The Effects of Phishing Emails: A Meta-Analysis

HARIS MOTIKA, University of Twente, The Netherlands

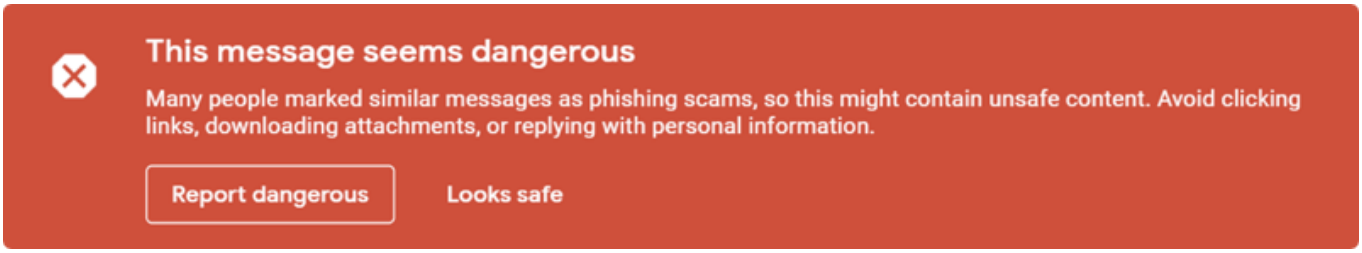

Fig. 1. Warning message for a likely phishing email

Over the years email has evolved from more than just a medium for interpersonal communications. With this have come some negatives, such as individuals or groups trying to exploit users. This has been done by the use of phishing emails. Phishing emails are attacks that attempt to trick people into releasing sensitive information, by using techniques to make it seem like the information is requested from a legitimate source. How successful have these phishing emails been at fooling users and why? To find an answer to these questions a literature research and meta-analysis will be conducted.

Additional Key Words and Phrases: Analysis, Email, Impact, Phishing, Social Engineering

1 INTRODUCTION

With individuals having an ever growing digital footprint, email has become a standardized way for communications. This has been the case for people, organizations and most importantly businesses. It is projected that the amount of emails send per day will reach 347 billion by 2023 [87]. It has evolved beyond basic peer to peer communication. Exchanging information, exchanging data, account creation for websites and services, customer service and the list goes on [35]. Due to this it has become the essential form of communication for businesses and organizations. While the benefits emails provide are clear, there are certain risks affiliated with it. Emails are widely adopted and relatively easy to deploy on a large scale, which is a positive and a negative. Certain individuals and groups use emails to target users on a wide scale. They accomplish this by deploying phishing emails [87]. The goal of these phishing attacks is for the attackers to acquire sensitive information from the person being phished. This could be passwords, bank account information, scamming users into sending them money or other personal information [33].

Phishing is not a new phenomenon. The history of phishing goes back to the mid-1990s, when programs that targeted users and attempted to acquire their passwords were distributed on America Online (AOL). It was here where the term phishing was coined [81].Since the late 90s numerous studies have been done about phishing emails. These studies have been predominantly on counter measures [38]. A relatively small amount of studies have been conducted to figure out either how much people fall for phishing emails and why? Is it age related? Sex? Education? Cyber-security knowledge? Personality traits? Nationality? The emails itself?

There are two distinct types of phishing email most speak of, regular phishing and spear phishing. Regular phishing emails are deployed on a wide scale to to target a large pool of individuals and are therefore not personalized. Spear phishing emails are usually used on a smaller scale and are personalized for a specific individual or group of individuals [31].

Some of the studies that have attempted to uncover why people fall for phishing are as follows. Kumaraguru et al [57] conducted a real world user study with 515 participants, they found that age is a factor in phishing susceptibility, as participants in the 18-25 age group were significantly more likely to fall for phishing emails than those in older age groups. On the other hand they did not observe any significant difference in gender. Sheng et al. [85] conducted a roleplay phishing study with 1001 participants and likewise found that participants between the age of 18 and 25 were significantly more susceptible to phishing. However, unlike Kumararugu et al. [57], they found that sex was a factor, as women were significantly more likely to click on a phishing email and also go on to give information than men. Blythe et al [13] conducted a online survey of 224 people and found no significant difference between age. What they did find was that there was a significant interaction between age and sex, with the younger group (18-30) having a significantly large difference in men and women, which disappeared in the older groups (31-46 and 46+). Lin et al. [62] confirmed these findings, having also found no significant difference in age and sex itself, but when combined there was a significant difference in groups. But Parson et al. [77] who conducted a role play experiment with 117 participants, who were asked to manage 50 emails, found no significance nor relationship between age and gender.

The first study I could find that tested for personality difference was Pattionson et al. [79] who asked 117 participants to evaluate 50 emails, half of which were phishing emails. They used the Big Five Personality test in combination of these results to see if any of the big five personality traits were significant in users ability to

TScIT 37, July 8, 2022, Enschede, The Netherlands

recognize phishing emails. The Big Five Personality test, consists of five traits, extroversion, agreeableness, openness, conscientious and neuroticism [65, 71].

(1) Extroversion: More friendly and outgoing

(2) Agreeableness: More co-operative and eager to help other people.
(3) Openness: More willing to try new experiences, in general more curious.
(4) Conscientious: Organized, high self control and strong minded.
(5) Neuroticism: More irrational thoughts, experience negative feelings more.

[47]

They found that one of the 5 traits, was significant, as users who were more extroverted were better at recognizing phishing emails. Ayob et al. [7] found that 2 out of 5 Big Five personality traits were significant, extroversion and conscientiousness. But then there is Ge et al. [42] who found in their research that 3 out of 5 Big Five personality traits were significant, conscientiousness, openness and neuroticism.

When it relates to education, Parson et al. [77] who was previously mentioned also tested on educational level and found that for participants who did not know they were participating in a phishing email, therefore mimicking a real life scenario, participants with a higher level of education where significantly better at recognizing phishing emails. On the other hand Lui et al. [74] conducted a similar experiment over a period of 19 months among students and employees of several universities in the U.S. and found no significant difference in education.

For general security knowledge Wright et al.found that an increase of security knowledge in participants had an significant effect on deception success. Meanwhile Parson et al. [77] found a significant effect, only in participants who were explicitly told they were conducting a phishing test. Suggesting that in a real life scenario, there would be no significance.

For the cues, Parson et al. [76] (2015) conducted a test to find out what cues typically differentiate phishing emails from legitimate emails. They found that phishing emails were significantly more likely to contain incorrect spelling and grammatical errors. Consequently Wang et al. [90] found that grammar and visual presentation were significant in recognizing phishing emails, while Blythe et al. [13] did not necessarily find any significance in grammar and visual presentation, due to the fact that phishers have gotten better and presenting themselves as genuine emails.

Although the research into phishing emails goes back as far as the mid 1990s, most of this research has been focused on how to prevent users from being phished and creating tools to protect users from phishing email. However, why users fall for phishing emails and just how successful they are, has been relatively unexplored. Just what exactly is the impact of phishing emails? This paper will analyze existing literature and conduct a meta-analysis to find new insights into how harmful phishing emails have been. We will attempt to this by answering the following research question: How harmful are phishing emails?

