



## Dishonesty, neutralisation and nudging

Takudzwa Mutyavaviri<sup>a</sup>, Karl van der Schyff<sup>b</sup>, Karen Renaud<sup>c,d,a,b,\*</sup>

<sup>a</sup> Rhodes University, South Africa

<sup>b</sup> Abertay University, UK

<sup>c</sup> University of Strathclyde, UK

<sup>d</sup> University of South Africa, South Africa

### ARTICLE INFO

#### Keywords:

Behavioural nudges  
Online dishonesty

### ABSTRACT

E-banking offers clients unparalleled convenience but also exposes them to potential fraud from cyber criminals. Traditionally, banks use technical security measures to ameliorate these kinds of threats. These measures, while essential, are not universally efficacious in preventing fraud. It would be wise to augment technical measures with softer measures such as behavioural interventions (i.e., nudges). In this paper, we report on the effectiveness of behavioural nudges designed to dissuade opportunistic “others” from committing e-banking fraud. Here, we report on an investigation into the impact of the deployment of a number of behavioural nudges in an e-banking customer interface. We evaluated their impact through semi-structured interviews with e-banking customers in the United States of America. We found that nudges which emphasise empathy and heightened awareness of traditional security measures were remarkably effective in dissuading dishonesty. Notably, deployment immediately after login yielded optimal results. Our findings highlight the potential of behavioural nudges to reduce e-banking fraud, thereby augmenting traditional technical countermeasures. We conclude with recommendations for future research.

### 1. Introduction

Online banking, referred to as e-banking in this study, has become a popular part of contemporary banking for many years (Sarreal, 2019; Pilcher, 2023). Despite initially being driven by banks to save on operational costs, e-banking’s continued popularity can be attributed to the unrivalled ease it provides customers, allowing them to access and manage their accounts remotely (Lee, 2009; Aravind et al., 2024; Hartl and Schmutzsch, 2016). In essence, e-banking eliminates the time and space restrictions imposed by traditional (i.e., physical) banking. Enhanced convenience has been marred by malicious third parties who actively exploit e-banking vulnerabilities (Nilsson et al., 2005; French, 2012; Belás et al., 2016). A recent example is a small US business who suffered a loss of \$63,000 when a hacker exploited an e-banking vulnerability linked to the online payroll system (Groff Networks 2023). Account takeovers, in particular, have led to millions of dollars loss in e-banking fraud (KrebsSecurity 2022) some of which e-banking customers have not been able to recoup (Zelle Report 2022). E-banking fraud (amongst others) is a persistent problem, having increased significantly since 2015 (KPMG 2019) with 33% of all banking expenses in the US being attributable to e-banking fraud (Alm et al., 2023; Deng,

2022). Considering that, circa 2022, over 65% of US citizens regularly use e-banking systems, it is worth investigating mitigation measures (Statista 2023). This is especially the case when one considers that the number of US customers using e-banking is projected to grow to over 279 million by 2024 (Statista 2023). Given the above, we argue that banks should consider combining traditional security measures with behavioural interventions when it comes to e-banking security. Strategically placed behavioural nudges might well be a low-cost and effective measure to deploy. Such nudges could (and typically should) be oriented towards encouraging a choice to be honest (Thaler and Sunstein, 2008). These nudges might include tweaking the website’s layout, interaction mechanisms, tailored information display, and the transactional choices customers are presented with when banking online (Thaler and Sunstein, 2008; Franco, 2018). Despite the fact that nudging has been used successfully in a number of other domains (Kroese et al., 2015; Broers et al., 2017; Kuhfuss et al., 2016; Castleman and Page, 2015), its use within an e-banking context has not yet been investigated. In particular, we sought to address the following research questions:

**RQ1.** Which behavioural nudges are most effective at dissuading e-banking fraud and where should they be placed?

\* Corresponding author.

E-mail address: [karen.renaud@strath.ac.uk](mailto:karen.renaud@strath.ac.uk) (K. Renaud).

<https://doi.org/10.1016/j.ejdp.2024.100052>

Received 8 December 2023; Received in revised form 18 June 2024; Accepted 24 June 2024

Available online 1 July 2024

2193-9438/© 2024 The Author(s). Published by Elsevier B.V. on behalf of Association of European Operational Research Societies (EURO). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

**RQ2.** Which neutralisation strategies do participants use most to rationalise committing e-banking fraud?

This study contributes to the body of knowledge surrounding the use of behavioural nudges in dissuading e-banking fraud – both practically and theoretically by demonstrating to what extent people employ neutralisation strategies to justify their behaviour. [Section 2](#) reviews the background literature. [Section 3](#) provides an outline of the methodological (and theoretical) aspects of this research. [Section 4](#) provides a discussion of this study’s findings within the context of the research questions. [Section 5](#) outlines the study limitations and provides readers with several research recommendations to consider when conducting similar future research. [Section 6](#) concludes the study.

