# State of Research on User Training against Phishing with Recent Trends of Attacks

Aniket Bhadane [a,*], Dr. Sunil B. Mane [a]
[a] College of Engineering Pune

[*]Corresponding author
Email addresses:
aniketbhadane93@gmail.com (Aniket Bhadane),
sunilbmane@gmail.com (Dr. Sunil B. Mane)

## Abstract

We present a survey of literature on User Training approaches to counter phishing and the current trends of phishing attacks. Phishing messages and websites masquerade as a trusted source and continue to be a problem for corporates and individuals causing huge tangible and intangible losses. Phishing is a wide-spanning attack and cannot be solved in one single way. It requires a collaborative effort in all directions. Solutions to mitigate phishing are mainly detecting the attack using automated software techniques, training users, and designing better interfaces to guide users in taking informed decision. Phishing mitigation community has not given enough importance to User Training, focusing more on developing automated approaches to detect phishing attacks. This paper aims at providing an organized study of User Training approaches to mitigate phishing. Phishing is constantly on rise with current trends showing huge increase in Spear Phishing attacks and Social Media-based attacks.

Keywords: Phishing, Social Engineering, Usable Security, Human Computer Interaction, User Characteristics

## 1. Introduction

Phishing attacks masquerade as a trustworthy source, often spread using socially engineered messages using media such as emails, social media, SMS, online multiplayer games, VoIP, etc. to persuade victims to perform certain actions of attacker's benefit [1]. These actions can be persuading the user to enter sensitive information on a phishing website; clicking a malicious/phishing link in an email; performing certain actions, such as money transfer, installing malicious software etc., as stated in the socially engineered message. Social engineering is psychological manipulation of people to make them perform certain actions [2].

Phishing attacks caused loss of over $3 Billion in last 3 years [3] and have seen an increase of 65% in 2016 over 2015 [4]. Spear Phishing attacks constituted 90% of all phishing attacks. A Spear phishing attack costs $1.6 Million on average, and $3.7 Million is spent a year by an average 10,000-employee company dealing with phishing attacks [5]. Very recent major phishing incidents include phishing attempts after Equifax data breach, the Google Docs phishing attack and the DNC hack. Phishing emails and websites were found masquerading as Equifax after its massive data breach [6][7]. In the Google Docs phishing scam, almost 1 million Gmail users were affected [8]. And the DNC hack [9] led to the leak of 19,252 emails and 8,034 attachments from the DNC, the governing body of the United States' Democratic Party.

The past work on phishing can be categorized into four categories: under- standing why people fall for phishing, automated software techniques to detect phishing, training people to not fall for phishing attacks, and better user interfaces to help people make better decisions when confronted with an attack [10].

Although a very important part of cyber security, User Training approaches have not received much attention from the research community and industry. There exists no software mechanism till date which is able to filter all types of phishing messages. Some phishing messages do reach the end users. So it is important for users to make better decisions and not fall for these attacks. This can be done by providing efficient User Training and Better Interfaces. We provide an ordered study of the current state of research on User Training approaches to mitigate phishing. This survey also provides details of recent studies on specific trends in phishing that are seen nowadays. We do not cover related topics in details, such as spam, but we do touch upon such points wherever required.

In Section 2, we give a Background on details of Phishing alongwith recent trends of these attacks. Section 3 describes User Training approaches as present in the literature. In Section 4, we provide the learnings of our study, and conclude in Section 5.

## 2. Background and Recent Trends of Attacks

Spam messages are "unsolicited" messages sent for commercial benefits, often in bulk quantities. Spam messages, in general, do not need to pretend to be someone else. For example, a health and medicine company advertising its products. Whereas, Phishing

