Phishing Attack Victims and the Effect on Work Engagement

Matthew James Werner and Kennedy Njenga(✉)

Department of Applied Information Systems, University of Johannesburg, Johannesburg, South Africa
knjenga@uj.ac.za

Abstract. Most of the research carried out in cybersecurity considers the technical aspects of the security of an organisation's systems. This work highlights the importance of considering the 'softer' social side of cybersecurity that looks at the lived experiences of phishing attack victims and the effect of such attacks on work engagement. In order to understand these effects, the study adopted the grounded theory (GT) approach to collecting and analysing data elicited from participants. The participants were theoretically sampled from the metropole area of Johannesburg and presented lived experiences of phishing attacks in their unique contexts. The data were transcribed and coded using GT techniques. From the codes, categories derived, and substantive theory that explains the effects of phishing attack victims on work engagement was generated. The implications of this theory to previous theories and scholars and practitioners are discussed.

Keywords: Cybersecurity · Phishing · Work engagement · Grounded theory

1 Introduction

1.1 Background on the Rise in Cyber Attacks

The 21st century saw a significant rise in mobile computing, with most mobile smartphones and tablets having advanced processing power compared to older mainframe systems. These advanced mobile computational devices brought unique sets of cybersecurity issues and concerns as these were connected to the Internet. In the discipline of Information Systems, the concern with how these mobile and other computational devices are to be protected is known as cybersecurity. Cybersecurity looks at the overall measures implemented within organisations and at an individual level to ensure electronic devices are secure from external threats such as hackers, viruses, malware, and, most notably, phishing attacks [1]. Cybersecurity also ensures that all of the security properties of the organisation are intact and up-to-date from these attacks [2].

Cybersecurity research in the social sciences is related more to human than technical aspects and is evolving [3]. Understanding Cybersecurity is essential to this study because cybersecurity issues are now considered multilateral, consisting of social, physical, and technical aspects. Cyber-attacks continue to evolve over the years, from traditional attacks which emphasised 'hacking' or gaining unauthorised access to data stored

P. Ndayizigamiye et al. (Eds.): IDIA 2022, CCIS 1774, pp. 203–217, 2023.
https://doi.org/10.1007/978-3-031-28472-4_13

on a computer system. Newer innovative attacks now involve phishing and smishing, which take the softer qualitative aspect of attacks [3]. Social approaches play a critical role in successful social engineering attacks.

1.2 Need for Research into Phishing Attacks

There is a justifiable need to look at the lived experience of a phishing attack victim and how the victim approaches work engagement after the attack. While many studies have focused on phishing attack ramifications [4, 5] and preventative measures [6, 7] few focus on the human dimension. This research considers the human dimension of work engagement and sees an employee's willingness and desire to passionately perform more than just the fundamental activities associated with their job role. Phishing attack victims will not necessarily display these qualities, and it is necessary to understand how these qualities are affected. It is important to note that phishing attack victims will, after an attack, not address tasks with pride and certainty and to the best of their ability after an attack.

This work, therefore, problematises this human dimension, emphasising the effects of phishing attacks on employee work engagement. These insights are essential because if organisations pay minimal attention to how phishing attacks affect their employees, they may not point to why productivity is declining. Importantly, this work not only points out the ramifications of the employee work engagement effects but importantly proposes measures that organisations may undertake to mitigate and manage the employee work engagement effects by coming up with a theory that explains this. The work, therefore, outlines the research objective in the following section.

1.3 Research Objective

In order to gain insights into the ramifications of employee work engagement from phishing attack victims, this research work explored the social, contextual and lived experiences elicited from cyber-attack victims. A qualitative grounded theory approach was undertaken for this purpose. To gain this understanding, the research addresses the following question.

1. What are the lived experiences of phishing attack victims, and to what extent is work engagement affected?

It is felt that South African organisations would benefit from research that addresses this question. South African organisations need to be aware of how phishing attacks affect work engagement so that they can device required support to victims. Importantly, understanding work engagement addresses the appropriate response measures to enhance cybersecurity.

To meet this stated research objective, the work is presented as follows: the introduction has laid context for understanding that the work engagement of victims of phishing attacks can be affected. The extent of this is unknown. A review of literature on cybersecurity then follows after the introduction section and points to the ongoing discourse on phishing as an innovative form of a cybersecurity attack. The methodology section

that follows after the literature review outlines the adaption of the grounded theory approach to this research work. The justification for using GT to elicit, analyse and develop a substantive theory is motivated. The data analysis section that follows the methodology points to how GT techniques of coding, interpreting and categorising data were employed. The discussion and implication of the results follow in the penultimate section, and the work is concluded.