## 2. Background

### 2.1. Impersonation

The most common e-banking threat is phishing which centres around gaining access to the customer’s credentials to impersonate them on some online service ([Shah et al., 2019](#); [Syniavska et al., 2019](#); [KrebsSecurity 2019](#)). If websites require only a single authentication check to permit access, this opens the door to account takeovers ([Claessens et al., 2002](#); [Choubey and Choubey, 2013](#)). Authentication is less reliable where a service provider does not make use of two-factor authentication (2FA) – a security measure few US banks enforce by default ([Aguiler, 2015](#); [Colbert, 2019](#)). Sometimes, customers’ own mistakes or omissions facilitate impersonation attempts. They might forget to log out of their accounts, save their credentials on public computers, or store their password insecurely ([Gehring, 2002](#); [Stobert, 2014](#); [Stobert and Biddle, 2014](#); [Sanchez, 2019](#); [Kenton, 2020](#); [Collins English Dictionary 2021](#)). Additionally, customers are ill-equipped to manage their passwords securely. They reuse passwords, write them down, or use weak passwords ([Boothroyd and Chiasson, 2013](#); [Stobert, 2014](#)). Unfortunately, such coping strategies increase the ease with which malicious third parties can gain access to e-banking accounts ([Inglesant and Sasse, 2010](#); [Egelman et al., 2011](#)). In such instances, traditional (and usually costly) security measures put in place by banks are rendered ineffective because it is impossible to detect impersonation if genuine credentials are used. By the time an account owner realises what has happened, accounts have often already been emptied ([Wang and Davis, 2023](#)).

### 2.2. e-Banking security

Banks may employ a variety of technical security measures to help manage the risks. These include lockouts, password composition (i.e., complexity) requirements, password length requirements, password expirations, and blacklists ([Gehring, 2002](#); [Egelman et al., 2011](#); [Florêncio et al., 2014](#); [Florêncio et al., 2014](#)). These are mostly software based ([Omariba et al., 2012](#); [Aravind et al., 2024](#)).

Despite a willingness to invest significant funds in security ([Yazdanifard et al., 2011](#))[70], banks are highly sensitive to potential impacts on customer convenience when implementing such mechanisms takeovers ([Claessens et al., 2002](#)). These challenges are compounded by the fact that no amount of security is ever sufficient with an ever-increasing number of security breaches occurring as of late ([Mason and Farah, 2023](#); [Toubba, 2023](#)).

Based on the information presented thus far, it is clear that, even though banks implement a wide variety of traditional security measures, e-banking fraud still occurs ([Ahmad et al., 2021](#)). We argue that security measures which incorporate (or consider) the human or behavioural aspect of information systems could potentially supplement existing technological security measures. This is where the use of behavioural interventions, such as nudges, become an attractive proposition. Thaler and Sunstein ([Thaler and Sunstein, 2008](#)) introduced the nudge concept in 2008. Essentially, they explain that all decisions are made within a

“choice architecture” – the environment within which the choice is made and when one is online, this includes all aspects of the user interface. A nudge is a manipulation of this choice architecture to persuade people to choose the wiser option, where the wiser option is better for the user. Behaving dishonestly is undeniably bad for perpetrator, so nudging is indicated in this context too.

Nudges have been deployed in a variety of disciplines to influence human behaviour. For example, Wang and Davis ([Wang and Davis, 2023](#)) propose the use of nudging to influence consumers to make better and more informed economic decisions. Ruggeri et al. ([Ruggeri et al., 2023](#)) takes the nudging process a step further by proposing the use of machine learning to personalise the behavioural interventions used to manipulate choice architectures. According to their research, this could enhance its efficacy in a public health context. They argue that the approach could be further adapted to automatically recalibrate which interventions are used based on the efficacy of those already in use. This kind of evaluation is advocated by Pawson ([Pawson, 2013](#)). Nudging has also recently been used to study households’ saving behaviour ([Despard et al., 2023](#)), the promotion of public transport ([Aravind et al., 2024](#)), public policy ([Banerjee and John, 2024](#)), improving tax compliance ([Alm et al., 2023](#)), and managerial decision-making in high-stress environments ([Renz et al., 2023](#)).