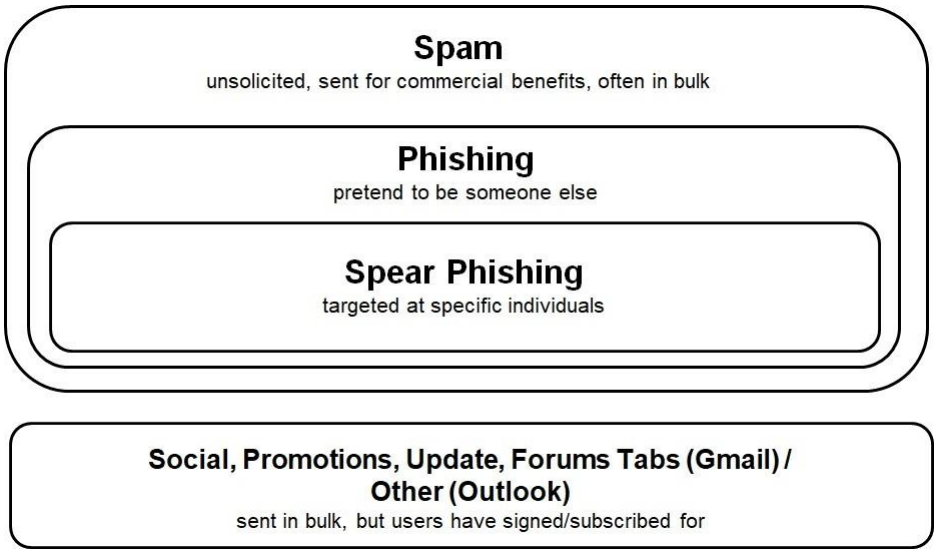


Figure 1: Classes of Messages in the vicinity of Phishing Messages.

messages are subset of spam messages, which "pretend to be someone else". Such as a phisher pretending to be from paypal to get sensitive information from user. Gmail provides the option to divide the inbox into Primary, Social, Promotions, Update, and Forums Tabs. The emails in later four categories are also sent in bulk quantity. But these are the ones that users have "signed/subscribed for" and can sometimes be personalized for the user. For example, a user has signed for receiving weekly newsletter from some site. The site will be sending bulk emails to all its subscribers. Such emails will go into user's Promotions tab since user has subscribed for it. Outlook also provides the option to divide the inbox into Focused and Other Tabs, with the Other tab having mails such as those in Gmail's later four category tabs. We've shown this diagrammatically in Figure 1. Gmail adds Phishing emails to the Spam folder itself. On viewing mails in the spam folder, it shows a warning message in red or yellow banner describing the type of message. Also, Gmail maintains sender reputation [11] as a feature to decide whether a message should be treated as spam or not, among other spam related features. We observed a spam/phishing mail sent from a reputed sender landed in receiver's inbox, whereas the same mail sent from a less reputed sender landed in Spam folder. Self-reputation can be seen in Gmail Postmaster [12]. Mail service providers implement anti-phishing measures on server side. Also various anti-phishing browser extensions are available on the client side which can be installed by individual users.

Phishing is a semantic attack. It exploits human vulnerabilities by targeting the way humans interpret content displayed on the system. This is commonly done using social engineering.

A phishing attack or a phishing taxonomy using phishing messages has three major stages: First stage corresponds to Attack Lure where the victim(s) receive a socially engineered phishing message. Second and Third stages correspond to Attack Exploit, where victim(s) perform action as suggested in the message, and attacker exploits the

action performed by the victim(s) for his benefit.

Phishing messages masquerade/impersonate as a trusted identity and use social engineering techniques to persuade user to perform actions of phishers' benefit. As phishing is carried over various communication media, the psycho- logical and behavioral factors leading to users' response to attacks also depends on the media.

Phishing messages persuade users to click on an URL in the message and entering sensitive information on resulting page, or replying to the message with sensitive information, or performing money transfer, etc. When using phishing websites to steal users' credentials and sensitive information tied to the target site, phishers may use free web hosting services, or register a new domain, and may also use compromised machines to host their files. Many phishing attacks made no attempt of disguising URL as target site and were successful. Very few phishers registered domain names that were confusingly similar to the brands, which shows that phishers do not need deceptive URLs to fool users [4]. Today, most of the phishing sites are created using Toolkits, which makes it very easy for attackers to create websites visually similar to their targets. The phishing website's URL may be customized to create innumerable URLs by adding random parameters, with all these URLs pointing to the same phishing site.

Phishers may use vulnerabilities in the DNS to divert internet traffic to their phishing websites. In case of DNS (Domain Name System) cache poisoning, the DNS returns IP of the phishing website instead of the correct IP of the domain name. In another technique, domain shadowing, phishers compromise a legitimate domain name's DNS to set up new subdomains. These new subdomains can then be used to point to the phishing content.

Social media platforms such as Twitter have their own phishing and malware detection mechanisms but are frequently bypassed with the use of URL shorteners and multiple redirections [13]. Automated spear phishing tools have also been developed to generate phishing tweets. One such tool [14] uses machine learning techniques to generate tweets based on existing spear phishing data, and the topics extracted from timeline posts of the target and of those they retweet or follow.

Phishing messages also employ Technical Subterfuge. These schemes plant crimeware onto PCs. An attacker can send an email to an employee masquerading as IT department of the company, asking the employee to install a security patch which is actually a malware.

