Phishing Attacks Root Causes

Hossein Abroshan(✉), Jan Devos, Geert Poels,
and Eric Laermans

Ghent University, 9000 Ghent, Belgium
{hossein.abroshan, jang.devos,
geert.poels, eric.laermans}@ugent.be

Abstract. Nowadays, many people are losing considerable wealth due to online scams. Phishing is one of the means that a scammer can use to deceitfully obtain the victim's personal identification, bank account information, or any other sensitive data. There are a number of anti-phishing techniques and tools in place, but unfortunately phishing still works. One of the reasons is that phishers usually use human behaviour to design and then utilise a new phishing technique. Therefore, identifying the psychological and sociological factors used by scammers could help us to tackle the very root causes of fraudulent phishing attacks. This paper recognises some of those factors and creates a cause-and-effect diagram to clearly present the categories and factors which make up the root causes of phishing scams. The illustrated diagram is extendable with additional phishing causes.

Keywords: Phishing · Scam · Root causes · Behaviour

1 Introduction

Human life has significantly changed as a result of online services including e-shopping and e-banking, etc. Although these services offer great convenience, they are accompanied by an increase in cybercrimes and present new security threats. An online phishing is a cybercrime to steal credentials from users, such as login and credit card details, "by masquerading as trustworthy entities in electronic communication" [1]. Then the attacker usually uses the collected information to sign into the genuine reputable website, such as those that are used for internet banking, to steal from the victim's online account [2]. In recent years, many researchers have focused on phishing attacks in order to offer an anti-phishing solution for protecting sensitive financial data from phishers. However, phishing still works, and every day brings with it new phishing websites and techniques which steal personal credentials.

By reviewing the existing anti-phishing techniques, we understand that most of them are trying to technically detect and/or prevent phishing attacks. We are of the opinion that focusing on the human psychological and sociological factors that attackers use to scam people would be an effective way to fundamentally tackle phishing attacks. We believe that current anti-phishing solutions are useful though insufficient, as phishers always use people's psychological weaknesses to design new types of phishing attacks. Several studies [3, 4] have already identified some of the

N. Cuppens et al. (Eds.): CRiSIS 2017, LNCS 10694, pp. 187–202, 2018.
https://doi.org/10.1007/978-3-319-76687-4_13

above-mentioned factors, but none of them have carried out a root cause analysis to list all the possible psychological factors at play and the tricks that scammers use to fool people.

The objective of this research is to identify human and psychological factors which phishers can use to scam people and make a successful phishing attack. Listing and categorising these root causes will enable us to develop improvement programmes for each factor. If we know that a psychological reason, for instance gullibility, is one of the root causes of phishing attacks then we can detect users' gullibility level, for example by using a psychological test and/or a trust game, as well as develop some improvement and treatment programmes, in the form of specific trainings for example, to improve gullibility level of to those who easily trust others. We hope that such programmes could help reduce the number of successful phishing attacks by treating the phishing root causes as identified in this paper. It is possible to systematically identify users' behaviour by monitoring their online activities, using online tests, and providing them relevant trainings based on the detected weaknesses. Therefore, these anti-phishing solutions can be automated.

For this purpose, we initially reviewed anti-phishing solutions to find out which techniques are being applied to deal with phishing attacks. We also used anti-phishing studies to figure out how the targeted phishing attacks work and what phishing tactics are being used by attackers. We then reviewed other studies, especially scam-related psychological articles, to identify which cognitive factors can be used by phishers to fool people and to design phishing attacks. We then identified tricks that a phisher might use to scam people. We focused on a selection of tricks from the reviewed studies, particularly anti-phishing studies. Finally, we illustrated the root causes, including the identified human factors and the tricks used via a cause-and-effect diagram. Such a diagram presents a clear and easily comprehensible picture of the issue at hand.

For conducting our literature review we used the Webster and Watson [5] structured approach. We therefore started with searching Phishing Attacks, Anti-phishing techniques, Social Engineering Attacks and Online Scam literatures. We performed our queries on journal databases such as Science Direct, Google Scholar, and WorldCat, and browsed seventy journals such as MIS Quarterly, ACM Transactions on Information and System Security, International Journal of Security and Its Applications, Journal of Personality and Social Psychology, etc. We also queried and examined related conference papers. We selected articles that explained and defined phishing methods, root causes, and other useful information and references for our study. Then we went through the citations of the selected articles to determine whether there were more publications that we should review. In the last stage, we used the Web of Science to identify more articles citing the key articles we had identified in our earlier stage.

The paper starts with reviewing the existing anti-phishing techniques. It then presents several phishing attacks. Next, it explains psychological factors which can influence a phishing process and describes tactics scammers use to trick people. Finally, it comes up with a cause-and-effect diagram and provides concluding remarks.

2 Anti-Phishing Techniques

The existing anti-phishing approaches are classified as either server based and/or client based [6], where most of the client side anti-phishing systems are plug-ins or web browser toolbars. In recent years, many research efforts have been conducted in developing anti-phishing systems to detect and prevent phishing emails and/or websites. Table 1 indicates some existing anti-phishing techniques and grouped them into five anti-phishing categorises based on their technical and/or non-technical approaches to detect or prevent Phishing. Those techniques which are using webpage features like URL and web ranking to detect phishing attacks are not able to recognise all phishing websites. Heuristics and machine learning methods use webpage features for phishing detection, however they mostly have “high complexity” and “high false positive rates” issues [7]. The blacklists and whitelists need to be frequently updated. Blacklists are only useful to detect the detected phishing websites and emails and are not agile in responding to “zero-hour attacks” [8]. Using time-sensitive tokens works until the criminals implement real-time attacks.

Table 1. Anti-phishing categories and techniques.