Crucially, nudging has also been used within the computing context. For example, Dolan et al. ([Despard et al., 2023](#)) employed digital nudging to encourage social network users to be more mindful of their privacy. Choe et al. ([Choe et al., 2013](#)) and Zhang and Xu ([Zhang and Xu, 2016](#)) employed nudging to reduce privacy-invasive applications on their devices. Turland et al. ([Turland et al., 2015](#)) and Jeske et al. ([Jeske et al., 2014](#)) employed nudging to encourage the use of secure wireless networks. Importantly, Ioannou et al.’s ([Ioannou et al., 2021](#)) systematic literature review found that nudging could alter privacy-related behaviour. Renaud et al. ([Renaud et al., 2017](#)) and Hartwig and Reuter ([Hartwig and Reuter, 2021](#)) employed nudging to improve password strength.

Having said this, we are not advocating for a purely behaviour-centric approach, nor an approach where behavioural interventions replaces existing security measures. Instead, we suggest a hybrid approach. In this paper, our aim is to explore the potential impact of behavioural nudging in dissuading e-banking fraud in the presence of warnings and notices raising awareness of the existence of traditional security measures. In doing so, our research makes an important contribution to the study (and use) of behavioural interventions in the honesty context.

## 3. Methodology

### 3.1. Theoretical considerations

To theoretically ground this study, we made use of Neutralisation Theory, which aims to explain the complex interaction between abnormal (i.e., deviant) behaviour and societal standards ([Sykes and Matza, 2017](#)). Crucially, Neutralisation Theory provides important insights into the ways in which people justify their deviant behaviour. Fraud can be considered a deviant behaviour because society does not approve of thieves. As such, Neutralisation Theory may enable us to gain greater insights into fraudulent behaviours as well as the processes (i.e., rationalisations) people use to manage the conflict between conformity and deviance. Neutralisation Theory’s central tenet is that deviant behaviour on the part of people results from cognitive processes that momentarily suspend their adherence to social norms, rather than explicitly rejecting societal norms. These cognitive processes take the form of rationalizations, which work as psychological tools people use to “neutralise” the socially imposed moral and ethical restraints on their behaviours. At its core, Neutralisation Theory lists five strategies that people could engage ([Matza, 2018](#); [Sykes and Matza, 2017](#)) to rationalise their deviant behaviours:

- **Denial of responsibility:** This tactic includes removing responsibility from the individual and attributing the behaviour to outside forces such as peer pressure or uncontrollable events. People might lessen feelings of guilt or shame by separating themselves from responsibilities and claiming that they did not have control over what happened.
- **Denial of injury:** In this case, people minimise the damage brought on by their behaviour and persuade themselves that nothing serious has happened. They may emotionally remove themselves from the effects of their actions thanks to this justification. For example, they could point to the fact that the person has insurance to cover their losses.
- **Denial of victimization:** Using this strategy, people claim they are the victims of their circumstances while maintaining that their acts were necessary to safeguard their interests or well-being. In this framing, the wrongdoer is shown as a protector rather than an aggressor.
- **Condemnation of the condemners:** Those who use this tactic cast doubt on the moral standing or honesty of those who criticise their behaviour. They question the validity of social standards and other people's opinions by discrediting detractors.
- **Appeal to higher loyalties:** This tactic involves citing commitments to a higher cause or group, which is frequently at odds with cultural standards. Individuals justify their behaviours as essential sacrifices made for a higher benefit by placing these loyalties front and centre.

These strategies act as cognitive tools that help people deal with the ethical dilemmas that deviant behaviour inevitably triggers. They enable people to engage in behaviours that go against social norms while still maintaining a positive self-concept. They act as a psychological "safety net" to help people reconcile their deviant behaviour with their desire for social approval. Its use within the fields of criminology (and cybercrime) is not new (Ebot et al., 2023; Maruna and Copes, 2005), and although researchers have investigated to what extent the environment affects the adoption of neutralisation procedures – we argue that a nudge-based approach is novel, contributing to the field. The link between this study's methodological elements and Neutralisation Theory can be summarised as follows:

- The nudges in our design conditions act as deterrent tactics. These nudges were interspersed within the pre-login and post-login design conditions (i.e., websites) explained below.
- We decided to use multiple nudges at the same time in order to maximise the ability of the choice architecture to influence the user and deter dishonesty. A study by Fanghella et al. (Fanghella et al., 2021) found that the nudges did not interfere with each other, which that meant a combination was worth testing in our study.
- The user environment was simulated with the use of three scenarios which participants were asked to read before exploring the websites as part of the experimentation process. See Tables A.1-A.4 in the appendix for an outline of these scenarios. Note that the experimentation process took place in phases with a participant first reading the scenarios and then being asked to explore all three design conditions. This was followed by the interview process to ascertain the rationalisations based on the participant's exploration of these design conditions. Furthermore, note that we did not place any explicit nudges on the website associated with the control condition. We did tweak any design elements on this version of the website, which would have unduly influenced participant behaviour.