If the victim performs action as desired by the attacker, the attacker then exploits this action performed by the victim. For example, if the attack involves stealing of sensitive information or credentials, phishers may monetize the information themselves or sell the information on underground network marketplaces. Or if the attack involves installation of a malware, the attacker fetches/monitors sensitive data.

A particular type of phishing which constituted 90% of all phishing attacks is Spear Phishing. Spear Phishing is one of the biggest threats to corporates today with these being 95% of all attacks on corporates [15]. In contrast to normal phishing attacks, which target general public, spearphishing attacks are targeted at specific individuals or employees of an organization. Attackers gather specific information about their targets through their social network or acquaintance etc., and use this information and to create customized phishing messages for the particular target group.

A form of spear phishing attack, called Whaling, is directed specifically at senior level executives in businesses and other high-profile targets. At toy making company Mattel, a high level financial executive received an email requesting money transfer of $3 Million, impersonating as from the newly assigned CEO [16].

The calculation of cost of damages caused by phishing attacks differ extensively, and are largely dependent on the assumptions made by the organizations when calculating the damages and different departments affected within the organization. Phishing attacks not only cause direct damage, but also indirect damage, such as damage of reputation, leakage of source code and intellectual property, etc. [1]

Phishing Honeypots (network decoys) can be used by researchers and organizations to bait attackers. They are purposely kept vulnerable, so that attackers can be lured to use such resources. These honeypots are isolated and monitored. They can be used to capture activities of phishers, which can then be used for research purposes to get better understanding of attack flow and trends.

Many Phishing websites are found to redirect automated scripts or bots, such as web crawlers, to legitimate domain, but redirect browsers to phishing domain. This is done using robot.txt file, which is used by websites to communicate with web crawlers [13].

Other recent trends of phishing that we observed are:

- Social media phishing attacks increased by 500% in Q4 of 2016. Huge increase was seen in use of fraud accounts masquerading as customer support of popular brands. This tactic is relatively new and is called angler-phishing, where attackers register and use fake Twitter accounts masquerading as customer support of some brand [17].
- Specific brands were attacked more than regular on specific occasions, such as holiday season [4].
- The top ten targets faced over 75% of all the phishing attacks in 2016 [4].
- Attackers also were found to be using IP filters on Phishing sites, to disallow people from other countries to visit the site and even people from the target company [4].

It is important to block an attack in the initial few hours of the attack, as a large percentage of users read the phishing message till the blacklists are updated. As found by Jagatic et al. [18], most of the users fell victim to a phishing attack in the first few hours of the attack itself.

Signal Detection theory (SDT) has been used by various studies to measure user vulnerability to phishing attacks [19][20][21][22]. SDT is used to quantify or measure the ability of users to distinguish between signal (phishing) and noise (legitimate). It has two factors involved: Sensitivity (d') and Criterion (C). Sensitivity measures users' ability to differentiate between signal and noise. It is the gap between the means of the two distributions. The further apart the distributions, the greater the sensitivity or d'. Criterion is defined as the user bias or tendency when making a decision. It is measured by how far their decision threshold (criterion line) is from the intersection of the two distributions.

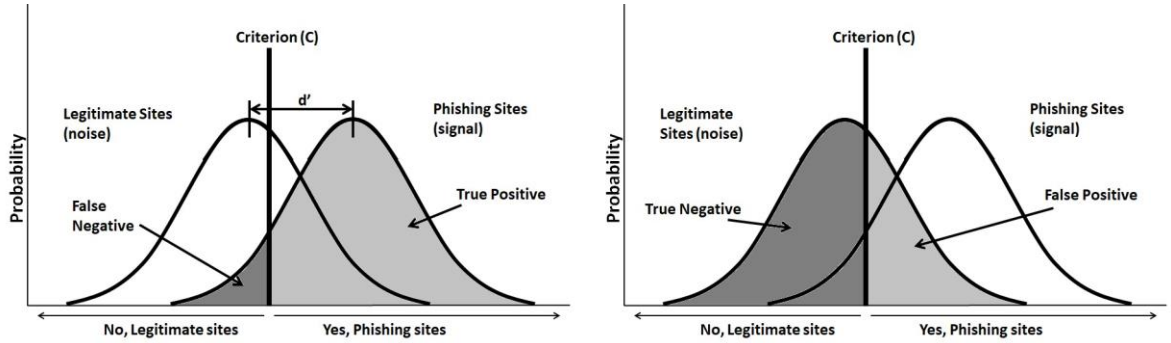


Figure 2: Use of Signal Detection Theory (SDT) in Phishing.

