulent web sites. Again, however, such training approaches are only useful if potential victims take the training.

Another study reports findings from a multi-method set of four studies that investigate why we continue to fall for phishing attacks [17]. The study found that phish are becoming more effective and that the use of logos in a phish email makes it more convincing.

Hale *et. al.* [18] examined another game based approach that seeks to incorporate learning techniques and combines the realism of in-the wild approaches with the training features of testing. This work proposes a three phase experiment to test the approach on a customized Cyber Phishing simulation platform.

Machine Detection:

In order to detect either traditional or spear phishing it is important to identify phishing emails. Various approaches have been proposed to enhance classification accuracy of phishing emails. In [19] the authors study the selection of an effective feature subset out of existing proposed features by evaluating various feature selection methods. Their system displays high accuracy while relying on a relatively small number of classifiers. In [20] a two dimensional approach to detect phishing emails is presented. The proposed framework called PhishSnag, operates between a user's mail transfer agent (MTA) and mail user agent (MUA) and processes each arriving email for phishing attacks even before reaching the user’s inbox. The authors claim a detection rate of 93 percent with about 0.5 percent false positives or over 99 percent with a higher level of false positives. Their scheme relies on detecting that unlike conventional emails which gives information in a passive manner, phishing emails seek to actively misdirect the victim.

Two algorithms, Adaline and Backpropagation, are presented in [21] which work along with a support vector machine to enhance the detection rate and classification of phishing attacks. Both algorithms have over a 99 percent detection rate.

Another detection and classification technique identifies suspicious web pages, based on the literal and conceptual consistency between the URL and web contents. PhishStorm [22], is an automated phishing detection system that can be used to analyze in real time any URL in order to identify potential phishing sites. The approach achieves 98% accuracy.

MobiFish, a novel automated lightweight anti-phishing scheme for mobile platforms, verifies the validity of web pages and applications (Apps) by comparing the actual identity to the identity claimed by the web pages and apps [23]. Mobifish consists of two applications: WebFish for checking web pages and AppFish for checking applications. In testing WebFish found 100% of pages checked and

In another study authors use the EMCUD (Extended Embedded Meaning Capturing and Uncertainty Deciding) method to build up phishing attack knowledge according to the identification of phishing attributes [24].

In [25], a system for client-side protection of banking sites is proposed. The system relies on the website structures and features (*i.e*. bank name, branch name, base URL, address) represented in RDF format to decide on its legitimacy. These systems can then be tested using a central database maintained by the relevant government.

4. Discussion: Phishing Countermeasures

There is no silver bullet to tackle the issue of phishing. However, we can adapt to better cyber hygiene that will make phishing harder to achieve. Bringing maturity into information sharing protocols will also go a long way in minimizing the damages inflicted by phishing campaigns.

In the following passages, we identify the critical areas of improvements and recommend immediate and gradual development practices. We divide our discussion into client-side tools and policies that help protect users from phish attacks and server-side tools and policies that web sites can apply.

4.1. Client-Side tools

Password Management: Users commonly choose passwords casually to be easy to remember and often use the same password across multiple sites. Users should be encouraged to use different passwords generated and managed by a password management system. The password generation system could check for password reuse. While this will not prevent capture of login credentials for a single site it should limit the damage.

Electronic Communication Filtering: Electronic content filtering should be adopted which filters the contents of the data exchanged on corporate networks. The data should be encrypted as a mandatory practice in order to ensure integrity of the data, prevent data poisoning, and to reinforce the trust on own data. Anti-phishing systems should be set up that filter messages and make recommendations about the trustworthiness of a message.

Firewalls and Filters: Firewalls and filters go a long way in reducing the volume of the "known" phishing scams. They can be an effective tool in reducing the number of phishing messages the user receives.

Antivirus and Anti-malware Technologies: In many ways, phishing can be achieved with an "anchor" at the user terminal in the form of malware. Antivirus technologies are somewhat effective in eradicating phishing payloads from the end user terminal and strengthening endpoint security. Many anti-virus programs also provide warnings about suspicious websites. Browsers are also more likely to warn users when they are entering data into a website that is not secured by SSL. This makes it much more difficult for

phishers to set up bogus websites to collect information. Unfortunately, because SSL allows any certificate authority to certify any website [26], it is not impossible for bogus websites to have legitimate security certificates. Some browsers also warn about links that have been reported as malicious.