Category	Techniques	
Phishing emails (Detection and prevention)	Features processing [11–15] Identification and authentication [16]	Heuristics method [13, 17] Hybrid methods [18, 19]
Phishing websites (Detection and prevention)	Content-based detection [20] Visual and layout similarity [21–24] Heuristics [25, 26] URL evaluation [27, 28]	User activities [29] Evaluation and ranking [30] Whitelists [31–33] Blacklists [34, 35] Hybrid [36, 37]
Network-based (Detection and prevention)	Authentication [38–41] Network security elements [42] Password management tools [41, 43]	Fraudulent activity detection (Transaction and log analysis) [44–46] Honeypot/phisher tracer [42, 47, 48]
Improvement of user knowledge	Knowledge evaluation and training systems [49, 50] Warning effectiveness [51]	
Prosecution	**Sending phishing messages** [52]: CAN-SPAM Act (18 U.S.C. § 1037) (US) E-Privacy Directive (EU) General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) [53] Directive (EU) 2016/680 [53] Anti-phishing Act of 2005 [54] Fraud Act 2006 (UK) [55] **Deterrence of identity theft** [52]: Crime Ordinance (Cap. 200) (HK) Theft Ordinance (Cap. 210) Identity Theft and Assumption Deterrence Act (18 U.S.C. § 1028) (US) Credit card fraud (18 U.S.C. § 1029) (US) Bank fraud (18 U.S.C. § 1344) (US) Computer fraud (18 U.S.C. § 1030(a)(4)) (US) Computer-related fraud (Article 8, Convention on Cybercrime) Fraud Act 2006 (UK) [55]	**Data privacy** [52]: Personal Data (Privacy) Ordinance (Cap. 486) (HK) Telecommunication Ordinance (Cap. 106) (HK) Telecommunication Privacy Directive (EU) E-Privacy Directive (European Union) Data Interference (Article 4, Convention on Cybercrime) System interference (Article 5, Convention on Cybercrime) General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) [53] Directive (EU) 2016/680 [53] Fraud Act 2006 (UK) [55] Rundschreiben 4/2015 (BA) (Germany) [56] **Fake websites** [52]: Copyright Ordinance (Cap. 528) (HK) Wire fraud (18 U.S.C. § 1343) (US) Infringements of copyright (Article 10, Convention on Cybercrime)

The phishing attacks will not disappear with "one solution" and at "one level" [9]. A study shows that even by utilising modern anti-phishing techniques, over 11% of users read the spoofed messages and enter their credentials [10].

3 Phishing Attacks

In recent years, researchers and organisations have categorised phishing attacks in similar or sometimes in different ways. Some examples of the mentioned categorisations of phishing tactics are "Deceptive Phishing" [57], "Malware-based Phishing" [11, 57–59], "Key-loggers" and "Screen-loggers" [57, 58], "Session Hijacking" [57], "Web Trojans" [57], "Hosts File Poisoning" [57], "System Reconfiguration" attacks [57, 59], "Data Theft" [57], "DNS-based Phishing" (Pharming) [57–59], "Content-injection Phishing" [57, 58], "Man-in-the-Middle Phishing" [57, 58], "Search Engine Phishing" [57, 59], "Website Forgery" [58], "Social Engineering" [11], "Mimicry" [11], "Email Spoofing" [11], "URL Hiding" [11], "Invisible Content" [11], "Image Content" [11].

By using the above tactics, scammers try to gain access to victims' sensitive information by masquerading as a reputable organisation or person. Figure 1 presents an example of a spear phishing attack. In this example, the phisher obtains basic information such as the name and email address of the targeted users by creating a real website that looks like the genuine website, or by hacking a real website. The fake or real website could be, for example, a promotional website, a lottery website, an e-shop, or any other website which asks for a user's personal information. Phishers can also obtain basic user information via public data or social media. In that case, the phisher uses the obtained information to create a phishing email.

Thus, a phisher relies on building trust, so that the victim believes that s/he is in contact with a reputable entity. A phisher might use tricks, persuasion, visceral influence, and/or any other technique to gain a user's trust.

4 The Influence of Cognitive Factors in the Phishing Process

Social engineering and technical tricks are two mechanisms phishers use to steal personal and financial credentials [60]. Social engineering targets individuals and the result of attacks depends on human decision, trust, and other cognitive factors. "Fraud is a human endeavor, involving deception, purposeful intent, intensity of desire, risk of apprehension, violation of trust, rationalization, etc. So, it is important to understand the psychological factors that might influence the behavior of fraud perpetrators" [61]. Therefore, to analyse the root causes of phishing attacks, we should study psychological and sociological factors to find out the main reasons why a user gets caught in a phishing net.

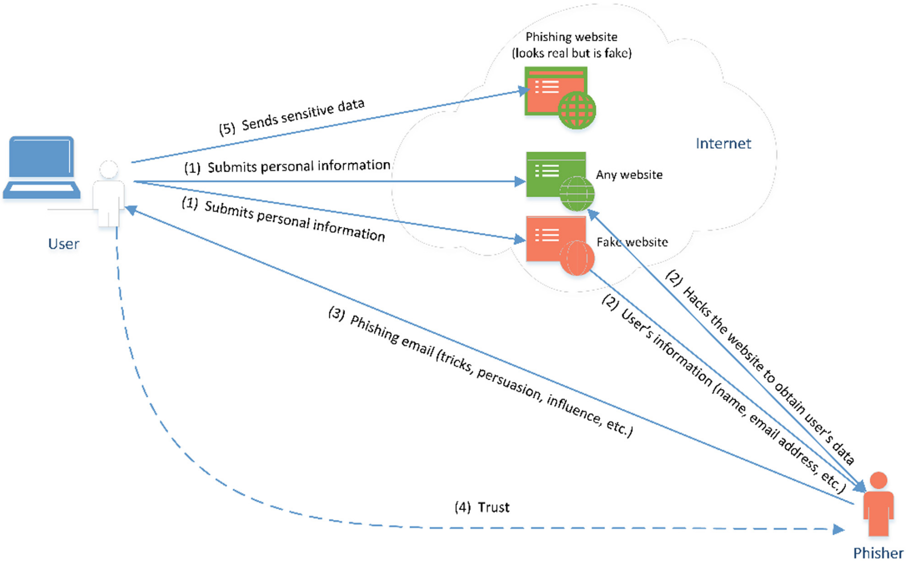
Phishing website
(looks real but is fake)
Internet
Any website
Fake website
(5) Sends sensitive data
(1) Submits personal information
(1) Submits personal information
(2) Hacks the website to obtain user's data
(2) User's information (name, email address, etc.)
(3) Phishing email (tricks, persuasion, influence, etc.)
(4) Trust
User
Phisher