To answer this question, the following sub-questions will be explored:

(1) How successful are phishing emails?

(2) What demographics are more susceptible to phishing emails?

2 METHODOLOGY

To anwser the research question at hand, a literature study and a meta analysis was performed. The studies on which this meta analysis was performed were acquired from the Scopus database. The Scopus database was queried on 24 May 2022, using the following query:

```
(TITLE-ABS-KEY((Phishing OR "social engineering") AND *mail* OR scam OR fraud OR simulation OR campaign* OR test* OR attack* AND NOT "machine learning" AND NOT covid* AND NOT corona AND NOT "deep learning" AND NOT "artificial intelligence" AND NOT "algorithm))
```

This search query resulted in 3407 records. These search terms were chosen to capture studies about phishing and social engineering that contained user experiments and to exclude studies pertaining to classification, deep learning, artificial intelligence and covid-19.

2.1 Eligibility criteria

Based on the eligibility criteria it would be decided to either include or exclude a study for the meta-analysis. Studies that did not meet the following eligibility criteria were excluded:

(1) Must be published in a scientific paper or PhD Thesis
(2) The manuscript must be written in English, Dutch or Bosnian; the author is proficient in these 3 languages.
(3) It should include some type of field or lab experiment
(4) There should be at least 20 observations, to avoid the possibility of results being based on random chance.
(5) No restriction regarding publication date.

2.2 Study Selection

Initially the titles and abstract of all 3407 studies were exported in Excel and screened for the eligibility criteria. This resulted in 316 relevant studies remaining, 3091 being excluded. These 3091 studies were excluded due to various reasons such as, not having human subjects, using computers for classifications, discussing about law and being about other forms of phishing. Of the remaining 316, 191 were determined to have some sort of experiment, with the other 125 being excluded from the data analysis and marked for possible context use. The 191 remaining studies were then screened full text for the eligibility criteria, which resulted in 81 studies being selected for the meta-analysis, excluding a further 110 studies. The reason these studies were excluded, was due to several reasons, such as: being a duplicate, being unavailable for full text analysis, not enough observations (<20) in experiment, no control groups in anti-phishing studies and no relevant data being available. If a paper was a duplicate, the most recently published version was chosen for the meta-analysis. Moreover for the studies that were selected, some had multiple experiments and were therefore coded as many

times. A flow chart depicting this process can be seen in Figure 2. Moreover below in Table 1 an overview of when the studies that were used were published can be seen, with a detailed breakdown of these studies in Table 2.

In total six predictors were chosen for the meta analysis, which will be used to come to a conclusion about why people fall for phishing emails. Age will look at, if certain age groups are more susceptible to phishing. Sex, will look if men or woman are more susceptible to phishing. Educational level will see if lower or higher educated people are more or as susceptible. Security knowledge, will see if people with general cyber-security knowledge are more, less or as susceptible. Cues will look if grammar (misspelling), visual representation (logo, style) and sender addresses (email sender) affect susceptibility to phishing.

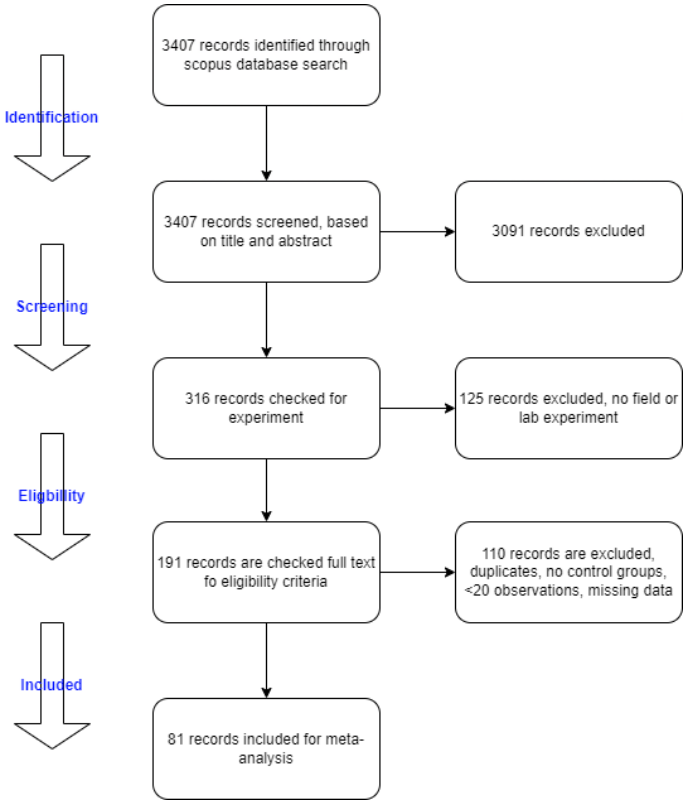

Fig. 2. Flow chart (Study Selection)

Table 1. Distribution of years from selected studies

Year	Number of Studies
2005	2
2007	5
2008	2
2009	2
2010	2
2011	2
2012	4
2013	5
2016	1
2017	9
2018	6
2019	12
2020	13
2021	8
2022	2

2.3 Codebook variables

Three different identifiers with variables were created to log the necessary data. These are as follows:

Study identifiers

(1) ID; identifier of the study (1-3407)
(2) Study; Author name + Year, e.g Desolda14
(3) Year; Year of publication e.g 2007

Population identifiers

(1) Age; average age of participant
(2) Female; amount of females among participants
(3) Nationality; origin of participants
(4) Education; No Diploma, High School, College and Mixed
(5) Population; Employees, Students, Adults, Children and Mixed
(6) nTotal; total sample size
(7) victims; amount of victims

Experiment identifiers

(1) Environment; Lab or Field experiment
(2) Test; type of test performed
  (a) Graphics, participants distinguish between emails and phishing emails
  (b) Rolepay, participants play a character and act out what they would do in an email scenario
  (c) Phishing attack, researches send out phishing emails and record data among subjects
(3) pre-study; where the participants aware that they were doing an experiment?
(4) pre-aware; where the participants aware that it was a study about phishing emails?
(5) mail-phish; amount of phishing emails that are send to or judged by the participant
(6) type-mail; type of mail send, regular phishing or spear phishing
(7) predictors

(a) Age
(b) Sex
(c) Personality
(d) Educational level
(e) Security knowledge
(f) Cues; Grammar, Visual representation and Sender address

2.4 Data Analysis

To answer the sub questions the following will be done. For sub-question 1. How successful are phishing emails? Click rates will be investigated, to accomplish this a proportions meta-analysis will be applied and the weighted average of regular and spear phishing emails will be taken to see how often people fall for phishing emails.

For sub-question 2. What demographics are more susceptible to phishing emails? Six different predictors will be looked at. For these predictors we will use the Standardized Mean Difference (SMD) [15]. SMD is a summary statistic that is used in meta-analyses when different studies assess the same predictor, but use a different statistic to measure it [37]. To convert all the acquired data to SMD we will use a effect size calculator, based on the work of Lipsey et al [63]. After acquiring all the necessary data, a tool called Comprehensive Meta-Analysis (CMA) will be used to perform the meta-analysis [16].