2 Literature Review

2.1 Literature Search

In order to obtain a clear understanding of the literature on phishing attacks in cybersecurity, a systematic literature search was carried out. Using Boolean operators, AND, OR, NOT [8] and keywords on select databases such as Association of Computing Machinery Digital Library (ACM DL), Association for Information Systems (AIS eLibrary), Compendex Plus (Access via Engineering Village), Emerald, Engineering Village, Henery Steward Talks, IEEE Xplore, IG Global and Inspec, as depicted in Table 1, a literature search was carried out on relevant work in order to establish a preliminary understanding of how cyber-attacks influence behaviour.

Table 1. Example of word search in databases by thematic area

Thematic area	Keyword search	Database
Cybersecurity	"Cybersecurity"	ACM DL, AIS eLibrary Science direct, IEEE Xplore, Science direct, IEEExplore, Compendex Plus, IG Global and Inspec
Attacks	"Stealth Botnet", "Computer worms", "Spear phishing", "Malware", "Trojan"	
Behaviour	"susceptibility & phishing", "fear & phishing", "motivation", "work", "Employee engagement", "Employee commitment", "Employee involvement", "benefits", "Factors reducing employee involvement"	

Results from the keyword search produced numerous articles, which the researcher evaluated to determine the relevance and appropriateness of addressing the research objective. Once relevant articles were obtained, an understanding of phishing attacks in cybersecurity was gained, and this is explained in the next section.

2.2 Background on the Rise of Phishing Cyber Attacks

Cybersecurity describes the efforts made by individuals and organisations to protect their hardware and software from continually evolving threats, such as viruses, worms, phishing, and clickjacking, as well as understanding the nature of these diverse threats to

computerised systems [9]. Phishing attacks are cybersecurity threats where the attacker utilises electronic communication channels to convey socially engineered messages to entice the individual or individuals to perform actions beneficial for the attacker. The more sophisticated phishing is spear phishing, where attackers send specially crafted emails targeting a specific individual or organisation. The attacker will carefully construct an email asking individuals to disclose their personally identifiable information (PII), such as credit card details. These emails are created in such a way as to obfuscate the actual source [10] and are tailored to an individual or the organisation the attacker wants to exploit [11].

According to a report by Verizon, phishing was the top threat in breaches in 2020. Phishing was also ranked 2nd as the top threat in incidences. Furthermore, email links were the principal malware vector used in breaches [12]. Phishing attacks severely affect organisations as they often result in the loss of confidential data, specifically PII and passwords. The attackers can sell this data on the black market to the highest bidder. Furthermore, because of a phishing attack, an organisation's reputation could be damaged, and its brand value could be negatively affected. Lastly, an organisation could also experience a drop in its share price because investors and suppliers do not want to be associated with data leaking and negative publicity [4].

2.3 Phishing Attacks on Work Engagement

Work engagement considers organisational staff members involved in their job roles physically, emotionally, and cognitively [13]. Furthermore, work engagement indicators include employees' emotional, physical, and cognitive behaviour [14]. Work engagement and motivation are closely tied to greater job satisfaction, leading to greater organisational productivity [14]. A demotivated employee is less job satisfaction, and this can have a devastating impact on any organisation. These employees could be a liability to the organisation as they are unwilling to carry out routine tasks or, if they do, will execute them poorly [15].

Studies have shown that phishing attacks affect employees of organisations negatively and that employees' trust in the Internet could be destroyed [4]. Phishing victims will shy away from interacting with Internet-based applications such as banking, procurement systems, and electronic commerce (e-commerce) [4].

Furthermore, the consequences of experiencing a phishing attack extend far beyond financial losses [16]. For example, social ramifications include loss of trust, doubt, shamefulness, and hesitation to seize opportunities. In addition, participants/employees noted that they were less likely to respond to businesses or job opportunity ads after a phishing attack as the participants were unsure whether it was a legitimate or a job opportunity.

In order to understand these ramifications, localised to the South African context, research was undertaken. The methodology used for this research is described in the next section.

3 Methodology

3.1 Grounded Theory Approach to Understanding the Impact of Phishing

This research applied the Grounded theory (GT) approach considered the most suitable to understand phishing attacks and resultant behaviour in a work engagement. GT is a well-known methodology that has been used in numerous behaviour research studies in information systems security. One of the benefits of GT is that it is compatible with both qualitative and quantitative data generation techniques. GT is used to discover or construct a theory from data. The data is obtained systematically and is analysed using comparative analysis. Despite grounded theory being a complex methodology, it is intrinsically flexible [17].