Fig. 1. Example of a phishing attack flow

4.1 Suspicion

A recent study [4] shows that suspicion is one of the determinative factors in the email phishing attacks. The study also indicated that the users determine suspicion based on how they process emails, systematically or heuristically.

If the users believe that their cyber action is risky then they will systematically process the email but in case the users believe that their cyber action is safe then they will heuristically process it.

The heuristic-systematic model [62] proposes two information processing modes. In systematic processing, independent variables such as “source factors” directly impact on “argument acceptance process”. In heuristic processing, on the other hand, those independent variables may directly impact on accepting the message itself without paying enough attention to the arguments.

Based on the heuristic-systematic model, we conclude that people who highly involve the received email messages usually employ a “systematic processing” strategy which cause high suspicion about the phishing emails, whereas those who weakly involve the messages usually employ a “heuristic processing” strategy which cause low suspicion about the phishing emails.

For instance, a user who think that cyber activities are very risky usually has focus on the email’s message cues, where a user who think that cyber activities are quite safe usually has not enough focus on content cues.

4.2 Trust

Trust is defined in this context as the "willingness of taking a risk", which means sometimes people trust a beneficiary when they believe that this trust will be beneficial for them, even though they know that it is possible to lose something in this relation [63]. That is one of the reasons why a victim trusts a scammer.

Moreover, characteristics of both the trustor and the beneficiary and the situation of trustor are several important factors of trust. People with different cultural background, experiences, and personal character have different propensity to trust. Some people trust others more easily, whereas others do not trust people or entities in many situations [63]. However, the beneficiary's previous behaviour as well as his/her character are crucial factors [64, 65]. For instance, if someone had positive experiences with an e-shop, then the person will trust that e-shop much more than an e-shop associated with a negative previous experience.

As mentioned above, trust is one of the factors that affect a phishing attack. Therefore, it is crucial to consider the conditions of trust, which are "availability, competence, consistency, fairness (perceived equity), integrity, loyalty (perceived benevolence), openness, overall trust, promise fulfilment, and receptivity" [65].

Sometimes people trust a predictable person or entity, more than they would others. However, predictability is not enough to build trust, as maybe the reason of that predictability was something else, such as "controls" [63]. In addition, we cannot necessarily expect that a person is being fully rational when s/he trusts people or organisations, as people might trust entities based on limited information and in many cases "biased information" [66]. People usually trust a source of information which they perceive to be similar to themselves, such as family members or friends for example [64]. Thus, people cannot be sure that their trust in an email or on a website is completely justified. Phishers might use affective trust factors and as conditions to encourage victims to trust them.

4.3 Decision-Making

A phishing attack, especially in the case of spear phishing, is a scamming process. Usually there are at least two steps in this process where a victim makes decisions. Figure 2 illustrates an example of the role of decision-making in a phishing attack. In some cases, people decide "either to trust or not trust" others [67, 68], so the first step is when the victim decides to trust the attacker and the second step is right before sharing sensitive information with the attacker.

There are several parameters which influence the victim's decision to trust an attacker, including beliefs, values, and behaviours [69]. Decision-making is a process in itself and a sub-process of a phishing attack. Decision-making consists of the following phases: "perception activity", "mental representation", "data processing", "problem solving", and "choice of solution" [70]. Thus, a user's abilities in each phase can affect the result of the decision and eventually, affect the outcome of a phishing attack. For instance, a user with better data processing knowledge and skill is more likely to make a wiser decision. However, sometimes the decision-making process does not play a major role in a phishing attack. In some cases, users do not have enough awareness of the risks of sending personal information to a phisher, or they are not sensitive to potential losses. In such cases, phishing (A) is neutral, but making some money (B) is considerable. When a phisher tries to attract a victim by offering an impressive result, the user evaluates B-A as earned money [71]. Based on a previous study [71], we can define the following possible effects of the decision-making factor in a phishing attack:

- If the person believes that the probability of gain is high, then the effect of the decision is low.
- If the person believes that the probability of loss is high, then the individual most likely will not go for it, so the effect of the decision is low.
- If the person believes that the probability of gain or loss is low, then the effect of the decision is high.

Hence, decision-making can play a major role in a phishing attack when the user believes that the chance of either utility or loss is low.