Regions C < 0 and C > 0 indicate more cautious/alert users and less cautious/alert users respectively. Figure 2 shows how the criterion line di- vides the graph to depict false positives, true positives, false negatives, and true negatives. A User Training approach should typically aim to i) increase users' cautiousness/alertness by shifting the criterion line to the right; ii) increase users' sensitivity, by increasing the separation between the two distributions, so people would be able to better differentiate between phishing and legitimate; or iii) a combination of i) and ii) [19].

## 3. Training Users

User Training can be used for increasing user awareness about phishing at- tacks and teaching them how to detect such attacks so that they can take better informed decisions in such circumstances. User Education and Training is an important part of online security, but it has not received enough attention from the phishing community.

In a recent study by Deloitte, more than 70% organizations mentioned lack of security awareness of employees to be their major vulnerability. More than 4 out of 10 organizations don't provide security education to their education [23]. A survey by PWC showed that organization providing security education to employees are half as likely to fall for such attacks [24].

Training increases the cost to the company and consumes time. But an employee falling for a phish can cause considerable amount of damage to the company. Some studies have shown training programs to be helpful [25][26][27][28], while some disagree or say that training has mixed benefits [29][30][31].

Security is largely considered as a secondary goal, and educating users about things which are not related to their primary tasks may hit their cognitive limits [30].

As evaluated in [26], after training people with the best available training programs, users were able to detect more phishing attacks, but still could not detect 29% of the attacks. Most companies have annual policy based training that's required for compliance, which have shown to be ineffective to change employees' behavior. Caputo et al. [29] surveyed employees' behavior with phishing emails in a large organization. They found that the anti-phishing training did not help in changing employees' behavior when dealing

with spear phishing emails. Users are seen not to be utilizing in their daily behavior, the knowledge they received during the training.

Users are found to not retain the knowledge [32] learned during the training and tend to forget after short period of time. Hence, there are studies advocating that training needs to be continuous. Organizations, banks, etc. send periodic security notices via emails or SMS's to their employees or clients about phishing threats. But such periodic notices have been found to be ineffective in changing users' behaviors [27]. Studies [25][21][1] have shown that anti-phishing training is most effective when it is done at the time when user is dealing with a phishing attack, and when it is done periodically.

Most training programs have focused on adults. Lastdrager et al. [33] explored training of school going children against phishing. Majority of children in USA and Europe access the internet daily. Attackers can get information about a target from their social networks and children in their social network can be used to get information of the target (e.g.: of his/her parents). Their results showed that training children against phishing works only for the short term. Although, they also suggest that such security programs in school curriculum can be helpful in making future generations aware of security threats.

Oliveira et al. [32] mention that demographic-tailored training and prevention approach will increase the effectiveness of security measures because a demographic-targeted solution will impose lesser requirements on people and will match their specific vulnerabilities.

Our learning was that the best way of training against phishing attacks is "at the moment of attack - periodic - demographic tailored" training.

Research on User Training against phishing is mainly done on developing Micro Games or Embedded Training.

## 3.1. Micro Games

In 2007, Sheng et al. [19] developed Anti-Phishing Phil (Figure 3), a game which educates users about various parts and cues to identify phishing and legitimate URLs. They used leaning sciences to build intervention based designs, and found it to be more effective than security notices emailed by companies to users. The mouse pointer is visualized as a fish, and asks users to hover the fish over worms which then show URLs. The game educates users about URLs and the fish has to eat (safe) or reject (phishing). Their evaluation with more than 4500 people showed 61% improvement in users' ability to identify phishing URLs and also decrease in false positives. Though the game teaches about URLs, it does not give real time experience of detecting a phish or about the social engineering techniques used in attacks.

Control-Alt-Hack [34] lets users interact with cards in a board game, through which it teaches users about different social engineering techniques attackers use. But this game is not meant for teaching users to identify phishing attacks; it makes users more aware about tricks used by attackers.

Recently, Wen et al. [35] developed game called What.Hack (pronounced what dot hack). They give example of DNC hackings during the 2016 US presidential election, where staff were tricked into sharing passwords which granted access to confidential