The primary principle of GT is that a theory will be constructed from actual data. Unstructured questions are asked to elicit rich and unique lived experiences [18]. These questions tend to be more flexible as the researcher wishes to understand specific aspects of the phenomenon. It avoids situations where responses to questions are convoluted and complex to analyse [18]. The approach used is illustrated by Fig. 1.

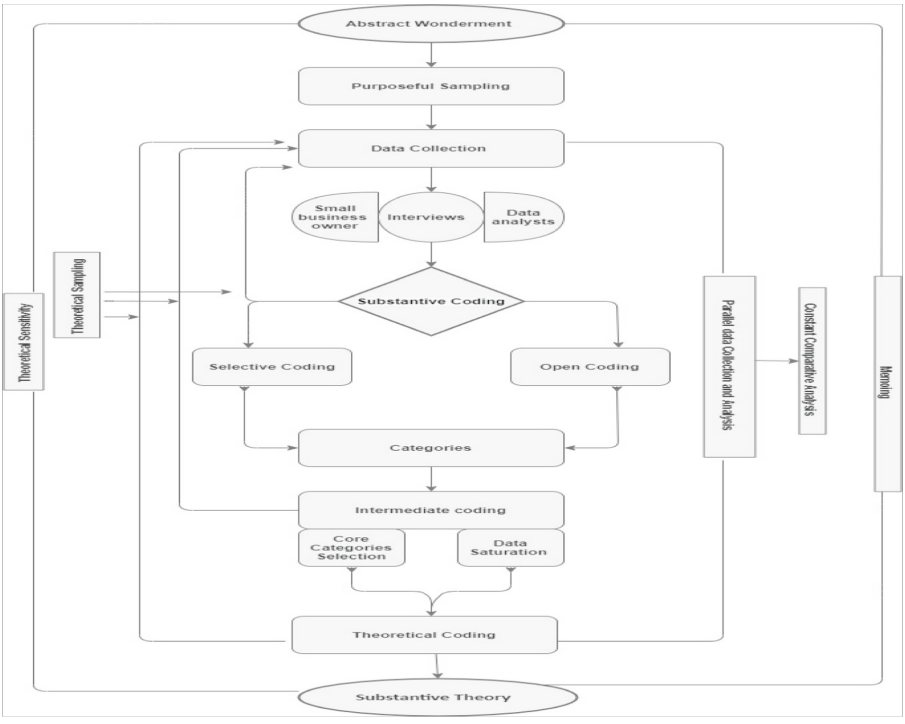

Fig. 1. The grounded theory approach. Source: Chun Tie, Y., Birks, M., & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. SAGE open medicine, 7 (Page 3).

A researcher will conduct preliminary unstructured interviews to obtain general information surrounding a phenomenon. This process of gathering general information is referred to as Abstract Wonderment. This wonderment is considered the first surprise that researchers face in conducting research despite the researcher identifying their limitations in knowledge surrounding the phenomenon under study [19]. What follows is the application of the purposeful sampling technique that asks questions such as whether the study participants have ever been victims of phishing attacks.

The purposeful sampling technique took the form of asking questions such as

- If the study participants have ever been a victim of a cyberattack? Yes/No
- If (yes) - Did the cyberattack occur at a place of work? Yes/No
- If (yes), Was the cyberattack a "phishing attack"? i.e., a type of cyberattack involving social engineering usually aims to gain confidential information, i.e., login credentials or passwords.

If the individual indicated that they had been a victim of a cyberattack, it occurred at their place of work, and it was a phishing attack, i.e., yes, then the researcher scheduled an interview with the individual to obtain the worker engagement effects to work that they experienced because of phishing attacks.

3.2 Interviews, Coding and Interpretation

Ten participants were pre-selected for an interview. Before any interviews or data were collected, ethical clearance was obtained. Interviews were scheduled at a mutually agreed time. Participants were told that should they feel uncomfortable answering questions. They were not obligated to continue. All interviews were transcribed. The raw data were coded on the transcripts and consisted of two levels, the first level being open coding, followed by selective coding [20]. The study adopted the Glaserian grounded theory method. The coding process was split into two stages; In vivo coding, where participants' exact words are used, and coding based on researcher interpretation (descriptive coding). Following this process, the lived experiences of victims of phishing attacks were documented. Progressively the codes started forming a higher level of abstraction and understanding. Following this, codes were numbered numerically, i.e., CD^1, CD^2….CD^n, representing either an in vivo code or a descriptive code. The coding process is for the first participant (P1), shown in Table 2.