3 RESULTS

In total 81 studies were included in the analysis, 37 of which had statistical tests for one or multiple predictors. There were a total of N=99598 subjects, having k=81 observations. Based on k=36, there are N=7798 females. Not every study provided this information. [1–14, 18–30, 32, 34, 36, 39–62, 64, 66–70, 72–80, 82–86, 88–94]

3.1 Research Question 1

3.1.1 Click Rate. I looked at two distinct type of phishing emails, regular and spear. For regular phishing there are N=30,874 with k=14. Of these 30,874 subjects, 6039 opened the regular phishing email and clicked on a link, opened an attachment or gave out information. This results in an average click rate of $\frac{6039}{30,874} * 100 \approx 19,56\%$. In Table 3 the results of the proportions meta-analysis are displayed. Using a fixed model, so using the relative weights of the studies, a weighted average of 22,7% with a lower-upper limit of [22,2-23,2] is acquired. Using a random model, so having weights be distributed proportionality,a weighted average of 18,3% with a lower-upper limit of [12,5-26,2] is acquired.

Meanwhile for spear phishing this study finds N=39,853 with k=22. Of these 39,853 subjects, 10,072 opened the spear phishing email and clicked on a link, opened an attachment or gave out information. This results in an average click rate of $\frac{10,072}{39,853} * 100 \approx 25,73\%$. In Table 4 the results of the proportions meta-analysis can be seen. Using a fixed model, a weighted average of 25,7% with a lower-upper limit of [25,3-26,2] is acquired. Using a random model, a weighted average of 30,8% with a lower-upper limit of [24,6-37,7] is acquired.

3.2 Research Question 2

3.2.1 Age. Does age affect phishing susceptibility? This study finds N=1912 subjects with k=10 observations. The results of the SMD meta-analysis for age can be seen in Figure 5. An standardized mean difference of 0,230 with a lower- upper limit of [0.103-0.357] is found. As the confidence interval does not cross the line of no effect (0,00), this result is significant. This can also be checked with a hypothesis test using z=3,539 and p=0,000 (smaller than 0.001). An SMD between 0.0 and 0.2 indicates a small effect, so these results would suggest a small effect of age on phishing susceptibility, with older people being slightly more susceptible to phishing.

3.2.2 Sex. Does sex affect phishing susceptibility? This study finds N=12403 subjects with k=12 observations. The results of the SMD meta-analysis for sex can be seen in Figure 6. An standardized mean difference of 0,087 with a lower- upper limit of [-0,005-0,179] is found. As the confidence interval crosses the line of no effect (0.00), this result is not significant. This can also be checked with a hypothesis test using z=1,854 and p=0.064. This would suggest there is no difference between sex on phishing susceptibility.

3.2.3 Personality. Does personality affect phishing susceptibility? This study finds N=512 subjects with k=4 observations. The results of the SMD meta-analysis for personality can be seen in Figure 7. An standardized mean difference of 0,080 with a lower- upper limit of [-0,136-0,295] is found. As the confidence interval crosses the line of no effect (0.00), this result is not significant. This can also be checked with a hypothesis test using z=0,724 and p=0.469. For the five individual personality traits, the following results are acquired. For extroversion an standardized mean difference of -0,381 is found. For agreeableness an standardized mean difference of 0,205. For openness an standardized mean difference of 0,303. For Conscientious an standardized mean difference of -0.189. Lastly for neuroticism an standardized mean difference of 0,595 is acquired. In this case extroversion and neuroticism both did not cross the line of no effect (0,00) meaning they are significant. While we have 14 data points, these are divided over 4 studies. Due to this small sample size (k<10) we can not make any conclusive statements about this. As Borenstein et al. stated, a meta-analysis performed with less than 10 observations is very unreliable and should not be used to make reliable conclusions [17]. Moreover in the case of personality traits, several studies only reported data on traits they found significance on. For example Alseadoon et al. and Ayob et al. both found 2 out of 5 personality traits significant and they reported the respective statistical findings, but did not report the results of the other 3 personality traits. Therefore certain data was not captured here.

3.2.4 Educational level. Does education affect phishing susceptibility? This study finds N=812 subjects with k=3 observations (studies). An standardized mean difference of -0.140 with a lower- upper limit of [-0,534-0.253] is acquired. As the confidence interval crosses the line of no effect (0.00), this result is not significant. However similarly as Personality due, to the small sample size (k<10) we can not make any conclusive statements about this.

3.2.5 Security Knowledge. Does security knowledge affect phishing susceptibility? This study finds N=2448 subjects with k=3 observations (studies). An standardized mean difference of 0,117 with a lower- upper limit of [-0,014-0,248] is found. As the confidence interval crosses the line of no effect (0.00), this result is not significant. However similarly as Personality and Educational level due,

to the small sample size (k<10) we can not make any conclusive statements about this.

3.2.6 Cues. Do cues affect phishing susceptibility? This study finds N=604 subjects with k=3 observations (studies). Three separate cues are assessed; grammar, visual representation and sender addresses. For all cues in general, an standardized mean difference of 0.206 with a lower- upper limit of [0.006-0.406] is found. As the confidence interval does not cross the line of no effect (0.00), this result is significant. However similarly as Personality, Educational level and Security Knowledge due, to the small sample size (k<10) we can not make any conclusive statements about this.

4 CONCLUSION

We found that a significant amount of people fall for both regular and spear phishing emails and investigated possible reasons for this, by looking at six different predictors. With these results we can fully or partially answer our sub questions. For sub-question 1. How successful are phishing emails? Using a random model - assuming the populations is not the same in each study - we found for regular phishing a weighted average click rate of 18,3%. Meanwhile for spear phishing using a random model, we found a weighted average click rate of 30,8%. People fall for phishing emails at a high rate. This very worrying, as for regular phishing emails it is possible to send out mass mail campaigns. One could realistically target hundreds of thousands if not millions of people as long as you have their e-mail addresses. If 18,3% of these people fell for a phishing email, it would be very successful in what it said out to do. Moreover for spear phishing emails that are targeted towards specific users or groups, it is becoming easier and easier to acquire the necessary information to craft the spear phishing emails. The digital footprint of regular people is continuously increasing as people are posting more and more information about themselves on social media platforms. Information such as where they work, where they were born, what school they went to, birthdays, who they associate with etc. With a weighted average click rate of 30,8%, it is extremely effective at fooling users.

Secondly we wanted to know what demographics are more susceptible to phishing? We found out that age was a factor, albeit small, in phishing susceptibility, indicating that older people are more likely to fall for a phishing email. Meanwhile there was no difference in phishing susceptibility between different sexes. Individual personality traits, extroversion and neuroticism were both significant when it came to phishing susceptibility. However due to the small sample size, no reliable conclusion can be made about this. Similarly Educational level and Security knowledge were not significant, but due to a small sample size, no reliable conclusion can be made about this. Lastly Cues were significant when it came to phishing susceptibility, but due to a small sample size, no reliable conclusion could be made.

So to answer our main question, how harmful have phishing emails been? We saw that over the years phishing emails have evolved, becoming more and more like their genuine counter part. Spear phishing campaigns targeting specific users and groups have increased, with much easier access to personal information through social media platforms. Not only that, but numerous tools are being created and improved to send and create regular phishing emails on a massive scale. Given the success rate of both regular and spear phishing emails and what falling could lead to, one could say that phishing emails have been very harmful. This could be in both monetary loss or psychological damage.

