Research Article • DOI: 10.2478/ijhrd-2024-0007 • IJHRD • 8(2) • 2024 • 100-113

The International Journal of HRD, Practice Policy and Research

How the big five psychological factors affect phishing: A literature review

Alex Gordon†, Darlene Russ-Eft

Purdue University

Abstract

Phishing is a social engineering attack which intends to steal information from an intended victim by masquerading as a reputable source. It is a ubiquitous problem in modern day society and organizations, which is not likely to slow down.
The Big Five psychological factors model is one which is widely used and has been shown to largely explain how someone behaves. Yet the results of the Big Five factors' interface with phishing response is not clear as of yet. The purpose of this study was to elucidate the interactions between phishing and the Big Five factors.
This study used an integrative literature review method to examine the relationship between the Big Five psychological factors and the phishing response. This theoretical model developed from the research can then be used to suggest human resource development (HRD) interventions within organizations. Such interventions can aid both the organizations and their employees to avoid the negative outcomes from phishing.

Keywords

phishing • email phishing • Big Five personality factors

Introduction

In the world's oceans it is estimated that a trillion or more fish are caught every year by fishermen (Rowland, 2017). This means the oceans are full of an incalculable number of fish. In our own way as humans, we are all currently living in a large and digital ocean of sorts known as the internet. Much like our own physical oceans, the waters are rising. There are currently over 5 billion internet users in the world today (Petrosyan, 2024). It is likely as time progresses more and more people will join us in this digital ocean. This can be viewed as an opportunity to help educate and bring the world closer together on the one hand. No longer does one have to go to their local library and open up an encyclopaedia to research a topic. Now a quick internet search will most likely yield all the knowledge someone needs on a topic, with some being potentially mis-information. The aforementioned 5 billion people can all talk with each other across the world instantaneously with this technology as well. Unfortunately, this newfound interconnectedness and knowledge also comes with a downside as well.

For instance, go online and do two separate google searches. One for "fishing" and one for "phishing." In one of these searches, you will quickly realize that humans are the apex predator and, in the other we are both the predator and the prey. Cybercrime is a current major problem and has been found to be one of the top 10 threats to global stability (Ge et al., 2021). Much like the rising levels of the ocean, it is something that affects us all. Phishing is among the top three cybercrimes in recent years (FBI, 2021). Phishing causes approximately $17,700 in damage every minute (Fruhlinger, 2020). It also has arguably shaped the course of history with its influence on the 2016 US Presidential election (Rashid, 2020). Hillary Clinton's campaign manager was phished which was responsible for the infamous pre-election email leaks. It has been said by some that history is like running water, that small shifts can alter its course for a long time. In this instance one phishing incident can do the same thing.

Phishing is what is known as a social engineering attack (Alsharnouby et al., 2015). It uses psychological tricks to fool a victim into thinking the attacker is someone that they are not. This is done to make the intended victim perform an action or divulge information they should not to the attacker. This can be particularly pernicious. As of 2023 phishers have increasingly been masquerading as company HR professionals (Zielinski, 2023). These attacks have been

†*Corresponding author: Alex Gordon*
E-mail: gordo186@purdue.edu

shown to be successful approximately one out of three times. This is alarming considering that these attacks accounted for approximately 42% of all phishing attacks in 2023 (Gideon, 2024). They can be after anything from financial information, personal information, passwords, etc. Depending on the information released and/or the context it can have varying different effects. For instance, the average cost of a cyber breach for businesses was $4,450,000 and has increased 15% over the last three years (IBM, 2024). The damage is not limited to just money either. It is much like a disturbance in calm water, it can send ripple effects that will be felt for some time to come. This is particularly pertinent to HR professionals as leaked information can be that which HR professionals are tasked with guarding. An organization's brand can be damaged and they can lose their competitive edge in many ways from a successful phishing attack. Figure 1 displays the different types of social engineering.

There are different ways in which someone can be persuaded by a phishing email. Cialdini (2021) outlined seven different persuasion principles which can be effectively utilized to persuade someone into performing an action. These principles have been applied to phishing with unsettling efficacy. For instance, in the year 2018 "only" 26,379 people were phished in the USA (Petrosyan, 2024). Fast forward to 2023 and that number increased to 298,878. Bear in mind that these are simply the attacks that are being reported and it is likely that there are many more which are not being reported.

Phishing attacks can also vary in their level of sophistication and efficacy. Generally speaking, phishing attacks can be broken down into two categories. One is mass phishing while the other one is known as spear phishing. Mass phishing attacks are easier to detect generally speaking. They rely on the sheer number of people they target to get some unfortunate prospective phish to take the bait. Spear phishing is a targeted attack on a specific group of people. These attacks can be highly sophisticated and very hard to detect. They rely on people missing minute details within the message and masquerading as someone the victim(s) know or should know. For instance a phisher without too much difficulty can pose as a HR professional to steal information. Often times phishers will observe and research their intended prey much like an angler might a trophy fish.

There is no technological fix that will eradicate this wave of phishing (Alsharnouby et al., 2015). This is mainly because phishing plays off psychology and humans are typically the weakest link in cyber defense. Indeed, technology may only worsen the tumultuous oceans of phishing and social engineering. For instance, AI deepfake technology was used in a social engineering attack resulting in $25,000,000 stolen by scammers (Chen & Magramo, 2024). It started with a phishing email that the target rightly suspected of being phishing. However, after the deepfake video call the victim was convinced and sent out the money via wire transfers. The sophistication and dangers of such attacks cannot be overstated in these sorts of attacks.