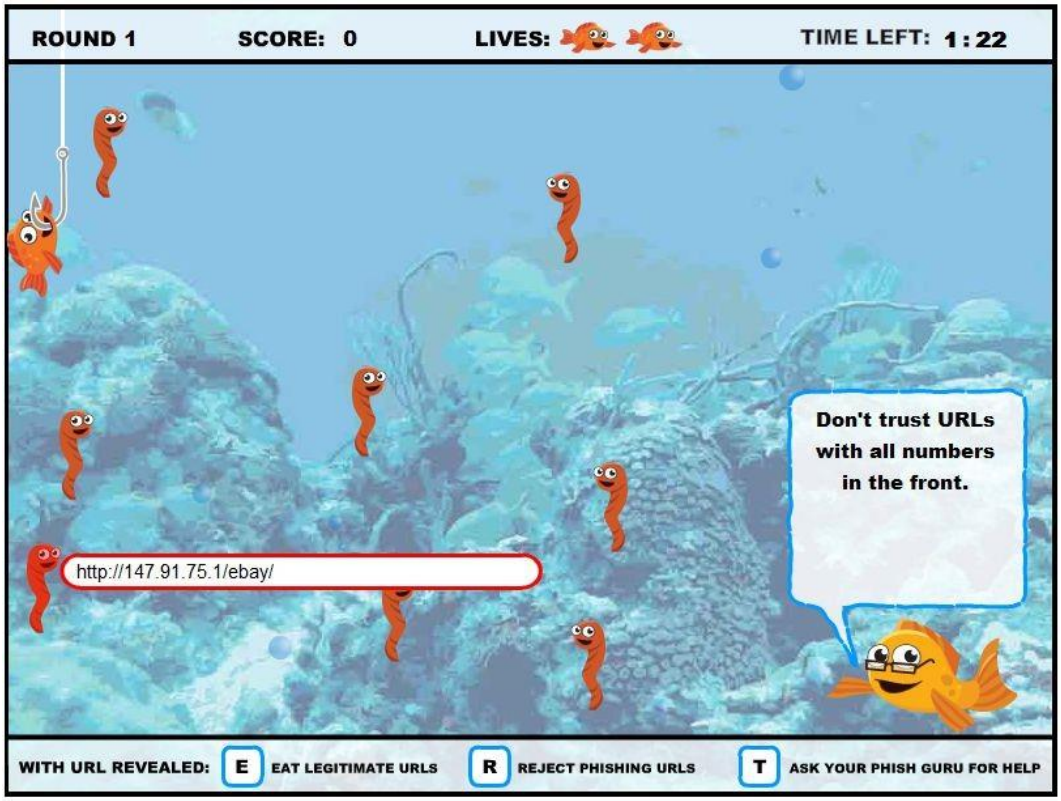


Figure 3: Anti-Phishing Phil micro-game.

information by fake Google security emails. They mention that vulnerabilities such as these are due to insufficient and tiresome training when it comes to information security, and a potential solution is the introduction of more engaging training methods, which teach information security in an active and entertaining way. The authors mention that existing games teach users about specific aspects of phishing, such as teaching for phishing URLs, but not for malicious attachments. The authors incorporate such combined phishing techniques in their game. What.Hack presents a sequence of puzzles in a story-based game context, to teach users about social engineering threats. The player is provided with a rulebook that tells the players which emails are safe or unsafe. The player is asked to correctly identify phishing emails else it will have negative consequences. The authors have yet to test the effectiveness of their game.

Several commercial offerings are available, but their details are not avail- able in public literature, for example Email Security or Anti-Phishing Phyllis by Wombat Security (Figure 4) [36]. It teaches users to identify phishing attacks, using interactive training and character-driven training game.