4.1 Shortcomings

Having initially gone through the background of phishing experiments and their reports, we had thought that we would find a decent amount of studies that had similar ideas when it came to predictors. That proved to be true for age and gender, but education, personality, security knowledge and cues still seem to be relatively unexplored. A large problem was the overall lack of proper reporting in acquired papers. While numerous papers performed experiments and reported their findings, a good portion of these did not fully report the necessary data to include them in the meta-analysis. This meant that for certain predictors we ended up k<10 observations. Due to this, we can not reliably say whether or not these predictors significantly impact phishing susceptibility. As one of the main goals of this paper was to find out why people fall for phishing emails, this ends up as a big shortcoming.

4.2 Future Work

For future work, more research needs to be conducted and gathered on the six predictors. In particular for those we have k<10 observations. Personally I am interested in how the predictors influence each other. As we saw when looking at the background, several studies found that a predictor influenced phishing susceptibility. But when combing predictors, the effect of said predictor disappeared. As there is no agreed upon way to report the results of phishing experiments, I recommend for a standardized framework to be created. With this all relevant information and data would be reported for future meta-analyses. This could significantly increase the amount of studies that could be included in a meta-analysis and would allow us to make more reliable conclusions.

REFERENCES

[1] Ahmad Syukri Abdullah and Masnizah Mohd. 2019. Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector. 26–31. https://doi.org/10.1109/ICoCSec47621.2019.8970803

[2] Dania Aljeaid. 2020. Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. *Information* 11 (11 2020), 547. https://doi.org/10.3390/info11120547

[3] Ibrahim Alseadoon, Taizan Chan, Ernest Foo, and Juan Nieto. 2012. Who is More Susceptible to Phishing Emails? A Saudi Arabian Study. *ACIS 2012 : Proceedings of the 23rd Australasian Conference on Information Systems.*

[4] Mohammed Alwanain. 2019. Effects of user-awareness on the detection of phishing emails: A case study. *International Journal of Innovative Technology and Exploring Engineering* 8 (01 2019), 480–484.

[5] Mohammed I Alwanain. 2019. An Evaluation of User Awareness for the Detection of Phishing Emails. *International Journal of Advanced Computer Science and Applications* 10, 10 (2019). https://doi.org/10.14569/IJACSA.2019.0101046

[6] Vivek Anandpara, Andrew Dingman, Markus Jakobsson, Debin Liu, and Heather Roinestad. 2007. Phishing IQ Tests Measure Fear, Not Ability. 362–366. https://doi.org/10.1007/978-3-540-77366-5_33

[7] Zalina Ayob and George Weir. 2021. *Is Human Behavior the Real Challenge in Combating Phishing.* 27–38. https://doi.org/10.1007/978-981-33-4062-6_3

[8] Aurélien Baillon, Jeroen de Bruin, Aysil Emirmahmutoglu, Evelien van de Veer, and Bram van Dijk. 2019. Informing, simulating experience, or both: A field experiment on phishing risks. *PLOS ONE* 14, 12 (Dec. 2019), e0224216. https://doi.org/10.1371/journal.pone.0224216

[9] Taimur Bakhshi. 2017. Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. In *2017 13th International Conference on Emerging Technologies (ICET)*. 1–6. https://doi.org/10.1109/ICET.2017.8281653

[10] Taimur Bakhshi, Maria Papadaki, and Steven Furnell. 2008. A Practical Assessment of Social Engineering Vulnerabilities. In *HAISA*.

[11] Piers Bayl-Smith, Daniel Sturman, and Mark Wiggins. 2020. *Cue Utilization, Phishing Feature and Phishing Email Detection*. 56–70. https://doi.org/10.1007/978-3-030-54455-3_5

[12] Zinaida Benenson, Freya Gassmann, and Robert Landwirth. 2017. Unpacking Spear Phishing Susceptibility. 610–627. https://doi.org/10.1007/978-3-319-70278-0_39

[13] Mark Blythe, Helen Petrie, and John Clark. 2011. F for fake: four studies on how we fall for phish. 3469–3478. https://doi.org/10.1145/1978942.1979459

[14] Marco De Bona and Federica Paci. 2020. A real world study on employees' susceptibility to phishing attacks. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*. ACM. https://doi.org/10.1145/3407023.3409179

[15] Michael Borenstein, Larry V. hedges, Julian PT Higgins, and Hannah R. Rothstein. 2010. A basic introduction to fixed-effect and random-effects models for meta-analysis. *Research Synthesis Methods* 1 (2010), 97–111. https://doi.org/10.1002/jrsm.12

[16] Michael Borenstein, Larry Hedges, Julian Higgins, and Hannah Rothstein. 2021. Comprehensive Meta-Analysis V3. https://www.meta-analysis.com/index.php?cart=BQ9J6945164

[17] Michael Borenstein, Larry V Hedges, Julian Higgins, and Hannah Rothstein. 2009. *Introduction to meta-analysis*. Wiley-Blackwell, Hoboken, NJ.

[18] Jan-Willem Bullée, Lorena Montoya, Marianne Junger, and Pieter Hartel. 2017. Spear phishing in organisations explained. *Information and Computer Security* 25 (10 2017), 00–00. https://doi.org/10.1108/ICS-03-2017-0009

[19] AJ Burns, M. Johnson, and Deanna Caputo. 2019. Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce* 29 (01 2019), 24–39. https://doi.org/10.1080/10919392.2019.1552745

[20] Marcus Butavicius, Kathryn Parsons, Malcolm Pattinson, and Agata McCormac. 2016. Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. (05 2016).

[21] Matthew Canham, Clay Posey, and Michael Constantino. 2022. Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks. *Frontiers in Education* 6 (01 2022). https://doi.org/10.3389/feduc.2021.807277

[22] Matthew Canham, Clay Posey, Delainey Strickland, and Michael Constantino. 2021. Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards. *SAGE Open* 11 (01 2021), 215824402199065. https://doi.org/10.1177/2158244021990656

[23] Deanna D. Caputo, Shari Lawrence Pfleeger, Jesse D. Freeman, and M. Eric Johnson. 2014. Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security Privacy* 12, 1 (2014), 28–38. https://doi.org/10.1109/MSP.2013.106

[24] Anthony Carella, Murat Kotsoev, and T.M. Truta. 2017. Impact of security awareness training on phishing click-through rates. 4458–4466. https://doi.org/10.1109/BigData.2017.8258485

[25] Surachai Chatchalermpun, Pongpisit Wuttidittachotti, and Therdpong Daengsi. 2020. Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand. 283–286. https://doi.org/10.1109/ISCAIE47305.2020.9108832

[26] David Cook and Premankit Sannd. 2018. Older Adults and the Authenticity of Emails: Grammar, Syntax, and Compositional Indicators of Social Engineering in Ransomware and Phishing Attacks. https://doi.org/10.1109/ICINPRO43533.2018.9096878

[27] Tom Cuchta, Brian Blackwood, Thomas Devine, Robert Niichel, Kristina Daniels, Caleb Lutjens, Sydney Maibach, and Ryan Stephenson. 2019. Human Risk Factors in Cybersecurity. 87–92. https://doi.org/10.1145/3349266.3351407