Research and theoretical work on personality began in the 1930s (Babcock & Wilson, 2020). Initially, "psychologists turned to natural language as the source of identifying attributes for a personality-naming structure" (p. 55). Initially,

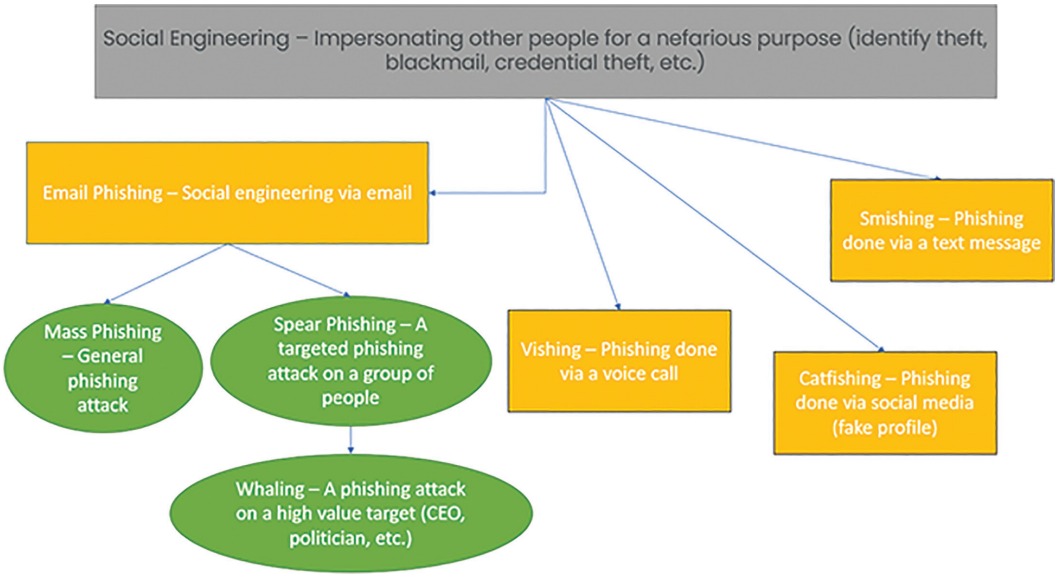

Figure 1. Social engineering Types: A Hierarchical View of Social Engineering.

there were many thousands of such attributes, but over time, some similar ideas emerged. Eventually, five factors were identified through exploratory factor analysis. The Big Five factor personality model has been shown to be capable of being able to explain how people generally behave (Goldberg, 1990). It is one of the most widely used personality models currently in use. The factors are orthogonal. That means that "getting a high or low score on one of these traits does not necessarily determine a specific score on any of the other traits" (Babcock & Wilson, 2020, p. 56).

The five factors can be remembered by using the acronym of OCEAN, in order to keep with the phishing theme. This acronym is comprised of Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism. Below is a brief explanation of each of these factors along with some key attributes which are pertinent for this study. Note that each of these factors should be viewed as a person's place on a spectrum anywhere from high to low.

Openness relates to how open someone is to new experiences (Goldberg, 1990). Someone who is higher in trait openness is typically more well read, and has better crystalized intelligence (Schretlen et al., 2010). They are also more adventurous, curious, and open to new ideas (Goldberg, 1990). Conversely a person who is lower in this trait will be less open to new ideas, less adventurous, and want to stick with known paradigms.

Conscientiousness relates to how hardworking, detail oriented, and obedient to rules one is (Goldberg, 1990). A person who is high in this trait will examine things assiduously, work inexorably towards their goals, and be adherent towards the established rules. If the polarity is flipped this can be indicative of low motivation, low adherence to rules, and low attention to detail. Interestingly enough, higher levels of this trait have been linked to better overall job performance for over 100 years (Wilmont & Ones, 2019).

Extraversion is the trait which measures how sociable someone is (Goldberg, 1990). Naturally, a person who is higher in this trait will be more sociable. People higher in this trait may seek to be the centre of attention. While unsurprisingly someone who is lower in this trait will be less sociable and may want less attention drawn to themselves.

Agreeableness relates to how well someone gets along with others (Goldberg, 1990). A person who is high in agreeableness will be less prone to engaging conflict and more apt to do as they are told to avoid said conflict. Naturally, lower levels of this trait are associated with being prone to engaging in confrontation.

Neuroticism is the trait which measures how emotionally stable someone is (Goldberg, 1990). Higher levels of this trait are generally correlated with lower levels of emotional stability and people being prone to anxiety and depression. At the lower end of the spectrum, it is generally correlated with greater emotional stability and lower levels of depression and anxiety. This trait also appears to be related to impulsivity as well.

Purpose and research questions

The purpose of this study is to elucidate the interactions between phishing and the Big Five factors. It aims to help answer the following questions:

RQ1: What do the existing studies show as the relationship between the Big Five factor traits and phishing response?

RQ2: In what ways, if any, do the existing studies show that there is a specific victim phishing personality profile? Ge et al. (2021) suggested that there is a victim personality. The present research will examine that possibility.

This study aims to answer the following questions by doing an integrative literature review. Beyond the review, it will offer a conceptualized model of the interactions between the individual Big Five factors and phishing response. It also intends to give practical takeaways and training recommendations to help combat the modern plague polluting our world's digital oceans.

Methodology

Integrative literature reviews are tools which can be used to synthesize the literature to date and help conceptualize a topic (Torracco, 2016). When doing an integrative literature review, it can be helpful to classify a topic as an emerging or mature topic. The topic of the relationship between Phishing and the Big Five personality model has been empirically studied for roughly the last 15 years. In the view of the current authors, this would place the topic more towards the emerging side of the spectrum. There are dozens of studies which study phishing in some form with its interaction with psychological factors (namely the Big Five). Currently the studies which examine this topic have generated mixed results. A meta-analysis by Sommestad and Karlzen (2019) showed that there was no clear consensus among the studies which they examined. However, two systematic literature reviews were able to help elucidate the relationships of neuroticism and extraversion with phishing response (Lopez-Aguilar & Solanas, 2021; Lopez-Aguilar et al., 2022). The present research builds upon this work with all five.