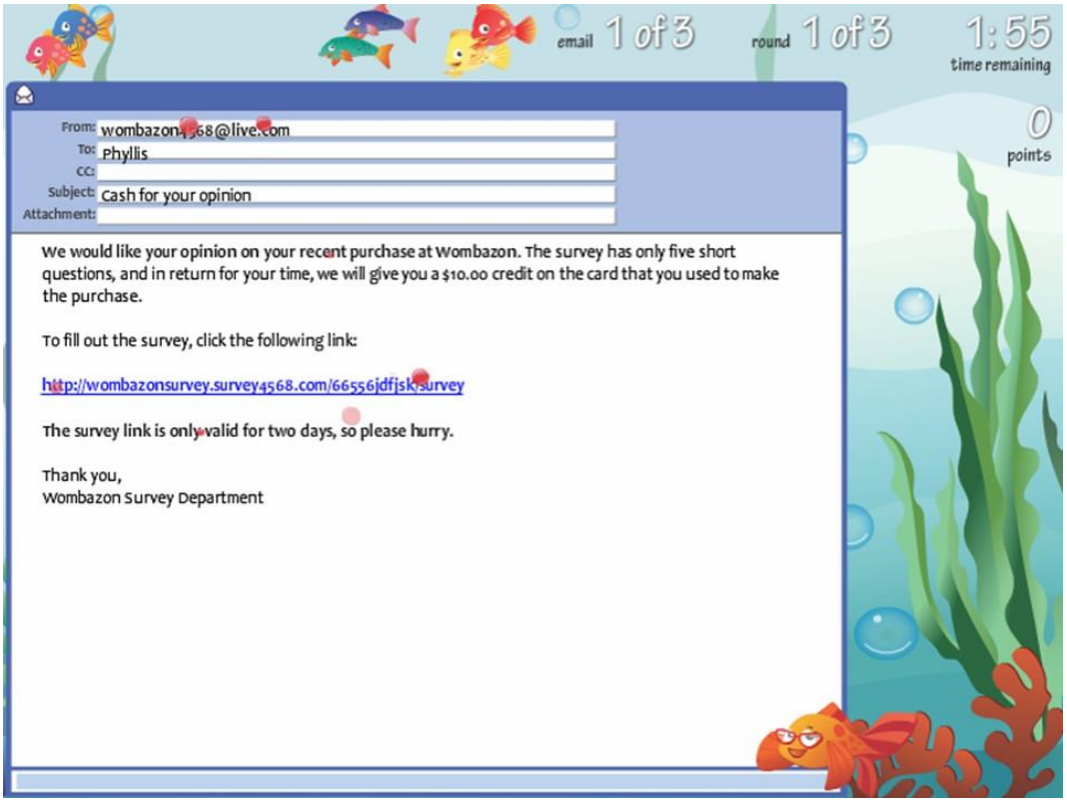


Figure 4: Anti-Phishing Phyllis micro-game.

## 3.2. Embedded Training

In this type of training, the educational material is embedded, i.e. integrated, into the daily primary tasks of users.

An approach where simulated phishing emails are sent to users to train them, have been used with Indiana University students [18], West Point cadets [37], and New York state office employees [38]. The approach led to an improvement in users' phishing detection ability.

Kumaraguru et al. [39] developed PhishGuru (Figure 5), which sends simulated phishing emails to users in their normal use of emails, and uses interventional educational messages to educate them. When the users fall victim to the attack, such as clicking on a link in the phishing email, the system teaches users about the attack. They use intervention type design to show educational messages. They tested two different design types, text-graphics and comic strip, to show their interventional educational messages. They found comic strip design type to be more effective than text-graphics.


Figure 5: PhishGuru embedded training.

## 4. Discussion

Phishing attacks have shown to be evolving over time, and continue to be a threat to corporates and individuals. Phishing cannot be dealt in one specific way, but requires a collaborative effort in all directions. Use of psychological factors and demographics can help in designing user training approaches for phishing detection. Interdisciplinary fields such as Learning Sciences, Cognitive Sciences and Educational Psychology can prove to be helpful in designing training approaches for enabling retention of knowledge learned in training and its application at the time of attack. Instead of only giving knowledge about these attacks to users, it is also important to teach them how to deal with these attacks in real time. And training users at the time of the attack has been found to be the most effective way of training users. As we mentioned in previous section, the best way of training against phishing attacks is “at the moment of attack - periodic - demographic tailored” training.

## 5. Conclusion

In this paper, we provided details on different approaches for Training Users to deal with phishing. Phishing remains to be a major security threat for the corporates and for the general internet users. Phishing is not limited to a single communication media, and spans across different types of media such as E-Mails, Social Media, online multiplayer games, etc. We provide an organized study covering User Training approaches against phishing, which we found to be lacking in the existing literature. Phishing, being a multifaceted attack, requires research to be done in all aspects. Technical solutions to mitigate phishing are not 100% effective and some attacks do reach the end users. Moreover, phishing attacks, especially Spear Phishing attacks, continue to become more sophisticated and cause loss of billions of dollars and also intangible loss such as dam- aged brand reputation. To build effective countermeasures, it is important to understand the psychology of users which makes them fall for phishing attacks. Training of users is effective if they retain the learning and are able to apply it in case of an attack. It is important to train users "at the moment" of the attack, periodically, and considering various user demographics. No single way can mitigate phishing; hence it requires collaborative effort in all directions. It is important to secure all doors to not allow phishers to conduct such attacks.

## Acknowledgement

The authors would like to thank anonymous reviewers for their valuable comments.

## References

[1] M. Khonji, Y. Iraqi, A. Jones, Phishing Detection: A Literature Survey, IEEE Communications Surveys Tutorials 15 (4) (2013) 2091–2121. doi: 10.1109/SURV.2013.032213.00009.