[28] Shelby Curtis, Prashanth Rajivan, Daniel Jones, and Cleotilde Gonzalez. 2018. Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior* 87 (05 2018). https://doi.org/10.1016/j.chb.2018.05.037

[29] Therdpong Daengsi, Phisit Pornpongtechavanich, and Pongpisit Wuttidittachotti. 2021. Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies* 27, 4 (Nov. 2021), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

[30] Ali Darwish, Ahmed Zarka, and Fadi Aloul. 2012. Towards understanding phishing victims' profile. *2012 International Conference on Computer Systems and Industrial Informatics, ICCSII 2012*, 1–5. https://doi.org/10.1109/ICCSII.2012.6454454

[31] Prateek Dewan, Anand Kashyap, and Ponnurangam Kumaraguru. 2014. Analyzing social and stylometric features to identify spear phishing emails. In *2014 APWG Symposium on Electronic Crime Research (eCrime)*. 1–13. https://doi.org/10.1109/ECRIME.2014.6963160

[32] Julie Downs, Mandy Lanyon, and Lorrie Cranor. 2007. Behavioral response to phishing risk. *Proceedings of the Anti-phishing Working Groups 2nd Annual ECrime Researchers Summit*, 37–44. https://doi.org/10.1145/1299015.1299019

[33] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. 2006. Decision Strategies and Susceptibility to Phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) *(SOUPS '06)*. Association for Computing Machinery, New York, NY, USA, 79–90. https://doi.org/10.1145/1143120.1143131

[34] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. 2006. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security - SOUPS '06*. ACM Press. https://doi.org/10.1145/1143120.1143131

[35] Christa Durscheid, Carmen Frehner, Susan C Herring, Dieter Stein, and Tuija Virtanen. 2013. Email communication. *Handbooks of Pragmatics [HOPS]* 9 (2013), 35–54.

[36] Natalie Ebner, Donovan Ellis, Tian Lin, Harold Rocha, Huizi Yang, Sandeep Dommaraju, Adam Soliman, Damon Woodard, Gary Turner, R. Nathan Spreng, and Daniela Oliveira. 2018. Uncovering Susceptibility Risk to Online Deception in Aging. *The journals of gerontology. Series B, Psychological sciences and social sciences* 75 (04 2018). https://doi.org/10.1093/geronb/gby036

[37] Stephen Faraone. 2008. Interpreting estimates of treatment effects: Implications for managed care. *P T : a peer-reviewed journal for formulary management* 33 (12 2008), 700–11.

[38] Ana Ferreira and Pedro Vieira-Marques. 2018. Phishing Through Time: A Ten Year Story based on Abstracts. 225–232. https://doi.org/10.5220/0006552602250232

[39] Waldo Flores, Hannes Holm, Marcus Nohlberg, and Mathias Ekstedt. 2015. Investigating personal determinants of phishing and the effect of national culture. *Information and Computer Security* 23 (06 2015), 178–199. https://doi.org/10.1108/ICS-05-2014-0029

[40] Waldo Flores, Hannes Holm, Gustav Svensson, and G.N. Ericsson. 2014. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management Computer Security* 22 (10 2014), 393–406. https://doi.org/10.1108/IMCS-11-2013-0083

[41] Edwin Frauenstein. 2018. An Investigation Into Students Responses to Various Phishing Emails and Other Phishing-Related Behaviours.

[42] Yan Ge, Li Lu, Xinyue Cui, Zhe Chen, and Weina Qu. 2021. How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics* 97 (11 2021), 103526. https://doi.org/10.1016/j.apergo.2021.103526

[43] Madeline George, Alessandra Teunisse, and Trevor Case. 2020. Gotcha! Behavioural validation of the Gullibility Scale. *Personality and Individual Differences* 162 (04 2020). https://doi.org/10.1016/j.paid.2020.110034

[44] Sanjay Goel, Kevin Williams, and Ersin Dincelli. 2017. Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems* 18 (01 2017), 22–44. https://doi.org/10.17705/1jais.00447

[45] William Gordon, Adam Wright, Ranjit Aiyagari, Leslie Corbo, Robert Glynn, Jigar Kadakia, Jack Kufahl, Christina Mazzone, James Noga, Mark Parkulo, Brad Sanford, Paul Scheib, and Adam Landman. 2019. Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open* 2 (03 2019), e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

[46] Matthew Grilli, Katelyn McVeigh, Ziad Hakim, Aubrey Wank, Sarah Getz, Bonnie Levin, Natalie Ebner, and Robert Wilson. 2020. Is this phishing? Older age is associated with greater difficulty discriminating between safe and fraudulent emails. (06 2020). https://doi.org/10.31234/osf.io/upf6c

[47] Tzipora Halevi, James Lewis, and Nasir Memon. 2013. A pilot study of cyber security and privacy related behavior and personality traits. 737–744. https://doi.org/10.1145/2487788.2488034

[48] Ayako Akiyama Hasegawa, Naomi Yamashita, Mitsuaki Akiyama, and Tatsuya Mori. 2021. Why They Ignore English Emails: The Challenges of Non-Native Speakers in Identifying Phishing Emails. In *SOUPS @ USENIX Security Symposium*.

[49] Hågen Hasle, Yngve Kristiansen, Ketil Kintel, and Einar Snekkenes. 2005. Measuring Resistance to Social Engineering. In *Information Security Practice and Experience*. Springer Berlin Heidelberg, 132–143. https://doi.org/10.1007/978-3-540-31979-5_12

[50] Farkhondeh Hassandoust, Harminder Singh, and Jocelyn Williams. 2020. The Role of Contextualization in Users Vulnerability to Phishing Attempts. *Australasian Journal of Information Systems* 24 (09 2020). https://doi.org/10.3127/ajis.v24i0.2693

[51] Hannes Holm, Waldo Rocha Flores, Marcus Nohlberg, and Mathias Ekstedt. 2014. An Empirical Investigation of the Effect of Target-Related Information in Phishing Attacks. In *2014 IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*. 357–363. https://doi.org/10.1109/EDOCW.2014.59

[52] Kyung Wha Hong, Christopher Kelley, Rucha Tembe, Emerson Murphy-Hill, and Christopher Mayhorn. 2013. Keeping Up With The Joneses: Assessing Phishing Susceptibility in an Email Task. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 57 (09 2013), 1012–1016. https://doi.org/10.1177/1541931213571226

[53] Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer. 2007. Social phishing. *Commun. ACM* 50 (10 2007), 94–100. https://doi.org/10.1145/1290958.1290968

[54] Helen Jones, John Towse, Nicholas Race, and Timothy Harrison. 2019. Email fraud: The search for psychological predictors of susceptibility. *PLoS ONE* 14 (01 2019), e0209684. https://doi.org/10.1371/journal.pone.0209684

[55] Mingqing Kang, Matthew Shonman, Anshul Subramanya, Haoruo Zhang, Xiangyang Li, and Anton Dahbura. 2021. Understanding security behavior of real users: Analysis of a phishing study. (01 2021). http://hdl.handle.net/10125/71483

[56] W.D. Kearney and Hennie Kruger. 2014. Considering the influence of human trust in practical social engineering exercises. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference* (11 2014). https://doi.org/10.1109/ISSA.2014.6950509

[57] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Blair, and Theodore Pham. 2009. School of phish: A real-world evaluation of anti-phishing training. *SOUPS 2009 - Proceedings of the 5th Symposium On Usable Privacy and Security*. https://doi.org/10.1145/1572532.1572536

[58] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. 2008. Lessons from a real world evaluation of anti-phishing training. In *2008 eCrime Researchers Summit*. 1–12. https://doi.org/10.1109/ECRIME.2008.4696970

[59] Elmer Lastdrager, Inés Gallardo, Marianne Junger, and Pieter Hartel. 2017. How Effective is Anti-Phishing Training for Children?