The coding process continued until theoretical saturation had been reached. Constant comparison of codes was made to ensure that the codes reasonably described the experiences, which would lead to the development of a substantive theory. Coding bias was avoided by allowing for systematic data analysis and the emergence of new ideas and concepts based on the interpretation that was grounded on data. The description of the categories that emerged from the coding process is detailed in the following analysis.

Table 2. Example of the coding process employed in the study

Extracts of transcripts	Open coding	
	In vivo coding	Descriptive coding
"I had to follow up something for him, so he forwarded a link…I was also crazy busy and of course because he send it on I thought it was all legit. It looked a bit weird CD[4] It was from the post office and he said I must track the parcel because he doesn't have time, and of course you know I obviously helped him with stuff…"	*It looked a bit weird*	*Suspicion*

4 Data Analysis

4.1 Codes and Categories Generated

From the transcripts of the ten participants, sixty-one codes were generated, and from these codes, ten categories were developed, and finally, five core categories emerged. This is illustrated by Fig. 2. The process of generating categories from codes and core categories from categories is the essence of the GT approach.

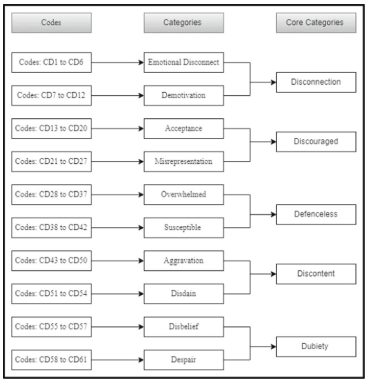

Fig. 2. Generating codes, categories and core-categories

The discussions that follow highlight how the above categories were derives from codes interpreted from participants' qualitative data. Many codes (underlined) were derived for each category, but for illustrative purposes, few selected codes are presented in the following narration.

4.2 Emotional Disconnect

It was noted and observed that victims of phishing attacks could not consequently manage and handle the stress that followed, hindering their emotional well-being. The category "Emotional Disconnect" was therefore derived from open codes from the following participants: Participant 1 (P1) mentioned that "*I don't know*[CD1] *what do you do" as a way of divorcing from commitment*. P2 explained that without support from management after the incident, commitment would remain low, thus advocating their intervention. "*Your emotional commitment*[CD2] *[will only] remain [high] by them being there for you and providing support*" P7 shared a similar sentiment and resounded this support by advocating raising answers through education, "*Basic education for non-technical people [is needed]*[CD3]". However, P4 shared a different opinion suggesting that emotional commitment need not be affected when one is confident in handling an attack suggesting, *"… give somebody that [has] the experience or … more confidence in handling these situations*[CD4]". P3 provided an additional measure proposing that employees be "*…allowed or provided with content*[CD5] *regarding the [nature] of attack…*" to raise awareness. As mentioned earlier, P4 motivated for "*… educating their staff on an emotional level*[CD6]" I think what the company…needs to do that. Six codes were derived from these interviews and were aggregated to form the category Emotional Disconnect.

4.3 Demotivation

The category 'demotivation' was derived from open codes as follows: P3 suggested that management support was crucial in encouraging a victim of a phishing attack to bounce back to normal after a phishing incident. P3 states, *"…a manager encouraging you to [continue working]*[CD7]". Moreover, P8 contended that motivating a phishing attack victim was necessary since "*threats continue evolving*[CD8]*, understanding different threats and also understanding their business…is required*". P8 added an interesting perspective alluding to a demotivated and pessimistic outlook after a phishing attack "*I don't think there is much more that the organisation can*[CD9] *do… Right?*" Additionally, P1 emphasised the importance of receiving support from management, given that a phishing attack victim could feel as they are going in the wrong direction or that is nothing is going right, "*Yeah, we did speak about it, but definitely it made a huge difference to get back on track and be as motivated as before…Because like I said, it felt like you know you're going 10 steps backwards*[CD10]" P7 shared a contentious view holding that while phishing attacks were inevitable, there were no outright solutions: "*I think it is a matter of understanding that firstly when we talk about phishing attacks….There is no way*[CD11] *that you can have 100% bulletproof solution to that*". This view could perhaps motivate employees indirectly in order not to allow this to hamper work engagement. While it may not be possible to have a 100% bulletproof solution for email phishing attacks, as alluded to by one of our participants, another participant, P1, believed that the basics work best, while not a solution to email phishing attacks, it could potentially provide a bit of reprieve from them, and stipulated that "*I think in hindsight we all just said…that we have to have a better/proper backup*[CD12] *On all the systems*". Six codes were derived from these interviews and were aggregated to form the category Demotivation.