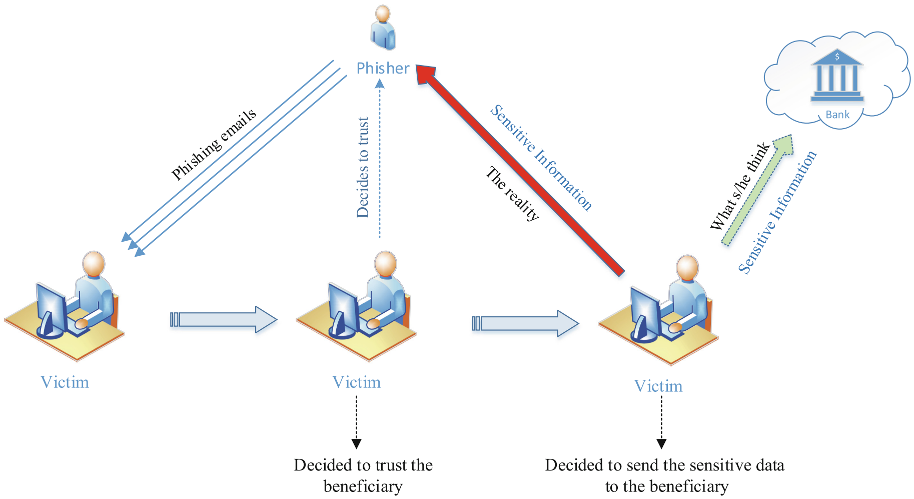

Fig. 2. Decision-makings in phishing attacks

4.4 Prediction

Phishers increase their resemblance with the targeted organisation in order to encourage the victim to believe that the phisher is who s/he claimed. This happens because people "predict by similarity" [72].

The individual's previous experience, as well as the person's knowledge, information, and/or experience with this particular type of phishing or the phisher, will affect the user's prediction in a given phishing attempt. However, the level of individual's "expected accuracy of prediction" will affect the effectiveness of evidences and his/her prior information about the particular phishing attack/attacker [72]. For instance, if the user's opinion or guess about a specific phishing is that it probably is not an attack, then the person might predict that it is a normal communication, even when the user has a degree of knowledge about phishing attacks. When a user is at the stage of making a decision to share or not to share sensitive data with a phisher, then some examples of the individual's prior information and other factors which can affect his/her prediction can be considered to be:

- Previous awareness and information about cybercrimes, especially phishing attacks, previous phishing experience, level of trust to the entity, knowledge about sensitive data, and risks of sharing the sensitive information with others.
- Similarity of the phisher to the claimed person or entity, how attractive is the phisher's offer, the phisher enforcement, real-time information, the user's impression of the offer, and the user's Emotional Quotient (EQ).

Where descriptions of what may influence a person's prediction are not available or are very limited, it is possible that the person makes a prediction based on a base rate information [72]. If a person does not receive any awareness about phishing attacks or no guidance or alarm is provided to warn of a phishing attack, or this person does not take advantages of a safeguard which is in place, then the individual might only rely on her/his prior understanding and knowledge of phishing attacks and/or the attacker.

5 Phisher's Tactics

Phishing scammers use an individual's behavioural weaknesses to offer attractive promotions as well as other techniques to trick the person into fulfilling the desired actions.

5.1 Scams and Tricks

The root causes of digital social engineering scams are very similar to the scams that happen in the real world. In both cases, the scammers use techniques and tricks to gain the victim's trust. They target the victims' psychological behaviours, and use the weaknesses of those behaviours to build a strong trust. They use the discovered psychological behaviours to design and create a scam. For instance, a phisher may find out that the victim is a person who usually tends to help others, then the scammer running a scam by feigning that they need a person to help them [73].

One of the reasons why phishing still works is because some people desire to take a gamble [74]. Therefore, an attractive prize or promotion could be enough to get them into a trap.

There are some "motivational and cognitive sources of errors" when people assess a phishing or a phisher. A phisher can use errors such as "visceral influences", "reduced motivation for information processing", "preference for confirmation", "lack of self-control", "mood regulation and phantom fixation", "sensation seeking", "liking and similarity", "reciprocation", "commitment and consistency", "reduced cognitive abilities", "positive illusions", "background knowledge and overconfidence", "norm activation", "false consensus", "authority", "social proof", "alter casting" [74], to phish.

5.2 Persuasion and Influence

There are individuals who usually desire to say yes to demands made by others, because they like reacting to “assertions of authority” [75]. They respond to others’ demands even to someone who does not have the related authority. They prefer to fulfil a request or a demand, instead of investigating and verifying the authenticity of the demander. That is why when a phisher sends a fake email, e.g. from a bank, and informs them that “you need to change your password”, then they do exactly what the phisher told them to do.

Moreover, “people have a natural tendency to think that a statement reflects the true attitude of the person who made it”, and also some people usually tend to do what others do or to say what others say, which “may prompt them to take actions that is against their self-interest without taking the time to consider them more deeply” [75].

There are two ways that a phisher may choose to push a victim to fulfil the demand [75]:

- “Central route to persuasion”
  The phishing message contains very “systematic and logical” reasoning which motivates the victim to rationally think and cogitate on the statements, and in the end to do whatever the phisher wants. The phisher has carefully designed the scenario and the argument, and knows the victim’s conclusion.
- “Peripheral route to persuasion”
  A phisher leads the victim to do the request without thinking about it. The phisher uses “mental shortcuts to bypass logical argument”. For example, the victims receive an email informing them that they won thousands of dollars and a very expensive laptop in a recent lottery promotion. This fantastic prize would stimulate many people to give personal information about themselves and can cause people to fall into the phishing trap.

5.3 Visceral Influence

A visceral motivation can cause less thinking about the legitimacy of transactions, as the person’s focus is on activities that could satisfy the visceral needs. In this situation, instead of rationally thinking about a given situation and analysing it accordingly, people usually do not care about the outcomes of their actions and make gut-feeling decisions. The influences of visceral factors are categorised to “low-level, middle-level, and high-level” [76] as defined below:

- Low-level: reasonable behaviour;
- Middle-level: people behaving in an opposite way to their actual interests, leading to them being upset with what they did, as they believe that they made an unreasonable decision;
- High-level: not making reasonable decisions.