### 3.2. Methodological justification

This study used a quasi-experimental approach to collect qualitative data from e-banking customers who were asked to experiment (and explore) the three design conditions. This was done by way of semi-structured interviews. We argue that the use of semi-structured

interviews is suitable given that it enabled us to:

- **Perform an in-depth exploration:** Researchers can delve deeply into the thoughts of interviewees who have engaged in aberrant behaviour through semi-structured interviews. Given that neutralisation tactics are frequently sophisticated and psychologically intricate, semi-structured interviews give interviewees a chance to go into great detail about their rationalizations and mental processes (Patton, 2014). Researchers might get insights using this way that could be challenging to learn using quantitative or more structured methods.
- **Flexibility:** Semi-structured interviews offer us a flexible format enabling us to modify our inquiries and probes in response to user responses or actions whilst exploring the websites (Olimpi et al., 2019). Such adaptability is essential when researching a complex idea like neutralisation since it enables the investigation of unanticipated directions and the explanation of statements that are unclear or conflicting (Rubin and Rubin, 2011).
- **Contextual understanding:** A variety of contextual elements, including the particular deviant behaviour, the environment (scenarios), and personal experiences, have an impact on neutralisation approaches. Semi-structured interviews offer a chance to comprehend the setting in which these methods are used. To contextualise user responses and develop a deeper knowledge of the processes at work, researchers can ask follow-up questions (Bryman, 2016). In other words, we were able to ask questions such as: why do you think this action is suitable (or not)?
- **Participant empowerment:** This ties into the above as we were able to ask open-ended questions which enabled interviewees to share their viewpoints and personal narratives. Giving participants a voice in the study process can be empowering (De Sutter et al., 2021). This further aids researchers in better understanding the subjective experience of rationalizing their deviant behaviour within the context of neutralisation investigations.
- **Ethical issues:** Researching abnormal behaviour and the justifications that support it can be delicate and even stigmatising for interviewees. Our use of semi-structured interviews enabled them to give their stories and justifications in a supportive and judgment-free setting, which promotes a more empathic and moral approach to research (Hakimi et al., 2020). Through increased trust and rapport between researchers and interviewees, more candid and open responses were obtained.
- **Comparative analysis:** Given that we were able to gather data from a wide variety of users, we were able to perform comparisons. In doing so contrasting the neutralisation strategies used across the provided scenarios.

In addition to the above, there is a wealth of similar (and recent) behavioural research that have used semi-structured interviews whilst utilising Neutralisation Theory (Addo, 2023; Edwards et al., 2022; Alshaiikh et al., 2021; Sakala and Chigona, 2020) or reviewed studies which used Neutralisation Theory in a similar context (Bilz et al., 2023).

### 3.3. Study participants

After receiving ethical clearance from the primary author's institution (approval no: 2022-5353-6499), e-banking customers were recruited via the Prolific and Amazon Mechanical Turk (MTurk) research support services (Hillman, 2022). Full informed consent was obtained from each user before participation for which they were remunerated at a fixed rate of £7.50 per hour - the USA's minimum wage (circa 2022). The sample size was relatively small ( $n = 15$ ), but adequate given the decision to carry out an in-depth qualitative analysis (McLeod, 2014; Boddy, 2016; Saunders et al., 2016). Interviewees were selected using convenience sampling (Jager et al., 2017), a non-probabilistic sampling technique where individuals (meeting pre-set criteria) are

recruited based on how easily they can be reached or accessed (Alkassim and Tran, 2016; Saunders et al., 2016). Individuals meeting the selection criteria (US citizens, > 21 years of age, English fluency, and active e-banking user) could apply to participate in the study. We focused on the US primarily because of its relatively low rate of two-factor authentication (2FA) adoption when using e-banking services (Horowitz, 2014; Colbert, 2019). To avoid sampling bias, we sampled using a stratified approach whereby an equal number of people were recruited from three age groups: young (21–39 years), middle (40–59 years), and senior (60 years and older). While the sample was not meant to be representative of the larger population of USA e-banking customers, this was implemented to ensure that perspectives of different age groups were sampled. See Table 1 below for a complete outline of the sample demographics.

### 3.4. Experiment design

During our experiment, the participants interacted with all three design conditions (i.e., websites); the design and functionality of which were based on an initial study of eight other international banks’ e-banking websites (Please see Table 2 for details). As part of the design process, Axure RP 10 (a wireframing tool) was used to develop functional versions of these three fictitious websites. As stated, the control version of the e-banking website represented an interface without the use of any deliberate nudges (see Fig. 1 below). The pre-login version represents an interface with nudges employed before a user logs in. Here, the nudges were aimed at preventing a third party from using compromised credentials to log in (see Figs. 2 and 3). The post-login version focused on employing nudges after the user had logged in. Note that once a user had logged in, they were redirected to an account summary webpage which contained the post-login nudges (see Fig. 4). Both the pre-login and post-login nudges were aimed at dissuading an individual from committing e-banking fraud. It is important to note that for experimentation purposes we defined the act of committing fraud as a participant who:

1. Viewed the account of legitimate account holder (view account menu option),
2. Added a recipient for a money transfer, and
3. Completed the relevant payment processes available.