[60] Patrick Lawson, Aaron Crowson, and Christopher Mayhorn. 2019. *Baiting the Hook: Exploring the Interaction of Personality and Persuasion Tactics in Email Phishing Attacks: Volume V: Human Simulation and Virtual Environments, Work With Computing Systems (WWCS), Process Control*. 401–406. https://doi.org/10.1007/978-3-319-96077-7_42

[61] Patrick Lawson, Olga Zielinska, Carl Pearson, and Christopher Mayhorn. 2017. Interaction of Personality and Persuasion Tactics in Email Phishing Attacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 61 (09 2017), 1331–1333. https://doi.org/10.1177/1541931213601815

[62] Tian Lin, Daniel Capecci, Donovan Ellis, Harold Rocha, Sandeep Dommaraju, Daniela Oliveira, and Natalie Ebner. 2019. Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Transactions on Computer-Human Interaction* 26 (07 2019), 1–28. https://doi.org/10.1145/3336141

[63] Mark W Lipsey and David B Wilson. 2001. *Practical meta-analysis*. SAGE publications, Inc.

[64] Roman Marusenko, Vladimir Sokolov, and Volodymyr Buriachok. 2021. *Experimental Evaluation of Phishing Attack on High School Students*. 668–680. https://doi.org/10.1007/978-3-030-55506-1_59

[65] Robert R. McCrae and Paul T. Costa. 1987. Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology* 52, 1 (1987), 81–90. https://doi.org/10.1037/0022-3514.52.1.81

[66] B. Medlin, Joseph Cazier, and Daniel Foulk. 2008. Analyzing the Vulnerability of U.S. Hospitals to Social Engineering Attacks: How Many of Your Employees Would Share Their Password? *IJISP* 2 (01 2008), 71–83.

[67] Jamshaid Mohebzada, Ahmed Zarka, Arsalan Bhojani, and Ali Darwish. 2012. Phishing in a university community: Two large scale phishing experiments. 249–254. https://doi.org/10.1109/INNOVATIONS.2012.6207742

[68] Gregory Moody, Dennis Galletta, Jon Walker, and Brian Dunn. 2011. Which Phish Get Caught? An Exploratory Study of Individual Susceptibility to Phishing. *International Conference on Information Systems 2011, ICIS 2011* 3.

[69] George Nasser, Ben Morrison, Piers Bayl-Smith, Ronnie Taib, Michael Gayed, and Mark Wiggins. 2020. *The Effects of Cue Utilization and Cognitive Load in the Detection of Phishing Emails*. 47–55. https://doi.org/10.1007/978-3-030-54455-3_4

[70] Jean-Robert Nino, Gustav Enström, and Alan R. Davidson. 2017. Factors in Fraudulent Emails that Deceive Elderly People. In *Human Aspects of IT for the Aged Population. Aging, Design and User Experience*. Springer International Publishing, 360–368. https://doi.org/10.1007/978-3-319-58530-7_28

[71] Warren T. Norman. 1963. Toward an adequate taxonomy of personality attributes: Replicated factor structure in peer nomination personality ratings. *The Journal of Abnormal and Social Psychology* 66, 6 (June 1963), 574–583. https://doi.org/10.1037/h0040291

[72] Alison M. O'Connor, Rebecca A. Judges, Kang Lee, and Angela D. Evans. 2021. Can adults discriminate between fraudulent and legitimate e-mails? Examining the role of age and prior fraud experience. *Journal of Elder Abuse &amp Neglect* (June 2021), 1–25. https://doi.org/10.1080/08946566.2021.1934767

[73] Daniela Oliveira, Natalie Ebner, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, and Tian Lin. 2017. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. 6412–6424. https://doi.org/10.1145/3025453.3025831

[74] Research Paper, Zhihui Liu, Lina Zhou, and Dongsong Zhang. 2021. Effects of Demographic Factors on Phishing Victimization in the Workplace.

[75] Kathryn Parsons, Marcus Butavicius, Paul Delfabbro, and Meredith Lillie. 2019. Predicting Susceptibility to Social Influence in Phishing Emails. *International Journal of Human-Computer Studies* 128 (02 2019). https://doi.org/10.1016/j.ijhcs.2019.02.007

[76] Kathryn Parsons, Marcus A. Butavicius, Malcolm Robert Pattinson, Dragana Calic, Agata McCormac, and Cate Jerram. 2016. Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails? *CoRR* abs/1605.04717 (2016). arXiv:1605.04717 http://arxiv.org/abs/1605.04717

[77] Kathryn Parsons, Agata McCormac, Malcolm Pattinson, Marcus Butavicius, and Cate Jerram. 2013. Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. *IFIP Advances in Information and Communication Technology* 405, 366–378. https://doi.org/10.1007/978-3-642-39218-4_27

[78] Pooja Patel, Dawn M. Sarno, Joanna E. Lewis, Mindy Shoss, Mark B. Neider, and Corey J. Bohil. 2019. Perceptual representation of spam and phishing emails. *Applied Cognitive Psychology* 33, 6 (Aug. 2019), 1296–1304. https://doi.org/10.1002/acp.3594

[79] M. Pattinson, C. Jerram, K. Parsons, A. Mccormac, and M. Butavicius. 2011. Managing Phishing Emails: A Scenario-Based Experiment.

[80] Justinas Rastenis, Simona Ramanauskaitė, Justinas Janulevicius, and Antanas Cenys. 2019. Credulity to Phishing Attacks: A Real-World Study of Personnel with Higher Education. https://doi.org/10.1109/eStream.2019.8732169

[81] Koceilah Rekouche. 2011. Early Phishing. *CoRR* abs/1106.4692 (2011). arXiv:1106.4692 http://arxiv.org/abs/1106.4692

[82] Fabio Rizzoni, Sabina Magalini, Alessandra Casaroli, Pasquale Mari, Matt Dixon, and Lynne Coventry. 2022. Phishing simulation exercise in a large hospital: A case study. *DIGITAL HEALTH* 8 (Jan. 2022), 205520762210817. https://doi.org/10.1177/20552076221081716

[83] BG Sanders, PS Dowland, and Steven Furnell. 2009. An assessment of people's vulnerabilities in relation to personal and sensitive data. *Advances in Communications, Computing, Networks and Security: Proceedings of the MSc/MRes programmes from the School of Computing, Communications and Electronics, 2007-2008* 6 (2009), 124.