Phishers create messages containing a scam reward and scam cues. Two types of scam rewards are “reward proximity” and “vividness” [77]:

- Reward proximity: if the phisher offers an easily and quickly-achievable reward, then it makes the individual hungrier than when a reward is not quickly-achievable, even if the value of the reward which is not quickly-achievable is higher.
- Vividness: when the phisher offers a very tangible reward, then it will be highly attractive for the victim. Professional phishers create different rewards for different targets groups to make each reward more clear and understandable for the related group of victims.

A person with low visceral influence is more likely to focus on scam cues, whereas one with high visceral influence is more likely to focus on the scam rewards. A victim who has high focus on the scam reward might get hooked by the phishing attack if s/he has low self-control, for example, and a victim who focuses on scam cues might get hooked if s/he has a low attention to the cues, in addition to having a high level of "social isolation", "cognitive impairment", "gullibility", "susceptibility to interpersonal influence", and/or low level of "skepticism", and/or "scam knowledge" factors [77].

However, even people with enough scam knowledge may follow a phishing cue if they enjoy activities such as gambling, for example. One of the reasons why those who have scam knowledge may still fall into a phishing trap is that sometimes experience is in opposition to knowledge, and that abnormal conditions may increase the effect of feelings on judgments [78]. That is a reason why some people process all the received emails even when they know about phishing attacks. It is therefore important to focus on the conditions which lead to decision-making. It is of crucial importance to keep in mind that visceral factors can influence behaviour even without "conscious cognitive mediation" [79]. For example, a person who is not hungry but starts eating just because someone is eating a sandwich in front of them [80].

6 Discussion

One of the techniques that scammers utilise to obtain individuals' sensitive data is social engineering [60]. The focus of this article is on the root causes of social engineering subterfuge in phishing attacks. A series of potential psychological and sociological effects have been identified.

There are several methods for root-causes analysis such as "Events and Causal Factors Charting", "Tree Diagrams", "Why-Why Chart", "Storytelling", and "Realitycharting" [81]. The Ishikawa Fishbone diagram [82] is a cause and effect analysis technique, which is useful for arranging the causes of a problem by focusing on potential factors in an organised way [83]. All the root cause analysis techniques and methods have useful features, however the Ishikawa Fishbone diagram was chosen to present the root causes of phishing attacks, which have been identified in this paper, as it is deemed to be a suitable technique to structure, categorise, as well as clearly illustrate all the extracted root causes.

Figure 3 presents the recognised root causes of phishing scams. This diagram consists of a main body, seven branches, and three sub-branches representing the grouped causes that are investigated in this paper. The presented extendable cause-and-effect diagram is a starting point, and future phishing causes could be added to the diagram.