### 3.5. Data collection

Our primary data consisted of semi-structured interview transcripts. A within-subjects approach was used as all interviewees were given the opportunity to interact with, and answer questions related to, all three design conditions. Interviewee interactions with the website(s) were also recorded to supplement the thematic analysis of the transcripts. The interviews and user interactions were recorded. We deemed a structured interview inappropriate given that it would not have afforded the opportunity to pose additional questions. The questions focused on the

**Table 1**  
Demographic outline of our sample.

| Demographics           | Group A<br>(21–39 years) | Group B<br>(40–59 years) | Group C<br>(60+ years) |
|------------------------|--------------------------|--------------------------|------------------------|
| Number of interviewees | 5                        | 5                        | 5                      |
| <b>GENDER</b>          |                          |                          |                        |
| Male                   | 3                        | 3                        | 2                      |
| Female                 | 2                        | 2                        | 3                      |
| <b>EDUCATION</b>       |                          |                          |                        |
| Associate degree       | 2                        | –                        | 1                      |
| Some college           | 1                        | 1                        | –                      |
| Bachelor’s degree      | 1                        | 2                        | 3                      |
| Some graduate studies  | –                        | 1                        | –                      |
| Master’s degree        | 1                        | 1                        | 1                      |

**Table 2**  
Nudge design.

|  | Design Conditions:  |   |   |
|--|---|---|---|
|  | Control   | Pre-Login   | Post-Login  |
| <b>Nudge:</b>                                    | No explicit nudges. Therefore, a neutral design to act as a behavioural baseline (see Fig. 1) | Nudges deployed as illustrated via the illustration of Website 1 (Figs. 2& 3) | Nudges deployed as illustrated via the illustration of Website 2 (Fig. 4) |
| <b>Rationalizations for dishonest behaviours</b> | N/A   | To be tested as a result of exploration when exposed to nudges                | To be tested as a result of exploration when ex-posed to nudges           |

behaviours and rationalizations of the third party within the provided scenarios. The websites were hosted locally on the primary author’s computer used during the interview and shown to the interviewees via Zoom’s “screen share” feature, which enables them to remotely interact with the e-banking websites. The interview guide is outlined in Appendix A.

### 3.6. Data analysis

The transcripts were analysed using thematic analysis, which focuses on grouping ideas and concepts found in qualitative data by formulating codes (Saunders et al., 2016). This method was appropriate due to the qualitative nature of the data and the nominal variation in the responses from the interviewees. It was used to look deeper at all the interviewee responses and to find common ideas and themes regarding how a hypothetical third party in the scenario could behave and rationalise their behaviour and decisions. Analysis was conducted using the NVivo QSR International software. The study employed the six-phase thematic analysis process as described by (Braun and Clarke, 2006). The first phase involved familiarizing ourselves with the data (Braun and Clarke, 2006). In the context of this study, this meant listening to the audio recordings of the interviews and manually transcribing the data. The second phase involved generating an initial list of codes (Braun and Clarke, 2006). This required going through the data set and sorting interesting observations from participant responses into various codes. The product of this phase was a full list of codes and several project map visualizations (see Figs. 7 and 8 in the Appendix).

The third phase involved grouping or sorting the various codes into broader themes (Braun and Clarke, 2006). Each theme generally referred to a common idea expressed by the participants during the interviews. The codes were reviewed before grouping them into initial themes. Note that the initial themes were primarily data driven (i.e., inductive), as they arose from a common idea found in the codes. The list of initial themes was then used as the primary input in the fourth phase focused on reviewing and refining the themes (Braun and Clarke, 2006). The initial group of themes shrank in size throughout this phase as some themes were merged with other themes due to their similarities (see Fig. 6 in the appendix for an example).

The refined themes were then used to produce this phase’s main product, namely the thematic maps. The thematic map represents the refined themes and how they may relate to other themes and codes. The penultimate phase of thematic analysis involved further refining the themes from the initial thematic map and writing detailed descriptions of each theme (Braun and Clarke, 2006). Each theme was then reconsidered in terms of what it revealed about the “bigger picture”. The number of themes shrank further after the refinement. The product of this phase was a set of core themes and subthemes that captured all the main findings from the data. Importantly, the above was repeated for the post-login and the pre-login design conditions.