The steps for the integrative literature review process as described by Russell (2005) are (a) problem formulation, (b) data collection/literature search, (c) evaluation of data,

(d) data analysis, and (e) interpretation of results. This is the framework which was used by the authors of this paper. Problem formulation was done by selecting the Big Five model to study and examining the psychological factors of a phishing victim. The rationale behind this choice is that the Big Five is a relatively well-established science and the most prevalent throughout literature on the psychology of phishing. Data collection, data analysis, and interpretation of results will appear below.

Literature search

The scope of this search was limited to articles and studies which directly examined the relationship between phishing and the Big Five personality model. The authors wanted to cast a wide net in this search to collect the most valid data. More specifically the work had to study phishing done via email and not the other various forms of it. Meaning that voice phishing, text message phishing, social network phishing, etc. were not included in this study. Beyond the topic of email phishing, these studies were done in an academic setting so as to uphold scientific rigor. The date range used was from 2010 to the present. The search terms “phishing” AND “big five” were used in multiple different search engines and databases. These are: Google Scholar, Purdue’s Library, Sci Summary, Elicit, typeset.io, Web of Science, and IEEE. Also, only English texts were used for this search.

From these searches a total number of 203 articles were identified to be possible fits for the aforementioned criteria. After screening and reading the articles there were a total of 16 studies which made it through review for quality and applicability. In addition to the empirical studies there were dozens of articles which also made valuable contributions such as the literature reviews done on specific traits.

Data extraction & analysis

Each of the studies was read a minimum of two times. During each reading data were extracted from them along with key findings. Such findings included observations from the researchers of each study and theories which they offered to help explain their results. Details behind the study were also recorded such as the Big Five measurement tool, population size, and types of emails used. This was then all put together in a table for comparison purposes.

The relationship between a trait and phishing response was placed into one of three categories. If a study found a statistically significant relationship between the trait and phishing it was categorized as either negative or positive. Negative correlations mean higher levels of that trait are linked to increased vulnerability or susceptibility to phishing. Whereas positive denotes that higher levels of that trait are linked to greater caution and lower vulnerability to phishing. The third category is neutral meaning the study found no significant relationship either way.

The data were then categorized by their relationship with each of the individual factors. This way each of the individual factors could be analysed as stand-alone factors before being analysed in the greater context of the Big Five and phishing. Comparing the available empirical and theoretical evidence of these studies they were then tied into the existing data and theory on the Big Five factors.

Interpretation of results

The interpretation of the results was based upon the data that were extracted. Primarily they were interpreted, and the model was built upon the empirical evidence uncovered and the existing theoretical knowledge. In a few instances there are results showing where the empirical evidence was not found. However, in the few instances where this is the case this has been explicitly stated.

Results

The results from the analysis of these studies were broken down as follows. First the results from the studies, which measured the relationship between the Big Five and phishing in the wild, are examined. Phishing in the wild is a term being used in this paper denoting studies that used actual emails sent to individuals to measure response rates. In all of these studies the Big Five traits were measured by researchers, and then at a later date, emails were sent and the responses noted.

Following this, studies which have been dubbed farm phishing shall be examined. These are comprised of measuring the subjects’ Big Five traits and then measuring their phishing susceptibility in another way. This was mainly done through having these subjects rate pdf images of emails on the likelihood that they thought an email was a phishing attempt. This was done both in the presence and not in the presence of researchers. Following this the results on a specific victim personality profile will be examined.

Phishing in the wild

Phishing in the wild yielded some interesting results. Below is Table 1 which summarizes the relationships each study found between the factors and phishing. The table displays

the various studies, along with the results on each of the personality factors.

Interestingly every study besides one found only no or negative correlations between individual Big Five traits and phishing. Thus, being higher in any trait only led to increased phishing victimization or did not affect it at all. Traits of conscientiousness and openness appeared to be the ones the least correlated to phishing victimization according to these studies. Interestingly enough these are the only two traits to have been shown in one study to offer protection against phishing attacks. In contrast, extraversion, agreeableness, and neuroticism were found to be more indicative of increased phishing susceptibility.

Phishing on the farm

Phishing on the farm yielded results which in many cases were far different than in the wild. The results can be found in Table 2.

According to these studies the traits of openness and conscientiousness were strongly correlated with people being less susceptible to phishing. Agreeableness and extraversion have mixed results which are fairly close to being neutral overall. Only the trait of neuroticism stood out as clearly being correlated with increased phishing susceptibility.

Victim personality

Several studies (Canham et al., 2022; Eftimie et al., 2022; Ge et al., 2021) have suggested a possible victim personality. Only six out of the total 16 studies examined directly supported the notion of a victim personality. Canham et al. (2022) found that 6% of people were habitual phishing victims and non-responders to anti-phishing training. It was also found by the same study that nearly one third of people are responsible for flagging emails as phishing. Eftimie et al. (2022) showed that only the trait of agreeableness was significantly receptive to anti-phishing training. Ge et al. (2021) suggested that the

Table 1. Phishing in the Wild: Studies Showing the Relationship of Phishing with Personality Factors

Author(s)	Year	Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Alseadoon et al.	2012					
Alseadoon et al.	2015					
Ayob & Weir	2021					
Canham et al.	2020					
Eftimie et al.	2022					
Halevi et al.	2013					
Halevi et al.	2015					
Vishwanath	2015					
Higher Trait = Better Phishing Detection (+)		1	1	0	0	0
No Signifcant Relationship Noted (=)		5	5	3	3	4
Higher Trait = Worse Phishing Detection (-)		2	2	5	5	4
Overall Result		-1	-1	-5	-5	-4

Table 2. Phishing on the Farm: Studies Showing the Relationship of Phishing with Personality Factors

Author(s)	Year	Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Baki et al.	2022					
Cho et al.	2016					
Diman & Rahman	2023					
Ge et al.	2021					
Lawson et al.	2020					
Pattinson et al.	2011					
Rahman et al.	2022					
Sarno et al.	2023					
Higher Trait = Better Phishing Detection (+)		5	5	2	2	0
No Signifcant Relationship Noted (=)		2	3	3	4	4
Higher Trait = Worse Phishing Detection (-)		1	0	3	2	4
Overall Result		4	5	-1	0	-4

victim profile is of people who are low in the traits of openness, conscientiousness, and high in the trait of neuroticism. Halevi et al. (2013) noted in their study that it has been shown that approximately 10-20% of the population are vulnerable to scams in general. Although they did not further expand upon the personality make up of these people. In this way the existing literature does seem to suggest that there are set personality types which are responsible for guarding against or susceptible to phishing. The studies do not show a clear consensus of the Big Five personality make up of a victim.