4.4 Acceptance

The category 'acceptance' was derived from open codes as follows: P4 contended that it would be better to find continuity and accept that while the attack has happened, this should not hold back on work engagement. "*I'm talking about living with it once it's happened*[CD13]". P1 also contended that it would be better to move on. "*I don't think there's anything that [one] could have done to be honest*[CD14]" and that "*there's nothing that they could*[CD15] *actually do to help*". Similarly, P7 echoed similar views suggesting that "*I don't think there's anything that they can do*[CD16]". P3 was more insight and suggested a possible way forward after an attack by introspecting on existing weaknesses. "*Allow us to interact with our business structure*[CD17] *to understand the business structure*". In addition, P5 shared the same perspective mentioned earlier as they said, "*I wouldn't say my work performance was affected…Because I just took it as one of these…Hard lessons to learn from*[CD18]". P10 echoed similar sentiments as they stipulated that "*I expect this to happen [receipt of phishing emails is considered "normal"]*[CD19]" Lastly, P1 provided additional clarification and agreed with the other perspectives put forward as they said, "*Well, I think we try to motivate each other, and you know the nature of the beast we all like miff and upset and so you just have to get on*[CD20]*, you know…And if you don't want to, you can pack your stuff and leave*". Eight codes were derived from these interviews and were aggregated to form the category Acceptance.

4.5 Misrepresentation

The category 'misrepresentation' was derived from open codes as follows: P4 gave an example of what could happen when facts were misrepresented: "*[They sent] fictitious purchase orders*[CD21] *to everybody that was [currently] in the mailbox and anyone who had been sent an email in the past*" Additionally, P4 highlighted the reason for misrepresentation was for personal gain, cautioning against these kinds of attacks:"[It is one way of] "*sourcing new business…you [now] think twice when you get an email*[CD22] *from any-body*" P3 shared the concern that the email misrepresentation and phishing attacks was widespread. "everybody's [computer] is compromisedCD23 …" Additionally, P4 described a probable cause as to why email phishing attacks could be increasing, by stipulating that "*People are desperate for business*[CD24]*, so they just see a purchase order and they Click to open and it causes absolute chaos for us*" Lastly, P7 said misrepresentation could adversely affect planning and decision making, "*also affects your planning because there were certain things [tasks] that you planned… but now you have to change*[CD25]". A potential solution to this increasingly frequent phenomenon to curb email phishing attacks and their associated misrepresentation was stipulated by, P7 who said "*basic education for non-technical people*[CD26]" This potential solution was expanded upon by P8, who said "*I think Preventative, as in you know, pre getting it…There's lots of E learnings and courses and even attendance….Classroom based training that's forced upon you as mandatory training to take right…every organisation I've worked for, they very diligent….In terms of….Ensuring all employees go through sufficient training*[CD27]*…to be aware…Of these type of things and how…To deal with it, so you know regarding their processes and so forth so*". Seven codes were derived from these interviews and were aggregated to form the category Misrepresentation.

4.6 Overwhelmed

The category 'overwhelmed' was derived from open codes as follows: P4 suggested that as a victim of a phishing attack, this whole experience was overwhelming, impacting on work engagement (performance). "*So yeah, I'd say for a good week and a half [this event] impacted our performance*[CD28]". P1 pointed out similar concerns on the impact on performance. "*So, you're almost like nervous*[CD29] *in a way to…do any [work] because of…, you know these guys [Perpetrators] are obviously very clever*[CD30]". Furthermore, P4 shared similar sentiments by indicating that their actions were rather frantic as opposed to calm and collected "*Obviously you are desperately trying to put out fires*[CD31]" P3 shared a potentially devastating impact on work engagement "*But after the…. phishing attack… my action plan file, which I store on my desktop…that file was also compromised…and those files are also no [longer] …readable*[CD32]". P3 also noted that while work engagement was unaffected before the phishing attack, once the attack was initiated, the whole experience was overwhelming to the point of abandoning work. "*So, before everything is like very smooth and fast, I knew where I stored all my files, all the files and folders are very well organised on my system",* but after the attack, *"I felt like running away*[CD33]". P1 contended that "*you actually feel …demotivated completely*[CD34]". P5 pointed out that "*it took a bit longer to complete certain tasks*[CD35]" P6 shared a different view by saying, "*I don't think it's really affect it*[CD36]". Lastly, P4 shared the harsh reality by saying, "*Our output because of all the extra efforts we've got to put in to scrutinise emails and all the…Rest of it…Quite possibly 10% [performance loss] on a daily basis*[CD37]". Ten codes were derived from these interviews and were aggregated to form the category Overwhelmed.