[84] Dawn Sarno, Joanna Lewis, Corey Bohil, and Mark Neider. 2019. Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *Human Factors: The Journal of the Human Factors and Ergonomics Society* 62 (06 2019), 001872081985557. https://doi.org/10.1177/0018720819855570

[85] Steve Sheng, Mandy Lanyon, Ponnurangam Kumaraguru, Lorrie Cranor, and Julie Downs. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Conference on Human Factors in Computing Systems - Proceedings* 1, 373–382. https://doi.org/10.1145/1753326.1753383

[86] Tjaart Steyn, Hennie Kruger, and Lynette Drevin. 2007. Identity Theft — Empirical evidence from a Phishing Exercise. *IFIP International Federation for Information Processing* 232, 193–203. https://doi.org/10.1007/978-0-387-72367-9_17

[87] A. Sundararaj and G. Kul. 2021. Impact analysis of training data characteristics for phishing email classification. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 12, 2 (2021), 85–98. https://doi.org/10.22667/JOWUA.2021.06.30.085 Cited By :1.

[88] Ronnie Taib, Kun Yu, Shlomo Berkovsky, Mark Wiggins, and Piers Bayl-Smith. 2019. *Social Engineering and Organisational Dependencies in Phishing Attacks*. 564–584. https://doi.org/10.1007/978-3-030-29381-9_35

[89] Pethpranee Unchit, Sanchari Das, Andrew Kim, and L. Camp. 2020. Quantifying Susceptibility to Spear Phishing in a High School Environment Using Signal Detection Theory.

[90] Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Vishwanath, and H. Raghav Rao. 2012. Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication* 55, 4 (2012), 345–362. https://doi.org/10.1109/TPC.2012.2208392

[91] Bradley Weaver, Adam Braly, and David Lane. 2021. Training Users to Identify Phishing Emails. *Journal of Educational Computing Research* 59 (02 2021), 073563312199251. https://doi.org/10.1177/0735633121992516

[92] Allaire Welk, Kyung Wha Hong, Olga Zielinska, Rucha Tembe, Emerson Murphy-Hill, and Christopher Mayhorn. 2015. Will the "Phisher-Men" Reel You In? *International Journal of Cyber Behavior, Psychology and Learning* 5 (10 2015), 1–17. https://doi.org/10.4018/IJCBPL.2015100101

[93] Emma J. Williams, Joanne Hinds, and Adam N. Joinson. 2018. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies* 120 (Dec. 2018), 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

[94] Ryan Wright and Kent Marett. 2010. The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *J. of Management Information Systems* 27 (07 2010), 273–303. https://doi.org/10.2753/MIS0742-1222270111

A APPENDIX

ID	Author	Paper	Year
65	Hasle et al.	[49]	2005
190	Downs et al.	[34]	2005
221	Anandpara et al.	[6]	2007
256	Jagatic et al.	[53]	2007
264	Steyn et al.	[86]	2007
278	Downs et al.	[32]	2007
325	Bakhshi et al.	[66]	2008
335	Curtis et al.	[10]	2007
428	Kumaraguru et al.	[58]	2008
460	Sanders et al.	[83]	2009
509	Kumaraguru et al.	[57]	2009
620	Wright et al.	[94]	2010
621	Sheng et al.	[85]	2010
734	Pattinson et al.	[79]	2011
781	Blythe et al.	[13]	2011
908	Wang et al.	[90]	2012
955	Mohebzada et al.	[67]	2012
1007	Alseadoon et al.	[3]	2012
1022	Darwish et al.	[30]	2012
1053	Flores et al.	[40]	2013
1081	Parsons et al.	[77]	2013
1083	Halevi et al.	[47]	2013
1203	Hong et al.	[52]	2013
1308	Caputo et al.	[23]	2013
1352	Kruger et al.	[56]	2014
1360	Rocha-Flores et al.	[51]	2014
1397	Rocha-Flores et al.	[39]	2014
1433	Butavicius et al.	[20]	2015
1439	Parsons et al.	[76]	2015
1505	Welk et al.	[92]	2015
1796	Goel et al.	[44]	2016
1813	Nino et al.	[70]	2017
1834	Bullée et al.	[18]	2017
1838	Benenson et al.	[12]	2017
1849	Lawson et al.	[61]	2017
1917	Oliveira et al.	[73]	2017
1943	Carella et al.	[24]	2017
1997	Moody et al.	[68]	2017
2116	Bakhshi et al.	[9]	2017
2212	Curtis et al.	[28]	2018
2248	Williams et al.	[93]	2018
2256	Sannd et al.	[26]	2018
2275	Lawson et al.	[60]	2018
2289	Jones et al.	[54]	2018
2293	Alwanain et al.	[4]	2019
2308	Frauenstein et al.	[41]	2018
2333	Taib et al.	[88]	2019
2346	Alwanain et al.	[5]	2019
2349	Lastdrager et al.	[59]	2017
2375	Hassandoust et al.	[50]	2020
2382	Burns et al.	[19]	2019
2401	Gordon et al.	[45]	2019
2421	Rastenis et al.	[80]	2019
2501	Parsons et al.	[75]	2019
2521	Lin et al.	[62]	2019
2526	Abdullah et al.	[1]	2019
2535	Cuchta et al.	[27]	2019
2557	Patel et al.	[78]	2019
2580	Baillon et al.	[8]	2019
2678	Liu et al.	[74]	2020
2682	Bayl-Smith et al.	[11]	2020
2683	Nasser et al.	[69]	2020
2735	Unchit et al.	[89]	2020
2769	Ebner et al.	[36]	2020
2781	Chatchalermpun et al.	[25]	2020
2826	Sarno et al.	[84]	2020
2827	George et al.	[43]	2020
2841	De Bona et al.	[14]	2020
2913	Aljeaid et al.	[2]	2020
2930	Marusenko et al.	[64]	2020
2949	Canham et al.	[22]	2021
2967	Ayob et al.	[7]	2021
2987	Kang et al.	[55]	2021
2990	O'Connor et al.	[72]	2021
3018	Hasegawa et al.	[48]	2021
3045	Daengsi et al.	[29]	2021
3241	Weaver et al.	[91]	2021
3256	Grilli et al.	[46]	2020
3258	Ge et al.	[42]	2021
3345	Canham et al.	[21]	2022
3357	Rizzoni et al.	[82]	2022

Table 2. ID, Authors and Years of selected studies for meta-analysis

Model	Study name	Event rate	Lower limit	Upper limit	Z-Value	p-Value	Weight (Fixed) Relative weight	Weight (Random) Relative weight
	Rocha-Florest et al.	0,051	0,026	0,098	-8,078	0,000	0,17	6,26
	Flores et al.	0,087	0,044	0,164	-6,355	0,000	0,17	6,22
	Mohebzada et al.	0,087	0,082	0,093	-69,221	0,000	19,94	7,37
	Rocha-Floerst et al.	0,092	0,080	0,105	-30,317	0,000	4,01	7,33
	Marusenko et al.	0,119	0,108	0,130	-37,579	0,000	8,07	7,35
	Rastenis et al.	0,130	0,114	0,147	-25,958	0,000	4,27	7,33
	Sarno et al.	0,155	0,113	0,209	-9,079	0,000	0,66	7,05
	Bullee et al.	0,193	0,152	0,242	-9,692	0,000	1,05	7,17
	Kruger et al.	0,223	0,202	0,245	-19,450	0,000	5,55	7,34
	Alwanian et al.	0,303	0,281	0,327	-14,804	0,000	7,26	7,35
	Baillon et al.	0,329	0,312	0,347	-17,512	0,000	13,82	7,37
	Rizzoni et al.	0,360	0,342	0,379	-14,202	0,000	14,02	7,37
	Caputo et al.	0,364	0,296	0,438	-3,528	0,000	0,92	7,14
	Goel et al.	0,410	0,394	0,426	-10,789	0,000	20,07	7,37
Fixed		0,227	0,222	0,232	-80,927	0,000		
Random		0,183	0,125	0,262	-6,428	0,000		