Digital Certificates: Within an organization Certificate Authorities (CA) should be established to ensure trust between the end user and webpages. Dedicated keys should be provided to the users of an organization in order to do secure transactions online.

Secure Email Protocols: It is of utmost importance that the email protocols among the organizations be revised so that the identity of the sender of the email is somewhat ensured to the receiver because without it both the user training and the technological revisions shall be of little use. Due to flaws in email protocols, it is not hard to fake identity of anyone. There have been some solutions that heuristically verify the identification of email senders but email spoofers devise newer ways to trick those systems. Organizations should use cryptographically signed email internally.

Communication: Once a phishing scam is exposed, the related companies whose identity is used in that scam should communicate with their customers and stakeholders about the scam. This is to contain the proliferation of the scams and prevent the users of information systems at the stakeholder's end from giving up their credentials to the attackers.

Preparedness: In the modern cyber world, security breaches can happen to any organization. Therefore, it is important that post breach procedures are in place detailing what to do if (when) a breach happens and to minimize the losses resulting from that breach

Counter phishing and Law Enforcement Support: An organization wide conscious effort has to be put in and a specialist facility established to handle phishing, scams, fraud, and malware mitigation.

Education and Training: By far the most important components of fight against fishing measures is education and training. The end users of the corporate systems should be trained in identification of phishing messages. This will help in not only in identification of phishing messages, it will also provide priority feed to the information security knowledge sharing portal that we highly recommended be set up for secure knowledge sharing.

4.2 Server-Side Protection

Authentication Procedures: Single factor authentication needs to be replaced with either two-factor authentication or with multi-factor authentication (whichever is cost effective). Unfortunately, there is a risk that overly intrusive security procedures may alienate users. These procedures should be revised and renewed frequently in order to match the pace of the anti-security research and development industry.

Site Personalization: One simple technique that websites can use to help safeguard users is personalization. Users can select an image that is shown after their username is entered and before they enter passwords.

4.3. Other Players

There is a growing community of security researchers. Organizations would be well advised to join the community and report incidents. The community of trusted users plays an important role in suspicious activities detection and prevention. A member of a trusted community of system administrators upon identification of phishing messages can alert the others in his network to update their blacklists or help in investigating a suspicious message or domains. Law enforcement organizations can also be informed of incidents.

Once a phishing scam is exposed, the related companies whose identity is used in that scam should communicate with their customers and stakeholders about the scam. This is

to contain the proliferation of the scams and prevent the users of information systems at the stakeholder's end from giving up their credentials to the attackers.

5. Conclusion

Phishing will never be completely eradicated. However, the threat can be reduced through a combination of user and corporate safeguards and server-side measures. User education remains the strongest and at the same time, the weakest link to phishing countermeasures. It is also an intellectual contribution to the employee career growth and ultimately to the evolution of the host organizations as safer, phishing free workplaces. Organizations providing web services also have a role to play.