[2] Social engineering (security), page Version ID: 800193757 (Sep. 2017). URL https://en.wikipedia.org/w/index.php?title= Social engineering (security)

[3] Internet Crime Complaint Center (IC3) | Business E-mail Compromise: The 3.1 Billion Dollar Scam (2016). URL https://www.ic3.gov/media/2016/160614.aspx

[4] apwg trends report q4 2016.pdf (2017). URL http://docs.apwg.org/reports/apwg trends report q4 2016.pdf

[5] J. Crowe, Phishing by the Numbers: Must-Know Phishing Statistics 2016 (2016). URL https://blog.barkly.com/phishing-statistics-2016

[6] Equifax or Equiphish? — Krebs on Security (2017). URL https://krebsonsecurity.com/2017/09/equifax-or-equiphish/

[7] After Massive Data Breach, Equifax Directed Customers To Fake Site (2017). URL http://www.npr.org/sections/thetwo-way/2017/09/21/552681357/after-massive-data-breach-equifax-directed- customers-to-fake-site

[8] A. Robertson, Google Docs users hit with sophisticated phishing attack (May 2017). URL https://www.theverge.com/2017/5/3/15534768/google-docs-phishing-attack-share-this-document-with-you-spam

[9] How hackers broke into John Podesta, DNC Gmail accounts – Naked Security (2016). URL https://nakedsecurity.sophos.com/2016/10/25/how-hackers-broke-into-john-podesta-dnc-gmail-accounts/

[10] Y. Zhang, J. I. Hong, L. F. Cranor, Cantina: A Content-based Approach to Detecting Phishing Web Sites, in: Proceedings of the 16th International Conference on World Wide Web, WWW '07, ACM, New York, NY, USA, 2007, pp. 639–648. doi:10.1145/1242572.1242659. URL http://doi.acm.org/10.1145/1242572.1242659

[11] Everything You Need to Know About Gmail's New Postmaster Tools (Jul. 2015). URL https://blog.returnpath.com/everything-you-need-to-know-about-gmails-new-postmaster-tools/

[12] Postmaster Tools – Google (2017). URL https://gmail.com/postmaster/

[13] A. Aggarwal, A. Rajadesingan, P. Kumaraguru, PhishAri: Automatic Realtime Phishing Detection on Twitter, arXiv:1301.6899 [physics]ArXiv: 1301.6899. URL http://arxiv.org/abs/1301.6899

[14] T. Fox-Brewster, Who's Better At Phishing Twitter, Me Or Artificial Intelligence? (2016). URL https://www.forbes.com/sites/thomasbrewster/2016/07/25/artificial-intelligence-phishing-twitter-bots/

[15] N. Weinberg, How to blunt spear phishing attacks (Mar. 2013). URL https://www.networkworld.com/article/2164139/network-security/how-to-blunt-spear-phishing-attacks.html

[16] C. Cimpanu, Toy Maker Mattel Loses $3m in BEC Scam, Then Fights for It and Gets It Back (2016). URL http://news.softpedia.com/news/toy-maker-mattel-loses-3m-in-bec-scam-then-fights-for-it-and-gets-it-back-502401.shtml

[17] P. Muncaster, Social Media Phishing Attacks Soar 500% (Feb. 2017). URL https://www.infosecurity-magazine.com/news/social-media- phishing-attacks-soar/

[18] T. N. Jagatic, N. A. Johnson, M. Jakobsson, F. Menczer, Social Phishing, Commun. ACM 50 (10) (2007) 94–100. doi:10.1145/1290958.1290968. URL http://doi.acm.org/10.1145/1290958.1290968

[19] Steve Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, E. Nunge, Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish, in: Proceedings of the 3rd Symposium on Usable Privacy and Security, SOUPS '07, ACM, New York, NY, USA, 2007, pp. 88–99. doi:10.1145/1280680.1280692. URL http://doi.acm.org/10.1145/1280680.1280692

[20] C. I. Canfield, B. Fischhoff, A. Davis, Quantifying Phishing Susceptibility for Detection and Behavior Decisions, Human Factors 58 (8) (2016) 1158– 1172. doi:10.1177/0018720816665025. URL https://doi.org/10.1177/0018720816665025

[21] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, J. Hong, Teaching Johnny not to fall for phish, ACM Transactions on Internet Technology (TOIT) 10 (2) (2010) 7. URL http://dl.acm.org/citation.cfm?id=1754396

[22] J. Nicholson, L. Coventry, P. Briggs, Can we fight social engineering at- tacks by social means? Assessing social salience as a means to improve phish detection, in: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), USENIX Association, 2017, pp. 285–298. URL https://www.usenix.org/system/files/conference/soups2017/ soups2017-nicholson.pdf

[23] Phishing Scams at All-Time High, Employee Training Not Keeping Pace |Wombat Security (2017). URL https://www.wombatsecurity.com/about/news/phishing-scams- all-time-high-employee-training-not-keeping-pace