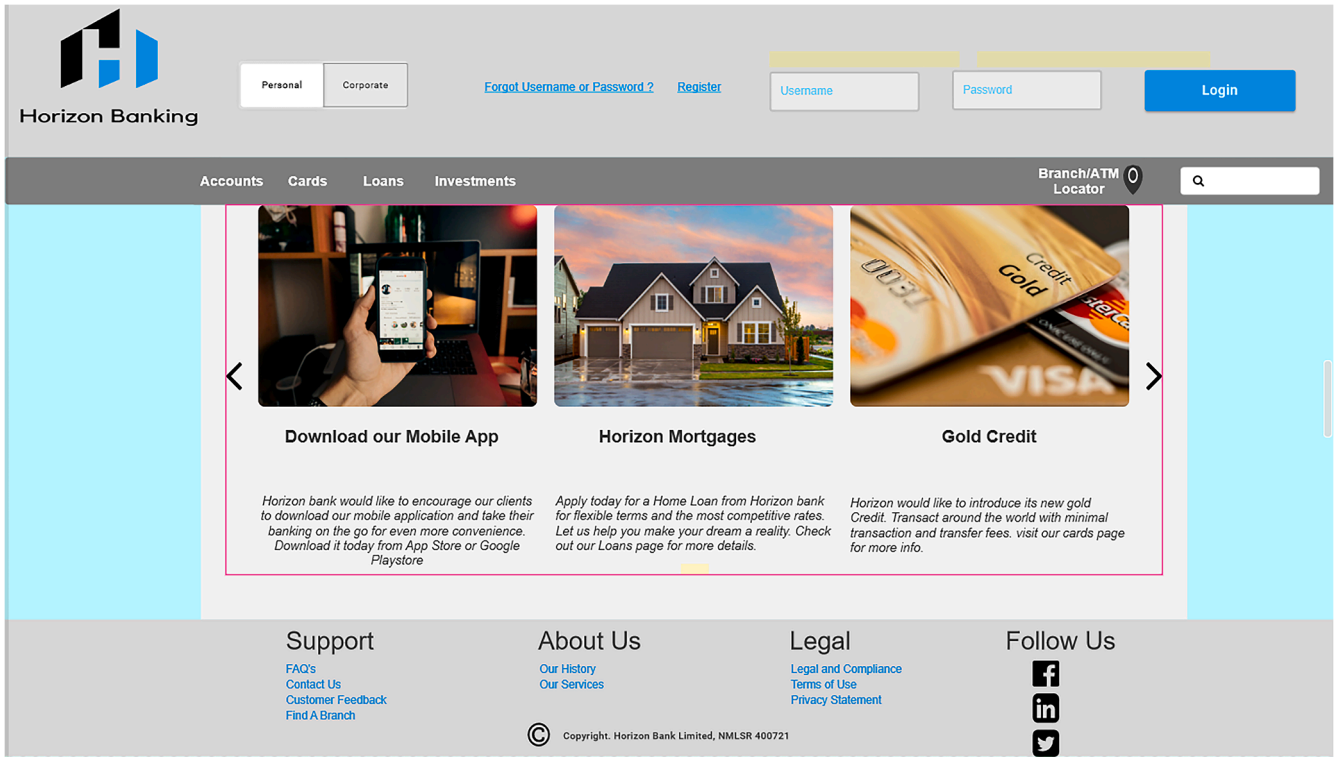


Fig. 1. Homepage of the control e-banking website.

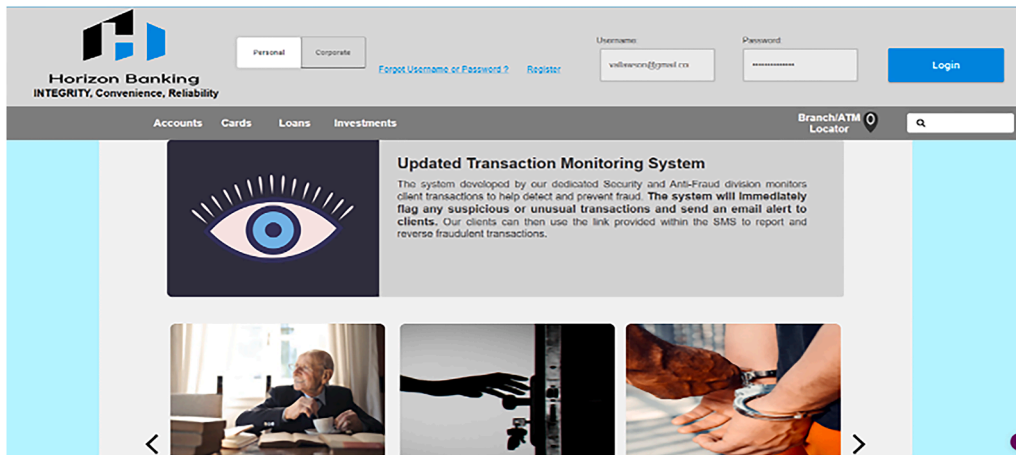


Fig. 2. The header of the pre-login interface.