References

[1] J.A Chaudhry, S.A Chaudhry, R.G Rittenhouse, R.G, "Phishing: Classification and Countermeasures", In: The 7th International Conference on Multimedia, Computer Graphics and Broadcasting. SERSC, Jeju, South Korea **(2015)**.
[2] G. Ollmann, "The Phishing Guide--Understanding & Preventing Phishing Attacks", **(2007)**.
[3] M. Jakobsson , S. Myers, "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft", Wiley, Hoboken, NJ, USA **(2006)**.
[4] J. Hong, "The state of phishing attacks. Commun", ACM. vol. 55, no. 74, **(2012)**.
[5] Anti-Phishing Working Group: Phishing Activity Trends Report. **(2014)**.
[6] A. Litan, "Phishing attack victims likely targets for identity theft", Gartner First Take FT-22. **(2004)**.
[7] R. Dhamija, J.D Tygar, M. Hearst, "Why phishing works. In: Proceedings of the SIGCHI conference on Human Factors in computing systems" - CHI '06. p. 581. ACM Press, New York, New York, USA **(2006)**.
[8] S. Sheng, M. Holbrook, P. Kumaraguru, L.F Cranor, J. Downs,"Who falls for phish? In: Proceedings of the 28th international conference on Human factors in computing systems" - CHI ' ACM Press, New York, New York, USA , vol. 10, **(2010)**, p. 373.
[9] E. Earley, "Understanding social engineering", http://www.net-security.org/article.php?id=1403.
[10] T.N. Jagatic, N.A Johnson, M. Jakobsson, F. Menczer, "Social phishing", Commun. ACM. vol. 50, **(2007)**, pp. 94–100.
[11] F. Zhou, "Phishing Sites and Prevention Measures", Int. J. Secur. Its Appl.vol. 9, **(2015)**, pp. 1–10.
[12] F. Howard, O. Komili, "Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware", Sophos Tech. Pap. **(2010)**.
[13] S.A Robila, J.W Ragucci, "Don't be a phish", ACM SIGCSE Bull. vol. 38, no. 237, **(2006)**.
[14] P. Kumaraguru, S. Sheng, A. Acquisti, L.F Cranor, J. Hong, "Teaching Johnny not to fall for phish", ACM Trans. Internet Technol. vol. 10, **(2010)**, pp. 1–31.
[15] Caputo, D.D., Pfleeger, S.L., Freeman, J.D., Johnson, M.E.: Going Spear Phishing: Exploring Embedded Training and Awareness. IEEE Secur. Priv. vol. 12, **(2014)**, pp. 28–38.
[16] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L.F. Cranor, J. Hong, E. Nunge, "Anti-Phishing Phil. In: Proceedings of the 3rd symposium on Usable privacy and security - SOUPS ' ACM Press, New York, New York, USA, 07, **(2007)**, p. 88.
[17] M. Blythe, H. Petrie, J.A. Clark, "F for fake. In: Proceedings of the 2011 annual conference on Human factors in computing systems", - CHI '11. p. 3469. ACM Press, New York, New York, USA **(2011)**.
[18] M.L Hale, R.F Gamble, P. Gamble, "CyberPhishing: A Game-Based Platform for Phishing Awareness Testing", In: 2015 48th Hawaii International Conference on System Sciences. IEEE, **(2015)**, pp. 5260–5269.
[19] M. Khonji, A. Jones, A, Y. Iraqi, " A study of feature subset evaluators and feature subset searching methods for phishing classification", In: Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference on - CEAS '11. pp. 135–144. ACM Press, New York, New York, USA (2011).
[20] R. Verma, N. Shashidhar, N. Hossain, "Two-Pronged Phish Snagging", In: 2012 Seventh International Conference on Availability, Reliability and Security. IEEE. **(2012)**, pp. 174–179.
[21] P. Singh, Y.P.S Maravi, S. Sharma, "Phishing websites detection through supervised learning networks", In: 2015 International Conference on Computing and Communications Technologies (ICCCT). IEEE. **(2015)**, pp. 61–65.
[22] Y.-S. Chen, Y.-H. Yu, H.-S. Liu, P.-C Wang, "Detect phishing by checking content consistency". In: Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014). IEEE. **(2014)**, pp. 109–119.
[23] L. Wu, X. Du, J. Wu, "MobiFish: A lightweight anti-phishing scheme for mobile phones", In: 2014 23rd International Conference on Computer Communication and Networks (ICCCN). IEEE. **(2014)**, pp. 1–8.

[24] S.-S.Tseng, C.-H Ku, A.-C., Lu, Y.-J Wang, G.-G Geng, "Building a Self-Organizing Phishing Model Based upon Dynamic EMCUD", In: 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE .**(2013)**, pp. 509–512.
[25] F. Alkhateeb, A.M Manasrah, A.A.R Bsoul, "Bank Web Sites Phishing Detection and Notification System Based on Semantic Web technologies", Int. J. Secur. Its Appl. vol.6, **(2012)**, pp.53–66.
[26] R. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", Wiley, New York **(2008)**.

Authors

Dr. Junaid Chaudhry specializes in Research and Analysis (R&A) of both network and application centric products. He received his PhD from Ajou University.

Dr. Shafique Ahmad Chaudhry. Is an Assistant Professor at Dhofar University in Oman. His research interests include Internet of Things, Service discovery and provisioning, Wireless Networks, Network Security

Dr. Robert G. Rittenhouse is an associate professor in the Department of Computer Engineering at Keimyung University in Daegu Korea. He received his Ph.D. from the University of California at Irvine. His research interests include security, ubiquitous computing and social informatics.