Individual traits

Overall, the results of this literature review on individual traits found in Table 3 were mixed. Each trait had varying degrees of support for its relationship with phishing in different sources. First each trait's result shall be discussed briefly. A deeper dive into them will be made in the next section in the new theoretical model. Below is a chart with the overall results for each factor.

Openness

The factor of Openness was shown overall to be indicative of less phishing victimization. Six studies showed increased openness leads to better phishing response (meaning more avoidance of responding to a phishing email with increased openness), seven showed no relationship, and three showed a negative relationship (meaning less avoidance to responding to phishing emails with higher openness). This leaves openness with the final score of **+3 studies in favour of higher levels of the trait being correlated to lower phishing vulnerability.**

There are a few possible reasons for this. People who are higher in this trait are typically more well educated and literate (Schretlen et al., 2010). An indicator of a phishing attack can be grammatical mistakes in the email. Ergo, a more literate and educated person could pick these out more easily.

Conversely the trait of openness is not without its possible pathways to increased phishing victimization. People who are higher in this trait are naturally more curious and exploratory by nature (Goldberg, 1990). It is reasonable to assume that this curiosity may help drive them into getting ensnared by these phishing emails.

Conscientiousness

Conscientiousness appeared to be correlated with less phishing victimization. Conscientiousness was shown by six studies to equate to better responses to phishing emails (meaning more avoidance of responding to a phishing email with increased conscientiousness), eight showed no correlation and two showed a negative correlation (meaning less avoidance responding to phishing emails with higher conscientiousness). Leaving conscientiousness with the final score of **+4 studies, meaning that higher levels of conscientiousness equate to lower phishing vulnerability.**

When examining the trait there was a strong argument to be made for this correlation. Conscientious people are more detail

Table 3. Overall results

Author(s)	Year	Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Alseadoon et al.	2012					
Alseadoon et al.	2015					
Ayob & Weir	2021					
Baki et al.	2020					
Canham et al.	2022					
Cho et al.	2016					
Diman & Rahman	2023					
Eftimie et al.	2022					
Ge et al.	2021					
Halevi et al.	2013					
Halevi et al.	2015					
Lawson et al.	2020					
Pattinson et al.	2011					
Rahman et al.	2022					
Sarno et al.	2023					
Vishwanath	2015					
Higher Trait = Better Phishing Detection (+)		6	6	2	2	0
No Signifcant Relationship Noted (=)		7	8	6	7	8
Higher Trait = Worse Phishing Detection (-)		3	2	8	7	8
Overall Result		3	4	-6	-5	-8

oriented (Goldberg, 1990). Often with phishing the details are exactly what will tell you whether or not an email is legitimate or not. Conscientiousness is also correlated with people following established rules and taking training more seriously. It does not require much extrapolation to see how this can correlate to a better phishing response. In general, they are more hardworking and educated (Mammadov, 2022). Education can be viewed as the antidote to phishing in many ways.

However, one study was specifically able to target this trait with an email containing an appeal to order message within it. This means that while conscientiousness is a strong predictor of better cyber behaviour it is not without its drawbacks.

Extraversion

Extraversion appeared to be correlated with increased phishing victimization. Two studies showed higher levels of extraversion being equated to better phishing response (meaning more avoidance of responding to a phishing email with increased extraversion), six show no correlation, and eight showed a negative correlation (meaning less avoidance responding to phishing emails with higher extraversion). This leaves extraversion with the final score of **-6 studies, meaning that higher levels of extraversion are correlated to higher rates of vulnerability to phishing emails.**

The most obvious explanation for this is that this trait denotes how sociable someone is. Ergo, these people by their very nature are more prone to interact with others and make themselves more vulnerable to phishing. There are also different persuasion principles which can be used specifically against this trait.

Agreeableness

Agreeableness was another trait that appears to be correlated with increased phishing victimization. Two studies showed higher rates of agreeableness lead to better phishing detection (meaning more avoidance of responding to a phishing email with increased agreeableness), seven showed no correlation, and seven showed a negative correlation (meaning less avoidance to responding to phishing emails with higher agreeableness). This leaves agreeableness with the final score of **-5 studies, meaning that higher levels of agreeableness lead to higher rates of phishing vulnerability.**

A person who is higher in this trait is less likely to be confrontational and more submissive (Goldberg, 1990). Therefore, when a phishing email comes asking them to do something they are more likely to do it.

Neuroticism

Last but not least is the trait of neuroticism. Overall, it would appear that this is the trait most strongly correlated with increased phishing victimization. No studies showed increased levels of neuroticism helping with phishing response, eight showed no correlation, and eight showed higher levels of this trait leading to less avoidance to responding to phishing emails. This left neuroticism with the final score of **-8 studies, meaning that higher levels of neuroticism are correlated with higher rates of phishing vulnerability.**

This was the only one of the five traits having no studies showing possible benefits to increased levels of a trait. People who are higher in this trait are more impulsive and less emotionally stable (Goldberg, 1990). This trait inherently makes people more vulnerable to phishing attacks. If someone is impulsive then said person is less likely to think about their actions carefully. Also, it is reasonable to suggest that phishing emails that aim to generate fear will affect them more. These types of phishing emails are quite prevalent.

For RQ1 the hypothesis of the Big Five factors is supported for each of the traits. For RQ2 the hypothesis of a victim personality is also supported, albeit without a definitive answer on what the exact make up of this personality is.