Fig. 3. Regular Phishing (Proportion)

Model	Study name	Event rate	Lower limit	Upper limit	Z-Value	p-Value	Weight (Fixed) Relative weight	Weight (Random) Relative weight
	Kumaraguru et al. (2009)	0,075	0,061	0,091	-22,959	0,000	1,20	4,67
	Hasle et al.	0,127	0,078	0,200	-6,972	0,000	0,19	4,16
	Alwanain et al.	0,128	0,112	0,146	-24,827	0,000	2,41	4,72
	Abdullah et al.	0,154	0,089	0,252	-5,432	0,000	0,15	4,01
	Wright et al.	0,162	0,135	0,194	-14,801	0,000	1,17	4,67
	Oliveira et al.	0,199	0,159	0,247	-9,874	0,000	0,73	4,60
	Chatchalermpun et al.	0,220	0,215	0,226	-75,881	0,000	51,90	4,78
	Cuchta et al.	0,224	0,215	0,232	-50,649	0,000	23,82	4,77
	Bakhshi et al. (2008)	0,230	0,170	0,304	-6,264	0,000	0,39	4,46
	Rocha-Flores et al.	0,272	0,208	0,347	-5,503	0,000	0,45	4,50
	Caputo et al.	0,289	0,240	0,343	-7,057	0,000	0,88	4,63
	Bullee et al.	0,289	0,240	0,343	-7,057	0,000	0,88	4,63
	Flores et al.	0,315	0,229	0,417	-3,457	0,001	0,29	4,35
	De Bone et al.	0,340	0,277	0,410	-4,334	0,000	0,62	4,57
	Kumaraguru et al. (2008)	0,351	0,268	0,444	-3,084	0,002	0,36	4,44
	Aljeaid et al.	0,418	0,345	0,495	-2,092	0,036	0,58	4,56
	Bakhshi et al. (2017)	0,469	0,335	0,608	-0,428	0,668	0,18	4,12
	Carella et al.	0,510	0,441	0,579	0,283	0,777	0,72	4,60
	Steyn et al.	0,535	0,486	0,583	1,399	0,162	1,43	4,69
	Rizzoni et al.	0,545	0,526	0,563	4,592	0,000	9,48	4,76
	Burns et al.	0,700	0,642	0,753	6,261	0,000	0,79	4,61
	Jagatic et al.	0,717	0,675	0,755	9,227	0,000	1,42	4,69
Fixed		0,257	0,253	0,262	-88,410	0,000		
Random		0,308	0,246	0,377	-5,156	0,000		

Fig. 4. Spear Phishing (Proportion)

Study name	Std diff in means	Lower limit	Upper limit	Z-Value	p-Value
Liu et al.	-0,305	-0,727	0,117	-1,415	0,157
O'Connor et	0,083	-0,197	0,363	0,584	0,559
Blythe et al.	0,125	-0,138	0,388	0,935	0,350
Moody et al.	0,132	-0,030	0,295	1,594	0,111
Lastdrager	0,267	0,104	0,430	3,212	0,001
Lin et al.	0,320	-0,077	0,716	1,578	0,114
Kumaraguru	0,352	0,108	0,595	2,832	0,005
Sheng et al.	0,408	0,139	0,677	2,976	0,003
Unchit et al.	0,806	0,257	1,356	2,876	0,004
Sarno et al.	0,936	-0,370	2,242	1,405	0,160
	0,230	0,103	0,357	3,539	0,000

Fig. 5. Age SMD

Study name	Statistics for each study					Std diff in means and 95% CI
	Std diff in means	Lower limit	Upper limit	Z-Value	p-Value	-2,00 -1,00 0,00 1,00 2,00
Hong et al.	-0,604	-1,166	-0,042	-2,105	0,035	
Lastdrager	-0,066	-0,275	0,143	-0,620	0,535	
Moody et al.	0,000	-0,163	0,163	0,000	1,000	
Liu et al.	0,000	-0,393	0,393	0,000	1,000	
Kumaraguru	0,019	-0,280	0,318	0,126	0,900	
Lin et al.	0,086	-0,227	0,398	0,538	0,590	
Jagatic et	0,094	-0,083	0,271	1,038	0,299	
Benenson	0,111	-0,014	0,237	1,735	0,083	
O'Connor et	0,142	-0,177	0,460	0,873	0,382	
Goel et al.	0,170	-0,405	0,745	0,579	0,562	
Blythe et al.	0,342	0,083	0,600	2,592	0,010	
Sheng et al.	0,364	0,096	0,632	2,665	0,008	
	0,087	-0,005	0,179	1,854	0,064	

Fig. 6. Sex SMD

Model	Study name	Statistics for each study							Std diff in means and 95% CI
		Std diff in means	Standard error	Variance	Lower limit	Upper limit	Z-Value	p-Value	-2,00 -1,00 0,00 1,00 2,00
	Lawson et al.a	-0,704	0,217	0,047	-1,129	-0,278	-3,239	0,001	
	Parsons et al.a	-0,699	0,137	0,019	-0,969	-0,430	-5,086	0,000	
	Ayob et al.d	-0,397	0,150	0,023	-0,691	-0,103	-2,645	0,008	
	Lawson et al.c	-0,202	0,211	0,045	-0,616	0,212	-0,956	0,339	
	Parsons et al.b	-0,114	0,059	0,003	-0,229	0,001	-1,944	0,052	
	Lawson et al.d	-0,101	0,211	0,045	-0,514	0,313	-0,477	0,633	
	Parsons et al.d	-0,068	0,034	0,001	-0,135	-0,001	-2,001	0,045	
	Lawson et al.e	0,040	0,211	0,045	-0,373	0,454	0,191	0,849	
	Alseadoon et al.a	0,260	0,142	0,020	-0,019	0,538	1,827	0,068	
	Lawson et al.b	0,309	0,213	0,045	-0,108	0,726	1,453	0,146	
	Alseadoon et al.c	0,347	0,142	0,020	0,068	0,626	2,435	0,015	
	Ayob et al.b	0,420	0,150	0,023	0,125	0,715	2,794	0,005	
	Parsons et al.c	0,764	0,112	0,012	0,546	0,983	6,850	0,000	
	Parsons et al.e	1,158	0,158	0,025	0,848	1,468	7,322	0,000	
Random		0,080	0,110	0,012	-0,136	0,295	0,724	0,469	

Fig. 7. Personality SMD