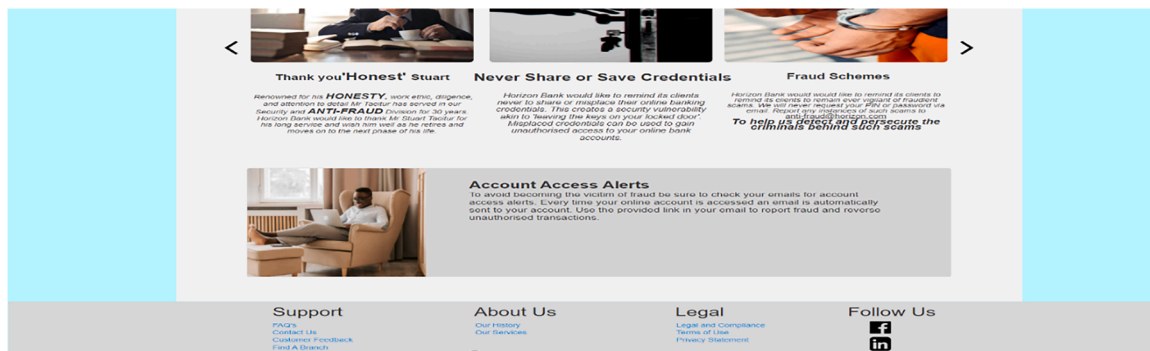


Fig. 3. The footer of the pre-login interface.

Horizon Banking  
INTEGRITY, Convenience, Reliability

V. Lawson  
If this isn't you please [Click Here](#) [Logout](#)

My Accounts My Cards My Loans My Investments Branch/ATM Locator

Summary  
Transaction History  
Payments  
Internal Transfers

**Accounts**

| First Name(s) | Surname | Account type | Account Number | Balance \$ | Available Balance \$ |
|---------------|---------|--------------|----------------|------------|----------------------|
| Vanessa       | Lawson  | Checking     | 6347300380     | 7722.60    | 7772.60              |

Today's Date —

Support  
FAQ's  
Contact Us  
Customer Feedback  
Find A Branch

About Us  
Our History  
Our Services

Legal  
Legal and Compliance  
Terms of Use  
Privacy Statement

Follow Us  
f  
in  
t

© Copyright: Horizon Bank Limited, NMLSR 400721

Fig. 4. The summary webpage of the post-login e-banking website.

## 4. Findings and discussion

### 4.1. Effectiveness and placement of nudges

This section discusses the effectiveness of the behavioural nudges (i.e., deterrent tactics) as used within the pre-login and post-login design conditions. This discussion aligns with the first research question:

**RQ1.** Which behavioural nudges are most effective at dissuading e-banking fraud and where should they be placed?

Overall, from the nudges which encouraged empathy as well as creating a stronger impression of traditional website security and monitoring (i.e., clear warnings in this regard) seem to be the most effective ways to dissuade individuals from committing e-banking fraud. Importantly, this was most effective when reiterated repetitively. For example, the image of Vanessa (the individual illustrated in Fig. 4) and the “If this isn’t you, please click here” link – was used together in a deliberate and repetitive manner. The are other examples of this such as the many warnings used (see Appendix B). This combination of deterrent tactics was particularly effective at making people contemplate their behaviour:

*The fact that there is something every step, literally, from the time I saw you know the screen of. ‘Here’s the photo. Is this you?’ I’m having that repetitiveness, or I have to be faced with it. Oh, I’m committing a crime, or they know they’re going to catch me...*

Participant 12 (Male, 33, Master’s Degree)

Importantly we found nudges aligned with the cultivation of empathy (see Appendix B) to be most effective when used in the post-login design condition.

*So, I think that seeing the picture here makes it, like, very personal, and I think that this person in the scenario would feel very bad about, like, tampering with any information here. With this, with two large pictures staring at you and she’s obviously an older woman. She’s smiling. She seems friendly, so I would probably log out in this case or hit ‘If this isn’t you, click here’, so I probably do the same thing. I mean, do the right thing here in here. Hit click here.*

Participant 3 (Female, 30, Bachelor’s Degree)

For the following participant the cultivation of empathy also has age implications, which seemingly further strengthens the effect.