Explaining the differences between studies

Overall, the studies were quite heterogeneous in their results. The ones of phishing in the wild versus at the farm appeared to be the most obvious. Having someone identify phishing emails at unspecified times and sometimes unknowingly is likely a better measure than having them rate a pdf. This is not to say that the latter is not without its merit. However, it is likely that when being watched by an observer a person is paying more attention to emails than they normally would. Indeed, the study by Eftimie et al. (2022) hypothesized that people would be more alert checking their emails in the morning than later in the day due to people being more alert in the morning. While such a detail is not noted in any other study it is likely that these details can influence the results.

These studies were all of varying sample sizes and populations. Table 4 highlights some of the key differences within the studies.

Some were carried out in the general population, others in academia, and others in industry. They were also in different parts of the world. An argument can be made that studying students within a certain programme at a university is not as generalizable as studying the general population. This also brings age into question. Eftimie et al. (2022) noted in their study that people tend to become more agreeable as they get older. There were several studies done on undergrad students at a university which were comprised mainly of people under

Table 4. Study Details

Author(s)	Year	Population	Study Size	Email Type(s)	Big Five Test
Alseadoon et al.	2012	Saudi Arabian Computer Science Students	100	Information Request	Not Specified
Alseadoon et al.	2015	Saudi Arabian Students	187	Blog Post Email	Not Specified
Ayob & Weir	2021	Malaysian Government Workers	122	Three Unspecified Emails	Not Specified
Baki et al.	2020	US Stem Students	1852	Greed	44 BFI
Canham et al.	2022	Unspecified Company	101	Several Types	IPIP-NEO
Cho et al.	2016	Unknown	Unknown	Unknown	Unknown
Diman & Rahman	2023	General Population Above 20	400	Unknown	BFI Inventory
Eftimie et al.	2022	Unspecified Software Company	235	Four Persuasion Principles	97 Question Big Five Test
Ge et al.	2021	Chinese General Population	414	Greed and Fear	44 BFI
Halevi et al.	2013	Stem Students	100	Greed	NEO-PI FFM
Halevi et al.	2015	Tech Company	40	Conscientiousness Based	20 Question IPIP
Lawson et al.	2020	Undergrad Students	102	Four Persuasion Principles	NEO-FFI-3
Pattinson et al.	2011	Business and Psychology Students	117	All Persuasion Principles	44BFI
Rahman et al.	2022	Unknown	173	Fear with possible others	IPIP-NEO
Sarno et al.	2023	Amazon Mechanical Turk Employees	150	Good Mixture	BFI Inventory
Vishwanath	2015	Undergrad Students	200	Fear	10 Item Big Five

the age of 30. Such results are likely not as generalizable to the general population as they could be. It should be noted that picking the population from a specific company or university also brings the training they have received into question. The anti-phishing training received at workplaces varies depending on the workplace.

There also was a fair amount of variance between the way that the Big Five were measured in each one of these studies. There were several different measurement tools used in the studies which were examined by this literature review. It is reasonable to suggest that this could have some effect on the data as well.

New model & recommendations

This section contains a new theoretical model of how each of the Big Five traits affects phishing response. It also includes proposed safeguards and solutions to help mitigate vulnerabilities towards this threat as well.

The first recommendation is that of tailored training for each one of the traits for the individual. It appears somewhat likely that people will be vulnerable to phishing attacks based on their Big Five make up. Different persuasion principles will target different traits in a person. For instance, an appeal to sympathy or humanity through a “charity” phishing email would at least in theory be the most efficacious in enticing people high in agreeableness to respond. In contrast, someone who is lower in this trait would be less affected by it. Ergo, the training should focus the training in areas where people are the most vulnerable. Phishing training is often given as a one size fits all training to organizations without accounting for the individual variability of people and the phishing emails themselves. While these can be helpful in detecting mass phishing attacks, it is likely that it is far from optimal in the more advanced spear phishing attacks.

It should be noted that someone’s Big Five traits profile could potentially offer better paths to motivation to take this training and to guard against phishing more seriously. The same pathways that can be used to manipulate someone into clicking on a phishing email may also offer the solution to motivating them to take the appropriate training. Indeed, it is likely that these motivation pathways could be used far

beyond the limited scope of anti-phishing training. By offering people motivation which is tailored to their specific personality it is plausible that employers could potentially get better engagement from their employees. With that in mind, the following text suggests some interventions related to each personality factor.

Openness

Higher levels of the trait of openness were shown to be overall indicative to help guard against phishing. As mentioned earlier these people are more well read and educated, which should help with phishing detection. However, these people tend to be more curious in general. This curiosity can be used against them to explore places where they should not. Rahman et al. (2022) made note of this saying that the trait of openness leads to greater fantasizing. Thus, if an attacker can plant the seeds of fantasy in an email, they can leverage this trait. In other words, dangling an intellectual carrot in front of such open people may effectively play on this trait. For instance, an email talking about a new technique for brain optimization or some esoteric information is likely to engage these people.

Conversely people who are lower in this trait may offer some unique challenges when guarding against phishing. If someone is low in openness they are not as likely to have the language skills or possibly the critical thinking to help identify phishing emails. In this case, training may need to be much more explicit, with multiple examples.

Conscientiousness

It is likely that most aspects of conscientiousness help guard against phishing. There are many positive aspects such as taking training more seriously, better education levels, stricter adherence to rules, and others which help with phishing. However, there are still several pathways which need to be guarded against, with those having this trait.

Halevi et al. (2015) used an appeal to order to specifically target this trait in their study. They sent out an email about an issue with a time sheet that needed to be rectified quickly. As conscientious people are orderly this proved to be efficacious. Vishwanath (2015) was also able to demonstrate how higher levels of this trait could be a liability. They hypothesized that conscientious people check email more frequently and might click links out of a sense of duty. Naturally, training these people that it is their duty to avoid clicking links without properly vetting them would help guard against such phishing response. The authors of this article would also like to posit the following weakness with this trait as well. Conscientious people would likely want to get things done quickly as they are quite industrious. Training these people to take their time to respond to emails would likely help yield better results.