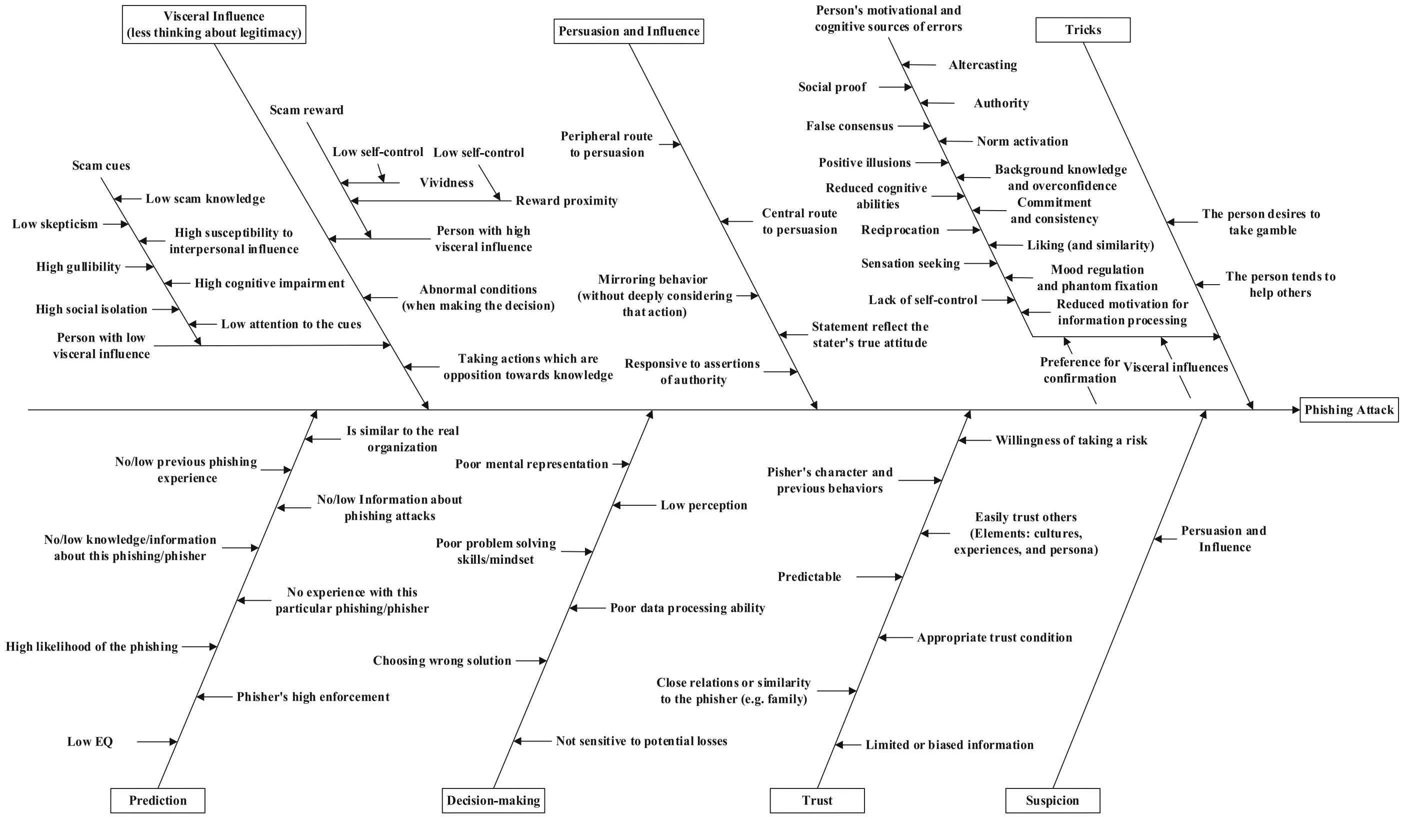

Fig. 3. Fishbone diagram of phishing attacks

Mitigating the identified causes will reduce the probability of phishing scams. Thus, focusing on the root causes to find and utilise appropriate mitigating techniques and solutions is fundamental to tackle phishing attacks from the root.

By using a psychological test, we can measure a specific cognitive behavior of a user. Then we can test the user's vulnerability to a simulated phishing attack which is founded on one of the listed root-causes. By choosing a sample of random internet users and testing different root-causes, we can describe the degree of relationship between different types of phishing attacks and their related cognitive behaviors.

If we identify an individual's weaknesses, for example by measuring his/her behaviors on one or some root-causes, then we would be able to design and provide improvement programs, such as specific trainings, to immune the person against that type of phishing attacks.

7 Conclusion

Many techniques, solutions, and tools have been developed to prevent or at least reduce the number of successful phishing attacks. Some of these techniques try to stop phishing emails or websites, whereas others try to notify or alert the user. There are also other solutions available, such as improving people's awareness of phishing scams. However, none of these solutions have so far managed to prevent phishing attacks a hundred per cent. Phishers are always developing new scams that the current anti-phishing techniques cannot detect and/or stop. Furthermore, they use human cognitive and behavioral attributes to design new tricks. This paper has identified and attempted to categorise some of the factors that phishers might use to phish the victims.

Future studies may recognise other root causes of phishing which can then be added to the cause-and-effect diagram presented in this paper. Meanwhile, the root causes identified can already be used to develop new anti-phishing techniques which can proactively prevent the future phishing scam, whether focused on the tools used by phishers or on the users who ultimately make the decisions.

References

1. Chang, E.H., Chiew, K.L., Sze, S.N., Tiong, W.K.: Phishing detection via identification of website identity. In: International Conference on IT Convergence and Security (ICITCS), pp. 1–4 (2013)
2. Li, S., Schmitz, R.: A novel anti-phishing framework based on honeypots. In: eCrime Researchers Summit, eCRIME 2009, pp. 1–13 (2009)
3. Harrison, B., Vishwanath, A., Rao, R.: A user-centered approach to phishing susceptibility: the role of a suspicious personality in protecting against phishing. In: 2016 49th Hawaii International Conference on System Sciences (HICSS), pp. 5628–5634. IEEE (2016)
4. Vishwanath, A., Harrison, B., Ng, Y.J.: Suspicion, cognition, and automaticity model of phishing susceptibility. Commun. Res. (2016). https://doi.org/10.1177/0093650215627483
5. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: writing a literature review. MIS Q. **26**, xiii–xxiii (2002)

6. Tayade, P.C., Wadhe, A.P.: Review paper on privacy preservation through phishing email filter. Int. J. Eng. Trends Technol. (IJETT) **9**, 4 (2014)
7. Zhuang, W., Jiang, Q., Xiong, T.: An intelligent anti-phishing strategy model for phishing website detection. In: 2012 32nd International Conference on Distributed Computing Systems Workshops, pp. 51–56 (2012)
8. Hong, J.: The state of phishing attacks. Commun. ACM **55**, 74–81 (2012)
9. Lynch, J.: Identity theft in cyberspace: crime control methods and their effectiveness in combating phishing attacks. Berkeley Technol. Law J. **20**, 259 (2005)
10. Jakobsson, M., Ratkiewicz, J.: Designing ethical phishing experiments: a study of (ROT13) rOnl query features. In: Proceedings of the 15th International Conference on World Wide Web, pp. 513–522. ACM, Edinburgh (2006)
11. Bergholz, A., De Beer, J., Glahn, S., Moens, M.-F., Paaß, G., Strobel, S.: New filtering approaches for phishing email. J. Comput. Secur. **18**, 7–35 (2010)
12. Chandrasekaran, M., Karayanan, K., Upadhyaya, S.: Towards phishing e-mail detection based on their structural properties. In: New York State Cyber Security Conference (2006)
13. Rigoutsos, I., Huynh, T.: Chung-Kwei: a pattern-discovery-based system for the automatic identification of unsolicited E-mail messages (SPAM). In: CEAS: First Conference on Email and Anti-Spam (2004)
14. Fette, I., Sadeh, N., Tomasic, A.: Learning to detect phishing emails. In: Proceedings of the 16th International Conference on World Wide Web, pp. 649–656. ACM, Banff (2007)
15. Toolan, F., Carthy, J.: Phishing detection using classifier ensembles. In: eCrime Researchers Summit, eCRIME 2009, pp. 1–9 (2009)
16. Herzberg, A.: DNS-based email sender authentication mechanisms: a critical review. Comput. Secur. **28**, 731–742 (2009)
17. Yu, W.D., Nargundkar, S., Tiruthani, N.: PhishCatch - a phishing detection tool. In: 33rd Annual IEEE International Computer Software and Applications Conference, COMPSAC 2009, pp. 451–456 (2009)
18. Hamid, I.R.A., Abawajy, J.: Hybrid feature selection for phishing email detection. In: Xiang, Y., Cuzzocrea, A., Hobbs, M., Zhou, W. (eds.) ICA3PP 2011. LNCS, vol. 7017, pp. 266–275. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24669-2_26
19. Ma, L., Ofoghi, B., Watters, P., Brown, S.: Detecting phishing emails using hybrid features. In: Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, UIC-ATC 2009, pp. 493–497 (2009)
20. Zhang, Y., Hong, J.I., Cranor, L.F.: Cantina: a content-based approach to detecting phishing web sites. In: Proceedings of the 16th International Conference on World Wide Web, pp. 639–648. ACM, Banff (2007)
21. Chen, T.-C., Dick, S., Miller, J.: Detecting visually similar web pages: application to phishing detection. ACM Trans. Internet Technol. **10**, 1–38 (2010)
22. Rosiello, A.P., Kirda, E., Ferrandi, F.: A layout-similarity-based approach for detecting phishing pages. In: Third International Conference on Security and Privacy in Communications Networks and the Workshops, SecureComm 2007, pp. 454–463. IEEE (2007)
23. Liu, W., Deng, X., Huang, G., Fu, A.Y.: An antiphishing strategy based on visual similarity assessment. IEEE Internet Comput. **10**, 58 (2006)
24. Zhou, Y., Zhang, Y., Xiao, J., Wang, Y., Lin, W.: Visual similarity based anti-phishing with the combination of local and global features. In: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 189–196 (2014)
25. Chen, T.-C., Stepan, T., Dick, S., Miller, J.: An anti-phishing system employing diffused information. ACM Trans. Inf. Syst. Secur. (TISSEC) **16**, 16 (2014)
26. Chou, N., Ledesma, R., Teraguchi, Y., Mitchell, J.C.: Client-side defense against web-based identity theft. In: NDSS. The Internet Society (2004)