[24] Phishing threatens todays - economy - ny - times final.pdf (2017). URL https://cdn2.hubspot.net/hub/372792/file-1519503800-pdf/ Phishing Threatens Todays Economy NY Times FINAL.pdf - -

[25] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, T. Pham, School of Phish: A Real-world Evaluation of Anti-phishingTraining, in: Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS '09, ACM, New York, NY, USA, 2009, pp. 3:1–3:12. doi: 10.1145/1572532.1572536. URL http://doi.acm.org/10.1145/1572532.1572536

[26] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, J. Downs, Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, ACM, New York, NY, USA, 2010, pp. 373–382. doi:10.1145/1753326.1753383. URL http://doi.acm.org/10.1145/1753326.1753383

[27] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, E. Nunge, Protecting People from Phishing: The Design and Evaluation of an Em- bedded Training Email System, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '07, ACM, New York, NY, USA, 2007, pp. 905–914. doi:10.1145/1240624.1240760. URL http://doi.acm.org/10.1145/1240624.1240760

[28] A. Alnajim, M. Munro, An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection, in: 2009 Sixth International Conference on Information Technology: New Generations, 2009, pp. 405– 410. doi:10.1109/ITNG.2009.109.

[29] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, M. E. Johnson, Going Spear Phishing: Exploring Embedded Training and Awareness, IEEE Security Privacy 12 (1) (2014) 28–38. doi:10.1109/MSP.2013.106.

[30] S. Gorling, The Myth of User Education, in: Proceedings of the 16th Virus Bulletin International Conference, 2006.

[31] The myth of the stupid user | Information & Design (2011). URL http://infodesign.com.au/usabilityresources/articles/ themythofthestupiduser/

[32] D. Oliveira, H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin, N. Ebner, Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing, in: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17, ACM, New York, NY, USA, 2017, pp. 6412–6424. doi:10.1145/ 3025453.3025831. URL http://doi.acm.org/10.1145/3025453.3025831

[33] E. Lastdrager, I. C. Gallardo, P. Hartel, M. Junger, How Effective is Anti-Phishing Training for Children?, in: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), USENIX Association, Santa Clara, CA, 2017, pp. 229–239. URL https://www.usenix.org/conference/soups2017/technical-sessions/presentation/lastdrager

[34] T. Denning, A. Lerner, A. Shostack, T. Kohno, Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13, ACM, New York, NY, USA, 2013, pp. 915–928. doi:10.1145/2508859.2516753. URL http://doi.acm.org/10.1145/2508859.2516753

[35] Z. A. Wen, Y. Li, R. Wade, J. Huang, A. Wang, What.Hack: Learn Phishing Email Defence the Fun Way, in: Proceedings of the 2017 CHI Conference Extended

Abstracts on Human Factors in Computing Sys- tems, CHI EA '17, ACM, New York, NY, USA, 2017, pp. 234–237. doi:10.1145/3027063.3048412. URL http://doi.acm.org/10.1145/3027063.3048412

[36] Email Security or Anti-Phishing PhyllisTM | Wombat Security (2017). URL https://www.wombatsecurity.com/training-modules/email- security-or-anti-phishing-phyllis

[37] eqm0517.pdf (2005). URL http://www.educause.edu/ir/library/pdf/eqm0517.pdf

[38] New York State Office of Cyber Security & Critical Infrastructure Coordi- nation. Gone phishing. . . a briefing on the anti-phishing exercise initiative for new york state government. Aggregate Exercise Results for public re- lease., 2005.

[39] P. Kumaraguru, Phishguru: A System for Educating Users About Semantic Attacks, Ph.D. thesis, Carnegie Mellon University, Pittsburgh, PA, USA (2009).

## Biographical Sketch

Aniket Bhadane received his Bachelor of Engineering (Computer) degree from Savitribai Phule Pune University (formerly University of Pune) in 2015. He is currently pursuing M.Tech. Computer Engineering degree from College of Engineering Pune (COEP). His research interests are in the field of cyber security, user authentication and usable security.

Dr. Sunil B. Mane is working as Associate professor, Department of Computer Engineering and Information Technology, College of Engineering, Pune (An Autonomous Institute of Govt. of Maharashtra). He has more than 15 years of teaching experience. Dr. Mane has over 25 research publications in various national/international journals and conferences. He is a Board of Studies member in Computer Engineering/Information Technology of various autonomous engineering institutes. He delivered lectures on information and cyber security domain as invited speaker. He is serving as Co-Chief Investigator for the Information Security Education and Awareness (ISEA) project, Ministry of Information Technology, Govt. of India. His area of research is data privacy and cyber security.