Conversely people who are low in the trait of conscientiousness pose a problem for guarding against phishing. The indicators of an email being phishing are often in the details and takes assiduous examination. People who are low in this trait by their very nature are not known for either of these things. An effective appeal would have to motivate them with indications of personal harm that might arise from inadvertently responding to a phishing email.

Extraversion

From the overall results higher levels of extraversion appeared to be related to increased phishing victimization. However, it is the position of this article that it does not have to be. One of the best things that someone can do when they are unsure of a phishing attack is to confirm or disprove an email through different channels. Indeed, in the Alseadoon et al. (2015) study a student did this by asking another student. However, the other student was also wrong in their appraisal of the situation, so this ended up not being helpful. However, if they had used a proper channel, it would have been effective. Ergo, if they are trained in the proper channels to use, this trait could help ward off phishing attacks. A proper method of verification is to verify an email's legitimacy that a phisher could not have tampered with. For instance, going to an organization's website and using their actual contact number to either disprove or prove the validity of a request.

Conversely someone who is lower in this trait will need to be trained not to submit to a request just because they do not want to talk to someone. However, there are other methods of confirming or denying the validity of an email. It is likely that the focus of the training for this trait should be focused on the modality of confirming or disproving the validity of the request.

Agreeableness

Higher levels of agreeableness appeared to increase phishing vulnerability. Agreeable people are easier to manipulate as they do not want to be seen to be unco-operative (Eftimie et al., 2022). Training for people with this trait should be focused on educating them to properly vet the emails to which they choose to respond. After all cyber incidents can be quite disruptive so they need to play their part to help guard against them.

Lower levels of agreeableness also offer potential challenges for guarding against phishing. People with lower levels of agreeableness tend to be more unco-operative. Thus, training might simply suggest that they can help defend against phishing by simply ignoring the phishers' requests. However, if they find a phishers' email enticing, they will need extra emphasis on not clicking these emails. It is likely that framing this message to be in their best self-interest may offer the necessary pathway.

Neuroticism

Neuroticism appears to be the most problematic trait for phishing. Increased impulsivity and lower levels of emotional stability offer a problem in the ocean of phishing. Getting someone who is prone to impulsive emotional reactions to stop and rationally evaluate a situation is no easy task. Fear-based emails are likely to be most efficacious against this personality trait. Reframing the true danger of these messages is the most likely pathway to prevent harm. Identifying the likelihood that a message is phishing and the damage that it can cause is far more deleterious to them than the opposite is a possible solution. It is possible that such an approach could turn the anxiety over decisions into a possible strength.

While it was not shown, there is a possible drawback to lower levels of neuroticism. For those with both high and low levels of neuroticism, a message of warning of the possible consequences of clicking on a phishing email might be a good caution to send. Reminding the unfearful of the consequences in certain scenarios might be beneficial.

Victim personality

As stated before, there is significant evidence which suggests there is a victim personality. It is likely that this would be someone who is low in openness and conscientiousness while being high in extraversion, agreeableness, and neuroticism. Lower levels of openness mean worse language skills while lower levels of conscientiousness would mean less rule abiding behaviour or less attention to detail. High extraversion (if someone is not trained properly) means possibly not confirming messages correctly. People who are higher in agreeableness are much more likely to submit to requests. And high neuroticism would mean that these people are less emotionally stable and more likely to be swayed by these requests. It is also possible that impulsivity is a mixture of low conscientiousness and high neuroticism. An impulsive decision to click on a link in a phishing email is certainly a risk. Impulsivity has been found by multiple studies (Pattinson et al., 2011; Sarno et al., 2023) to be strongly correlated with worse response rates to phishing emails.

Limitations, future work, and conclusion

This integrative literature review should help provide a greater understanding of the Big Five factors interacting with phishing vulnerability. It has put forth a new theoretical model which should elucidate the murky waters of the ocean of phishing. There is a great deal of disparity between the results of the studies which have been examined. This is likely to be due to the different set ups of the studies. This is a burgeoning area of research which has been the subject of debate. The Big Five factor model is a well-established one which has yielded useful results in many other areas. It is the view of the authors that it is likely that phishing should be no exception. Phishing relies on psychology at its core to be efficacious.

Limitations

This study is not without its limitations. The first of which is the number of pertinent studies which were available for examination. More studies on this subject would help take away the variability found within the individual studies. More specifically, studies that examine phishing in the wild. Ideally these studies would have bigger sample sizes. Indeed, all of the studies besides one had populations between 100-400 participants. Furthermore, most of them were done at specific universities or companies. It is likely that studies which examine the general population would produce more generalizable results.

The presupposition that the Big Five traits manifest themselves in the same ways both online and offline is being used in this article. However, online behaviour and offline behaviour can be quite divergent from one another. For instance, some people who are not extraverted or social in person might have a polarity shift online. A specific Big Five model or test for online behaviour might give a more accurate picture of someone's phishing behaviour. Also, the measurement of the Big Five tools themselves may be in some sense suboptimal. Newer measurement methods such as the use of AI to measure the Big Five have shown promise (Soleimani & Kashani., 2024).

The theoretical model itself is based upon the current empirical evidence at hand and the theoretical knowledge of the Big Five and phishing. However, these hypotheses themselves have not been specifically tested for scientific validity.

Future work

There are several recommendations for future work that the authors of this article would like to offer. The first of which would be more empirical studies measuring the Big Five and phishing response in the wild. Although studies of phishing on the farm may contribute some new ideas, the most appropriate approach to examine phishing and the response is in a real-world situation.