27. Garera, S., Provos, N., Chew, M., Rubin, A.D.: A framework for detection and measurement of phishing attacks. In: Proceedings of the 2007 ACM Workshop on Recurring Malcode, pp. 1–8. ACM, Alexandria (2007)
28. Nguyen, L.A.T., To, B.L., Nguyen, H.K., Nguyen, M.H.: A novel approach for phishing detection using URL-based heuristic. In: International Conference on Computing, Management and Telecommunications (ComManTel), pp. 298–303 (2014)
29. Wu, M., Miller, R.C., Little, G.: Web wallet: preventing phishing attacks by revealing user intentions. In: Proceedings of the Second Symposium on Usable Privacy and Security, pp. 102–113. ACM (2006)
30. Kim, Y.-G., Cho, S., Lee, J.-S., Lee, M.-S., Kim, I.H., Kim, S.H.: Method for evaluating the security risk of a website against phishing attacks. In: Yang, C.C., et al. (eds.) ISI 2008. LNCS, vol. 5075, pp. 21–31. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-69304-8_3
31. Cao, Y., Han, W., Le, Y.: Anti-phishing based on automated individual white-list. In: Proceedings of the 4th ACM Workshop on Digital Identity Management, pp. 51–60. ACM, Alexandria (2008)
32. Dong, X., Clark, J.A., Jacob, J.L.: Defending the weakest link: phishing websites detection by analysing user behaviours. Telecommun. Syst. **45**, 215–226 (2010)
33. Likarish, P., Eunjin, J., Dunbar, D., Hansen, T.E., Hourcade, J.P.: B-APT: Bayesian anti-phishing toolbar. In: International Conference on Communications, ICC 2008, pp. 1745–1749. IEEE (2008)
34. Prakash, P., Kumar, M., Kompella, R.R., Gupta, M.: PhishNet: predictive blacklisting to detect phishing attacks. In: 2010 Proceedings IEEE, INFOCOM, pp. 1–5 (2010)
35. Whittaker, C., Ryner, B., Nazif, M.: Large-scale automatic classification of phishing pages. In: NDSS. The Internet Society (2010)
36. Bo, H., Wei, W., Liming, W., Guanggang, G., Yali, X., Xiaodong, L., Wei, M.: A hybrid system to find & fight phishing attacks actively. In: Proceedings of the 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, vol. 1, pp. 506–509. IEEE Computer Society (2011)
37. Marchal, S., Armano, G., Grondahl, T., Saari, K., Singh, N., Asokan, N.: Off-the-Hook: an efficient and usable client-side phishing prevention application. IEEE Trans. Comput. **PP**, 1 (2017)
38. Braun, B., Johns, M., Koestler, J., Posegga, J.: PhishSafe: leveraging modern JavaScript API's for transparent and robust protection. In: Proceedings of the 4th ACM Conference on Data and Application Security and Privacy, pp. 61–72. ACM, San Antonio (2014)
39. Dhamija, R., Tygar, J.D.: The battle against phishing: dynamic security skins. In: Proceedings of the 2005 Symposium on Usable Privacy and Security, pp. 77–88. ACM, Pittsburgh (2005)
40. Huang, C.-Y., Ma, S.-P., Chen, K.-T.: Using one-time passwords to prevent password phishing attacks. J. Netw. Comput. Appl. **34**, 1292–1301 (2011)
41. Yee, K.-P., Sitaker, K.: Passpet: convenient password management and phishing protection. In: Proceedings of the Second Symposium on Usable Privacy and Security, pp. 32–43. ACM, Pittsburgh (2006)
42. Husák, M., Cegan, J.: PhiGARo: automatic phishing detection and incident response framework. In: 2014 Ninth International Conference on Availability, Reliability and Security, pp. 295–302 (2014)
43. Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J.C.: Stronger password authentication using browser extensions. In: Usenix Security, pp. 17–32. Baltimore (2005)