4.7 Susceptible

The category 'susceptible' was derived from open codes as follows: P3 perceived himself as always being the cautious type, only to fall victim to a phishing attack leaving him feeling susceptible and vulnerable. "*Before…I only heard about this…. but I never realized*[CD38] *I could [be a victim] and once this happened [to] me, then my interest on cyber security increased as I felt vulnerable*[CD39]. *I don't want to sleep*". P1 provided more insight regarding how to overcome susceptibility and suggested the importance of being more alert and cautious in the future. "*…yeah, we did speak about it…it made a huge difference to get back on track*[CD40] *and be motivated as before*". Lastly, P3 shared a potential solution to reducing susceptibility to email phishing attacks by ensuring that from both an organisation and individual perspective. Once a victim has received training on how to identify and not engage with phishing emails, there needs to be some form of additional training or assessment that revaluates the individual's understanding regularly. As they said, "*Accepted the fact that this happened…And now he [the manager] wants you [the victim/participant] to learn from it [phishing email, which the participant interacted with]… and he says, you know, if this were to happen again [receiving another phishing email], what would we [the participant] do differently*[CD41]". P10 confirmed the need for training of non-technical individuals and overall awareness about phishing emails and suggested it could be a potential solution for reducing susceptibility, by saying that "*Arrange training and make sure that this stuff [phishing attacks] is aware*

of[CD42]". Five codes were derived from these interviews and were aggregated to form the category Susceptible.

4.8 Aggravation

The category 'Aggravation' was derived from open codes as follows: P7 was left feeling frustrated or annoyed after they had been a victim of an email phishing attack. As they indicated that their planning had to be reworked to address vulnerabilities that had been uncovered by stipulating that "*but in so doing it also affects your planning because there were certain things [tasks] that you planned on doing, but now you have to change back and start saying, OK, let's park this [postpone this task] for now*[CD43]." *Let's expedite this [implement this task as soon as possible]*[CD44]". P1 shared similar sentiments as they indicated that they had to complete mundane tasks, such as restoring data, due to an email phishing attack, as they stipulated "*so everybody had to reload [data/information] everything*[CD45]". Next, P2 provided another mundane task by saying that "*Phoned AMD… But then still she felt that it would be best if we update my password and everything*[CD46]". As if having to deal with mundane tasks was not undesirable enough, P4 further added that they had to resolve the direct damage of the email phishing attack and the indirect damage by stating that "*Obviously you are desperately trying to put out fires*[CD47] *[various issues that are arising due to the email phishing attack]*". P4 also provided a harsh reminder of how devasting phishing attacks can be, adding that, "*So I don't know How much actual business…I'm deleting because I don't want to risk opening up that email…you cautious and that, but at the same time you kind of thinking okay but I could potentially be losing a new customer*[CD48]". Although P9 did not necessarily have to complete mundane tasks, they still expressed their overall frustration with the situation, by stating that "*and I think it's like makes me feel irritated and frustrated*[CD49]". Conversely, one positive outcome that could be salvaged from an individual experiencing a phishing attack, as indicated by P8, as they said "*you kind of use that historical….Experience to now start to be a little bit more proactive*[CD50]*, so even though things have happened*". Seven codes were derived from these interviews and were aggregated to form the category Aggravation.

4.9 Disdain

The category 'disdain' was derived from open codes as follows: P1 was left feeling disdain after experiencing an email phishing attack. As they stipulated that they were unable to use their digital infrastructure or company computer network, as the email phishing attack had caused the system to become unusable, unless a ransom was paid, by stipulating that "*They can't use the actual system*[CD51]*, which makes it easier because you have to wait until all the work is captured again*". P1 went on to provide additional information, indicating that if the company had implement the necessary protections and trained their staff about phishing attacks, the consequences of the outcome could have been minimised, which would not have resulted in their employees expressing these emotions, as they stipulated that "*Yeah MJ, I don't think there's anything that they could have done to be honest, it was just a matter of because like I said if the proper stuff was in place before this happened*[CD52]*, I think less damage would have taken… Place and if we*

were trained properly[CD53]*…To lookout for these things…But when it actually happened and after …I mean there's nothing that they could actually do to help*". Furthermore, P3 shared similar sentiments as they also had the unpleasant experience of experiencing resentment towards their organisation as they had to reset all their credentials, by stating that "*Every password is compromised*[CD54] *and that time just because of my computer already have like firewalls and all that so they don't access my personal account*". Four codes were derived from these interviews and were aggregated to form the category Disdain.