Secondly, research exists around issues related to persuasion and to the processing of incoming information (Cialdini, 2021; Eftimie et al., 2022; Halevi et al., 2013, Lawson et al., 2018). More work on the Big Five factors' interaction with heuristic and systematic processing would be helpful. Systematic processing has been uniformly shown to help with phishing responses. However, there is no clear consensus on how, or if at all the Big Five interact with these two processing pathways. A hypothesis worthy of consideration is that the trait of openness would directly influence this choice. Being that the trait of openness is linked to more curiosity and psychological exploration it is likely that this would be correlated with systematic processing. Alas, the current data on this subject is very limited and is contradictory.

Further study and possible improvement in this theoretical model are likely to be needed. Confirming or disproving the pathways posited by this article by empirical studies would be prudent to help determine its accuracy. This is the first model of its type that the authors are aware of. It is likely to be the first step of many on the voyage to understand which phish get ensnared in nets.

Lastly, this article has proffered the hypothesis that understanding someone's Big Five traits make up is key to effective motivation. This within itself is an interesting area of possible future studies. Indeed, it would not necessarily even have to be in the area of phishing. However, this is a possible tool which can help HR professionals more efficaciously manage their respective work forces.

Conclusion

The relationship between the Big Five and phishing is still one that has not been fully elucidated. This study should hopefully help shine light on murky waters. However, science and research are often iterative and collaborative processes. Hopefully, this new theoretical model will help incrementally advance our understanding of the psychology behind phishing. The Big Five factor model has stood the test of time. Certain traits such as conscientiousness have been shown to be a predictor of workplace success in all areas for over 100 years (Wilmont & Ones, 2019). The Big Five has withstood multiple meta-analyses and a great deal of scientific scrutiny (Barrick & Mount, 1991; Mammadov, 2022). It is likely that it does meaningfully affect phishing response. The empirical studies on the Big Five's relationship with phishing are mixed. However, there is such a great variance between the studies that this should be expected. While it is confusing if one looks beneath the surface of these tumultuous waters, they should see the underlying currents responsible for it.

Phishing is a problem that is here to stay. Indeed, the technology behind it will likely change. However, at its core it is a psychological problem. Preventing phishing should not only be viewed as an IT function but one of collaboration between IT and HR personnel (Zielinski, 2023). Phishing represents an intersection between humans and technology. Humans have been shown to be the weakest link in cyber defence (Alsharnouby et al., 2015). There will be no technological elixir that will cure it. Indeed, the problem may only get worse with the burgeoning use of AI. No longer will phishers have to write their own emails. In theory this will take out some of the grammatical cues that can help identify phishing emails and worsen the problem. It is also likely that our world will continue its trend of digitizing even further. More and more we find ourselves working and indeed living online. Filling things out by hand is slowly but surely becoming the way of the past. In short, the phish are swimming in uncharted waters.

References

Alseadoon, I., Chan, T., Foo, E., & Nieto, J. G. (2012). Who is more susceptible to phishing emails?: A Saudi Arabian study. *ACIS 2012 : Proceedings of the 23rd Australasian Conference on Information Systems*.

Alseadoon, I., Othman, M.F.I., & Chan, T. (2015). What is the influence of users' characteristics on their ability to detect phishing emails? *Advanced Computer and Communication Engineering Technology, 315*, 949-962. https://doi.org/10.1007/978-3-319-07674-4_89

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*(1), 69-82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Ayob, Z., & Weir, G. R. S. (2021). Is human behavior the real challenge in combating phishing. *Advances in Intelligent Systems and Computing, 1291*(1), 27–38. https://doi.org/10.1007/978-981-33-4062-6_3

Babcock, S. E., & Wilson, C. A. (2020). Big Five model of personality. In B. J. Carducci, C. S. Nave, C. S. Nave (Eds.). *The Wiley encyclopedia of personality and individual differences: Models and theories.* (pp. 55-60). Wiley-Blackwell.

Baki, S., Verma, R. M., & Gnawali, O. (2020). Scam augmentation and customization: Identifying vulnerable users and arming

defenders. *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 236–247. https://doi.org/10.1145/3320269.3384753

Barrick, M. R., & Mount, M. K. (1991). The Big Five personality dimensions and job performance. A meta-analysis. *Personnel Psychology, 44*(1), 1–26. https://doi.org/10.1111/j.1744-6570.1991.tb00688.x

Canham, M., Posey, C., & Constantino, M. (2022). Phish derby: Shoring the human shield through gamified phishing attacks. *Frontiers in Education (Lausanne)*, *6*. https://doi.org/10.3389/feduc.2021.807277

Chen, H., & Magramo, K. (2024, February 4). *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'.* CNN. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Cho, J. H., Cam, H., & Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016*, 7–13. https://doi.org/10.1109/COGSIMA.2016.7497779

Cialdini, R. B. (2021). *Influence, new and expanded: The psychology of persuasion.* Harper Business.

Diman, A. P., & Rahman, T. K. A. (2023). Examining individual tendency to respond to phishing e-mails from the perspective of protection motivation theory. *Journal of Education and Social Sciences, Vol. 25(*1). 40-51.

Eftimie, S., Moinescu, R., & Racuciu, C. (2022). Spear-phishing susceptibility stemming from personality traits. *IEEE Access*, *10*, 73548–73561. https://doi.org/10.1109/ACCESS.2022.3190009

FBI. (2021, March 17). *IC3 releases 2020 Internet Crime Report.* Federal Bureau of Investigation. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

Fruhlinger, J. (2020, March 9). *Top cybersecurity facts, figures, and statistics*. CSO Online. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Fruhlinger, J. (2022, April 12). *What is phishing? Examples, types, and techniques.* CSO Online. https://www.csoonline.com/article/514515/what-is-phishing-examples-types-and-techniques.html

Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. (2021). How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics, 97*(1), 1103526-103526. https://doi.org/10.1016/j.apergo.2021.103526

Gideon, S. (2024, July 11). *Over 40% of top phishing scams at work come from HR related email subjects.* Human Resources Online. https://www.humanresourcesonline.net/over-40-of-top-phishing-scams-at-work-come-from-hr-related-email-subjects