44. Bignell, K.B.: Authentication in an internet banking environment: towards developing a strategy for fraud detection. In: International Conference on Internet Surveillance and Protection (ICISP 2006), p. 23 (2006)
45. Steel, C.M., Lu, C.-T.: Impersonator identification through dynamic fingerprinting. Digit. Investig. **5**, 60–70 (2008)
46. Ramachandran, A., Feamster, N., Krishnamurthy, B., Spatscheck, O., Van der Merwe, J.: Fishing for phishing from the network stream. Technical report (2008)
47. Li, S., Schmitz, R.: A novel anti-phishing framework based on honeypots. In: 2009 eCrime Researchers Summit, pp. 1–13 (2009)
48. Han, X., Kheir, N., Balzarotti, D.: PhishEye: live monitoring of sandboxed phishing kits. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1402–1413. ACM (2016)
49. Alnajim, A., Munro, M.: An evaluation of users' anti-phishing knowledge retention. In: International Conference on Information Management and Engineering, ICIME 2009, pp. 210–214. IEEE (2009)
50. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E.: Protecting people from phishing: the design and evaluation of an embedded training email system. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 905–914. ACM (2007)
51. Yang, W., Xiong, A., Chen, J., Proctor, R.W., Li, N.: Use of phishing training to improve security warning compliance: evidence from a field experiment. In: Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp, pp. 52–61. ACM, Hanover (2017)
52. Bose, I., Leung, A.C.M.: Unveiling the mask of phishing: threats, preventive measures, and responsibilities. Commun. Assoc. Inf. Syst. **19**, 24 (2007)
53. European Commission: Reform of EU data protection rules (2016)
54. https://www.congress.gov/bill/109th-congress/senate-bill/472/text. Accessed 11 May 2016
55. UK Legislation: Fraud Act 2006. UK Legislation (2006)
56. BaFin: Rundschreiben 4/2015 (BA): Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (2015)
57. PCWorld. http://www.pcworld.com/article/135293/article.html. Accessed 09 Nov 2015
58. Suryavanshi, N., Jain, A.: Phishing detection in selected feature using modified SVM-PSO. IJRCCT **5**, 208–214 (2016)
59. Chaudhry, J.A., Chaudhry, S.A., Rittenhouse, R.G.: Phishing attacks and defenses. Int. J. Secur. its Appl. **10**, 247–256 (2016)
60. Anti-Phishing Working Group: http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf. Accessed 11 Aug 2106
61. Ramamoorti, S., Olsen, W.: Fraud: the human factor; many discount behavioral explanations for fraud, but as the incidence of fraud continues to grow, placing the spotlight on behavioral factors may be an important approach not only to detection, but to deterrence as well. Financ. Exec. **23**, 53–56 (2007)
62. Chaiken, S.: Heuristic versus systematic information processing and the use of source versus message cues in persuasion. J. Pers. Soc. Psychol. **39**, 752–766 (1980)
63. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. Acad. Manag. Rev. **20**, 709–734 (1995)
64. Alesina, A., La Ferrara, E.: Who trusts others? J. Public Econ. **85**, 207–234 (2002)
65. Butler, J.K.: Toward understanding and measuring conditions of trust: evolution of a conditions of trust inventory. J. Manag. **17**, 643–663 (1991)
66. Khodyakov, D.: Trust as a process a three-dimensional approach. Sociology **41**, 115–132 (2007)

67. Klein, D.B.: Knowledge and Coordination: A Liberal Interpretation. Oxford University Press, Oxford (2011)
68. Huang, J., Nicol, D.: A Formal-Semantics-Based Calculus of Trust. IEEE Internet Comput. **14**, 38–46 (2010)
69. Oliveira, A.: A discussion of rational and psychological decision making theories and models: the search for a cultural-ethical decision making model. Electron. J. Bus. Ethics Organ. Stud. **12**, 12–13 (2007)
70. Bezerra, S., Cherruault, Y., Fourcade, J., Veron, G.: A mathematical model for the human decision-making process. Math. Comput. Model. **24**, 21–26 (1996)
71. Tversky, A., Kahneman, D.: Rational choice and the framing of decisions. J. Bus. **59**, S251–S278 (1986)
72. Kahneman, D., Tversky, A.: On the psychology of prediction. Psychol. Rev. **80**, 237 (1973)
73. Mitnick, K.D., Simon, W.L.: The Art of Deception: Controlling the Human Element of Security. Wiley, Hoboken (2011)
74. Lea, S., Fischer, P., Evans, K.: The psychology of scams: provoking and committing errors of judgement. Report for the Office of Fair Trading (2009). www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf
75. Rusch, J.J.: The "social engineering" of internet fraud. In: Internet Society Annual Conference (1999). http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm
76. Loewenstein, G.: Out of control: visceral influences on behavior. Organ. Behav. Hum. Decis. Process. **65**, 272–292 (1996)
77. Langenderfer, J., Shimp, T.A.: Consumer vulnerability to scams, swindles, and fraud: a new theory of visceral influences on persuasion. Psychol. Mark. **18**, 763–783 (2001)
78. Strack, F., Neumann, R.: "The spirit is willing, but the flesh is weak": beyond mind-body interactions in human decision-making. Organ. Behav. Hum. Decis. Process. **65**, 300–304 (1996)
79. Bolles, R.C.: Theory of Motivation. HarperCollins Publishers, New York (1975)
80. Pribram, K.H.: Emotion: a neurobehavioral analysis. In: Approaches to Emotion, pp. 13–38 (1984)
81. Gano, D.L.: Comparison of common root cause analysis tools and methods. In: Apollo Root Cause Analysis-A New Way of Thinking (2007)
82. Ishikawa, K.: Introduction to Quality Control. Productivity Press, Cambridge (1990)
83. Juran, J.M., Godfrey, A.B.: Quality Handbook. Republished McGraw-Hill, New York (1999)