4.10 Disbelief

The category 'disbelief' was derived from open codes as follows: P1 was left in disbelief after experiencing an email phishing attack, as they could not believe the extent of the damage caused, by stating that "*It was terrible. It was the worst feeling ever*[CD55]*…the damage was done…it started already from the morning*". P3 echoed similar sentiments as they could not access any content on their Personal Company Computer (PCC), as they stipulated that "*I will tell you like this is a very horrible experience*[CD56]". P6 also expressed their concern after an email phishing attack, stating, "*I was confused, stressed*[CD57]". Three codes were derived from these interviews and were aggregated to form the category Disbelief.

4.11 Despair

The category 'Despair' was derived from open codes as follows: P1 was left in despair after they had experienced an email phishing attack. As they were unaware and did not have the knowledge, skills or training to deal with a phishing attack, they stated that "*I sent him [an expert in Information Technology] a screenshot from my phone*[CD58] *[to show what was happening with the computer system]*". Similarly, P3 shared similar sentiments as they stated that "*Immediately inform [victim informs] our [their company's] incident response team*[CD59]". P4 echoed a familiar perspective, as they stated, "*the only thing [no other viable option] that I could do was close down [revoke the license] that email address*[CD60]". However, P8 indicated they were not left in despair as they managed to recognise and halt the file being downloaded before any severe damage could be done, as they "*cancelled it [file being downloaded] quick enough*[CD61]". Four codes were derived from these interviews and were aggregated to form the category Despair.

5 Discussion

5.1 Deriving Core-categories from Categories to Formulating a Substantive Theory

From the 6 categories generated from open coding, the next phase according to GT approaches was to compare the codes with codes and codes with these categories. This process in known as constant comparative analysis which involved sorting and organising data into groups in a structured way to formulate a new grounded theory. Glaser, Strauss, & Strutzel [21], suggest that it is important to revise core-categories called "normative expectation" as data moves to a higher level of abstraction.

5.2 Emergence of Substantive Theory

The normative expectation as data analysis moved to higher levels of abstraction was for a theory to emerge. The theory that emerged then is shown by Fig. 3.

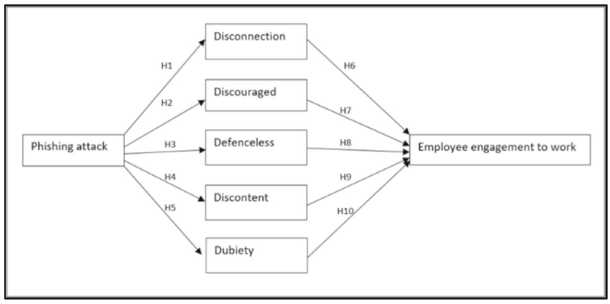

Fig. 3. Emergence of Substantive Theory (of Phishing effects on work engagement)

Figure 3 presents the following propositions:

- A phishing attack incident is likely to create a disconnection to work.
- A phishing attack incident is likely to leave the employee felling discouraged.
- A phishing attack incident is likely to leave the employee feeling defenseless.
- A phishing attack incident is likely to leave the employee feeling discontent.
- A phishing attack incident is likely to leave the employee having dubiety (doubtfulness).
- Feeling disconnected to work will negatively influence work engagement.
- Feeling discouraged will negatively influence work engagement.
- Feeling defenseless will negatively influence work engagement.
- Feeling discontent will negatively influence work engagement.
- Having dubiety (doubtfulness) will negatively influence work engagement.

Since the aim of a GT approach is to develop a theory, the outcome of this research as shown by Fig. 3, has elucidated the use of GT in context of employees working around Johannesburg area and fulfills this criteria. The substantive model shows five important core categories namely, *disconnection*, *discouraged, defenseless, Discontent, and Dubiety* as outcomes of a phishing attack. These five emotive feelings will likely determine work engagement. Organisations are therefore encouraged to adapt measures that can help employees manage these emotions. What is important is that the employees should receive the support that they require. Organisations can also adapt additional measures such as educating employees on risks imminent in the cyber space, remaining current with existing attacks, and developing policies and procedures to handle phishing attacks. These measures could alleviate the feelings of *disconnection*, *discouraged, defenseless, discontent, and dubiety.*

5.3 Implications on Information Systems Theory

The theoretical strength of this research lies in showing through original work, how GT can be used to formulate a theory that can predict work engagement from phishing attacks. The research work has developed some theoretical propositions from the substantive theory which can be generalised outside the Johannesburg business contexts to the broader national and international contexts. The research work was done is such a way as to minimise research bias for this purpose. It is from the deep interaction with the study participants, that the theoretical basis to predict work engagement was determined. The research work, therefore offers new insights and perspectives that can shape and improve the existing body of knowledge in cybersecurity and specifically phishing attacks.