Goldberg, L. R. (1990). An alternative "description of personality": The Big-Five factor structure. *Journal of Personality and Social Psychology, 59(*6), 1216–1229. https://doi.org/10.1037/0022-3514.59.6.1216

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and Facebook. *arXiv.Org*. https://doi.org/10.48550/arxiv.1301.7643

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *SSRN Electronic Journal.* http://dx.doi.org/10.2139/ssrn.2544742

IBM. (2024). *Cost of a data breach report 2023.* International Business Machines Corporation. https://www.ibm.com/reports/data-breach

Lawson, P. A., Crowson, A. D., & Mayhorn, C. B. (2018). Baiting the hook: Exploring the interaction of personality and persuasion tactics in email phishing attacks. *Advances in Intelligent Systems and Computing*, *822*, 401–406. https://doi.org/10.1007/978-3-319-96077-7_42

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, *86*, 103084–103084. https://doi.org/10.1016/j.apergo.2020.103084

Lopez-Aguilar, P., & Solanas, A. (2021). The role of phishing victims' neuroticism: Reasons behind the lack of consensus. *International Journal of Information Security and Cybercrime, 10*(2), 75–80. https://doi.org/10.19107/IJISC.2021.02.07

Lopez-Aguilar, P., Patsakis, C., & Solanas, A. (2022). The role of extraversion in phishing victimization: A systematic literature review. *2022 APWG Symposium on Electronic Crime Research (eCrime)*, 2022, 1–10. https://doi.org/10.1109/eCrime57793.2022.10142078

Mammadov, S. (2022). Big Five personality traits and academic performance: A meta-analysis. *Journal of Personality, 90*(2), 222–255. https://doi.org/10.1111/jopy.12663

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2011). Managing phishing emails: A scenario-based experiment. *Proceedings of the 5th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2011*, 75–85.

Petrosyan, A. (2024, April 15). *Number of phishing attack victims in the United States from 2018 to 2023.* Statista. https://www.statista.com/statistics/1390362/phishing-victim-number-us/

Petrosyan, A. (2024, November 5). *Worldwide digital population.* Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/

Rahman, A. U., Al-Obeidat, F., Tubaishat, A., Shah, B., Anwar, S., & Halim, Z. (2022). Discovering the correlation between phishing susceptibility causing data biases and Big Five personality traits using C-GAN. *IEEE Transactions on Computational Social Systems*, 1–9. https://doi.org/10.1109/TCSS.2022.3201153

Rashid, F. Y. (2020, November 24). *8 types of phishing attacks and how to identify them.* CSO. https://www.csoonline.com/article/3234716/8-types-of-phishing-attacks-and-how-to-identifythem.html

Rowland, M. P. (2017, July 24). *Two-thirds of the world's seafood is over-fished – Here's how you can help.* Forbes. https://www.

forbes.com/sites/michaelpellmanrowland/2017/07/24/seafood-sustainability-facts/

Russell, C. L. (2005). An overview of the integrative research review. *Progress in transplantation (Aliso Viejo, Calif.)*, *15*(1), 8–13. https://doi.org/10.1177/152692480501500102

Sarno, D. M., Harris, M. W., & Black, J. (2023). Which phish is captured in the net? Understanding phishing susceptibility and individual differences. *Applied Cognitive Psychology*, *37*(4), 789–803. https://doi.org/10.1002/acp.4075

Schretlen, D. J., van der Hulst, E.-J., Pearlson, G. D., & Gordon, B. (2010). A neuropsychological study of personality: Trait openness in relation to intelligence, fluency, and executive functioning. *Journal of Clinical and Experimental Neuropsychology, 32*(10), 1068–1073. https://doi.org/10.1080/13803391003689770

Soleimani, M., & Kashani, H. B. (2024). Frozen or fine-tuned? Analyzing deep learning models and training strategies for optimizing Big Five personality traits prediction from text. 2024 *10th International Conference on Artificial Intelligence and Robotics* (QICAR), 11–16. https://doi.org/10.1109/QICAR61538.2024.10496606

Sommestad, T., & Karlzen, H. (2019). A meta-analysis of field experiments on phishing susceptibility. *eCrime Researchers Summit*. https://doi.org/10.1109/eCrime47957.2019.9037502

Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review, 15*(4), 404–428. https://doi.org/10.1177/1534484316671606

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication*, *20*(5), 570–584. https://doi.org/10.1111/jcc4.12126

Wilmot, M. P., & Ones, D. S. (2019). A century of research on conscientiousness at work. *Proceedings of the National Academy of Sciences - PNAS, 116*(46), 23004–23010. https://doi.org/10.1073/pnas.190843011

Zielinski, D. (2023, November 30). Beware cybercriminals masquerading as HR professionals. SHRM. https://www.shrm.org/topics-tools/news/hr-magazine/beware-cybercriminals-masquerading-as-hr-professionals

About the Authors

Alexander Gordon

Alexander Gordon is a new researcher and a Doctoral Candidate at Purdue University. He currently works for the City University of New York (CUNY) Hostos where he both teaches cybersecurity and supervises students researching various topics within cybersecurity. He recently retired from the US Air Force and since retiring has been teaching cybersecurity in both academia and private industry. His research focuses on the psychology of cybersecurity and in Artificial Intelligence Large Language Models.

Professor Darlene Russ-Eft

Darlene Russ-Eft Ph.D. from the University of Michigan, is Professor Emeritus, Oregon State University and a Faculty of Practice in Technology Leadership and Innovation, Purdue University. At Purdue she serves as major advisor for doctoral students in the Doctor of Technology program. She was Academy of Human Resource Development president, editor of Human Resource Development Quarterly, past board member of the American Evaluation Association, and is currently associate editor of Frontiers in Psychology. She was inducted into the HRD Scholar Hall of Fame and elected as Fellow to the International Board of Standards for Training, Performance, and Instruction (ibstpiTM).