5.4 Implications for Organisations and Practice

Reflecting of the substantive theory developed in this research, potential use of the substantive theory is identified as follows: Professionals 'workspace is increasingly becoming Internet driven and computing technology centric. This increases the likelihood of these professionals experiencing email phishing attacks. The overarching benefit of this work is that professionals as well as organisations could be able to aid their employees in returning to their optimal level of performance if the issues around *disconnection*, *discouraged, defenseless, discontent, and dubiety* are addressed. Practitioners can therefore use this theory as a guide to phishing attacks management.

6 Conclusion

This paper has demonstrated that beyond the technical aspects of cybersecurity that a lot of research has been undertaken, the social contextual aspects has often been overlooked. This paper shows the importance of this social contextual aspect namely, the emotions phishing attacks elicits on employees and the effects these emotions have on work engagement. From work carried out using the grounded theory approach, five emotions namely, *disconnection*, *discouraged, defenseless, discontent, and dubiety* were developed that formed the basis of the substantive theory for this work. The development of this substantive theory was underpinned by a rigorous process of coding and categorising of data supports these findings. It is envisaged that researchers and practitioners will find value and benefit from this research.

References

1. Craigen, D., Diakun-Thibault, N., Purse, R.: Defining cybersecurity. Technol. Innov. Manag. Rev. **4**(10) (2014)
2. Von Solms, R., Van Niekerk, J.: From information security to cybersecurity. Comput. Secur. **38**, 97–102 (2013)
3. Benson, V., McAlaney, J., Frumkin, L.A.: Emerging threats for the human element and countermeasures in current cybersecurity landscape. In: Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications, pp. 1264–1269. IGI Global (2019)

4. Jain, A.K., Gupta, B.B.: A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterp. Inf. Syst. **16**(4), 527–565 (2022)
5. Mihai, I.C.: Overview on phishing attacks. Int. J. Inf. Sec. Cybercrime **1**, 61 (2012)
6. Singh, A.P., Kumar, V., Sengar, S.S., Wairiya, M.: Detection and prevention of phishing attack using dynamic watermarking. In: Das, V.V., Thomas, G., Lumban Gaol, F. (eds.) AIM 2011. CCIS, vol. 147, pp. 132–137. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20573-6_21
7. Chaudhry, J.A., Chaudhry, S.A., Rittenhouse, R.G.: Phishing attacks and defenses. Int. J. Secur. Appl. **10**(1), 247–256 (2016)
8. Yushtina, A.: Ontology-based data extraction in the scholarship-related content. MS thesis (2013)
9. Gupta, C.P., Goyal, K.K.: Cybersecurity: a self-teaching introduction. Mercury Learning and Information (2020)
10. Cui, Q., et al.: Tracking phishing attacks over time. In: Proceedings of the 26th International Conference on World Wide Web (2017)
11. Shakela, V., Jazri, H.: Assessment of spear phishing user experience and awareness: an evaluation framework model of spear phishing exposure level (spel) in the namibian financial industry. In: 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD). IEEE (2019)
12. Bhardwaj, A., et al.: Why is phishing still successful? Comput. Fraud Secur. **2020**(9), 15–19 (2020)
13. Abu-Shamaa, R., Al-Rabayah, W.A., Khasawneh, R.T.: The effect of job satisfaction and work engagement on organisational commitment. IUP J. Organ. Behav. **14**(4) (2015)
14. Kuok, A.C.H., Taormina, R.J.: Work engagement: evolution of the concept and a new inventory. Psychol. Thought **10**(2) (2017)
15. Winkler, K., Saur, C.: Employee retention management: long-term retention of employees–a comparison of generations. J. Appl. Leadersh. Manag. **7**, 96–111 (2019)
16. Kelley, C.M., et al.: Something smells phishy: exploring definitions, consequences, and reactions to phishing. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 56, no. 1. SAGE Publications, Los Angeles (2012)
17. Strauss, A., Corbin, J.M.: Grounded Theory in Practice. Sage (1997)
18. Engward, H., Davis, G.: Being reflexive in qualitative grounded theory: discussion and application of a model of reflexivity. J. Adv. Nurs. **71**(7), 1530–1538 (2015)
19. Stoupe, D.: Understanding abstract wonderment: the reflections of a novice researcher. Grounded Theory Rev. **15**(2) (2016)
20. Glaser, B.G., Strauss, A.L.: The Discovery of Grounded Theory: Strategies for Qualitative Research. Routledge (2017)
21. Glaser, B.G., Strauss, A.L., Strutzel, E.: The discovery of grounded theory; strategies for qualitative research. Nurs. Res. **17**(4), 364 (1968)