*...And that she’s a bit older. So, she’d be less likely to catch on to what’s happening.*

Participant 5 (Male, 47, Bachelor’s Degree)

This is an important finding making it directly (and practically) applicable to the banking industry - irrespective of user environment. We therefore recommend that banks should focus on creating a post-login environment where the user should “picture” and thus imagine the impact of fraud on the legitimate account holder (i.e., Vanessa in this instance). Our analysis of the interview data also indicated that it is vital to place the nudges in an optimal location. In this regard, our findings suggest that the post-login design condition is more effective than the pre-login design condition. Most interviewees viewed the post-login design of the website to be more effective at dissuading e-banking fraud. In fact, only seven out of the 15 interviewees clearly displayed behavioural intentions to commit e-banking fraud whilst exploring the pre-login website. In short, banks are advised to focus on the placement of nudges after a user has logged in.

### 4.2. Rationalizations

Although our qualitative analysis revealed a mixture of themes, we focus exclusively on the post-login design condition here. We argue this is most appropriate given that our findings indicate this to be the most effective design condition to use when placing nudges. In particular, we set out to understand how the rationalizations we extracted align not only with our theoretical framework (i.e., neutralisation strategies), but also the nudges used within the post-login design condition (see entire list of post-login nudges in Appendix B and rationalization descriptors in Appendix C). To visually summarise the latter alignment, we developed two Sankey diagrams (see Figs. 5 and 6 below). We argue its suitability based on the fact that it enabled us to illustrate how the rationalizations (on the left in Fig. 5) align with the neutralisation strategies (on the right in Fig. 5) whilst taking relative frequencies into account. For example,

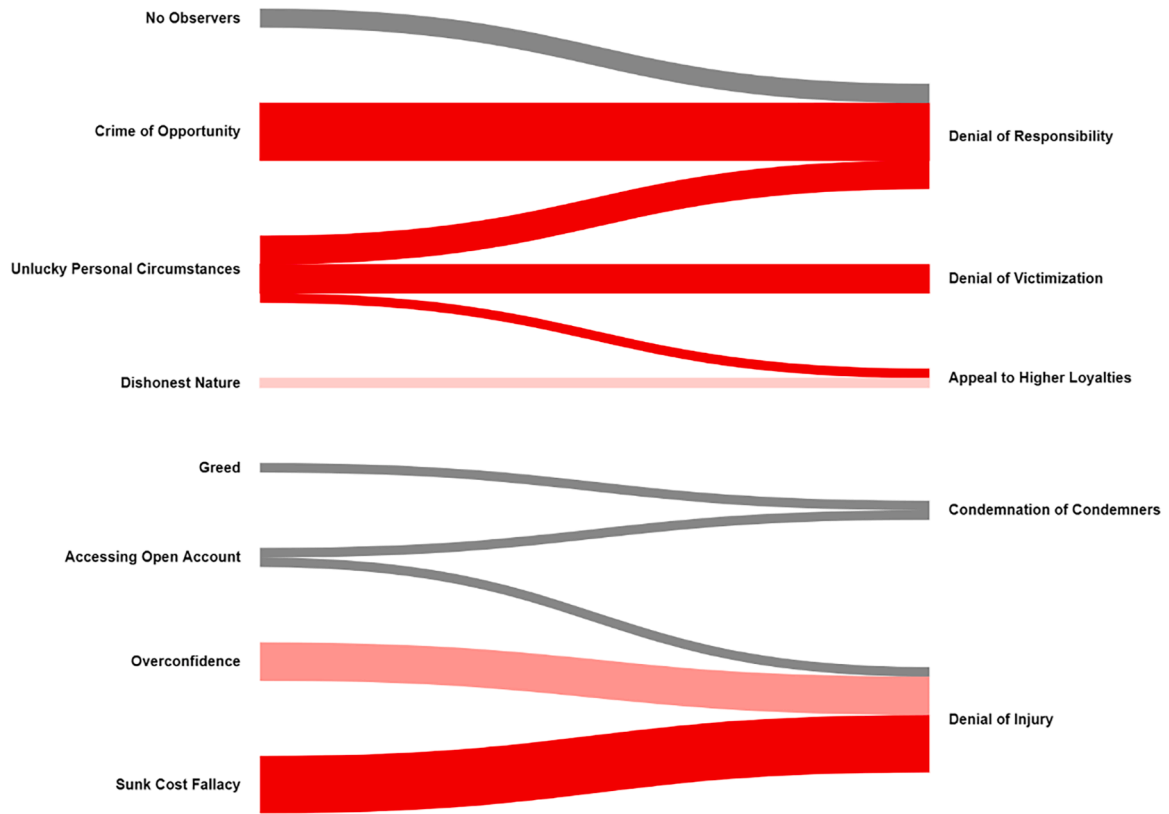


Fig. 5. Alignment of rationalizations and neutralisation strategies (illustrating theoretical alignment).

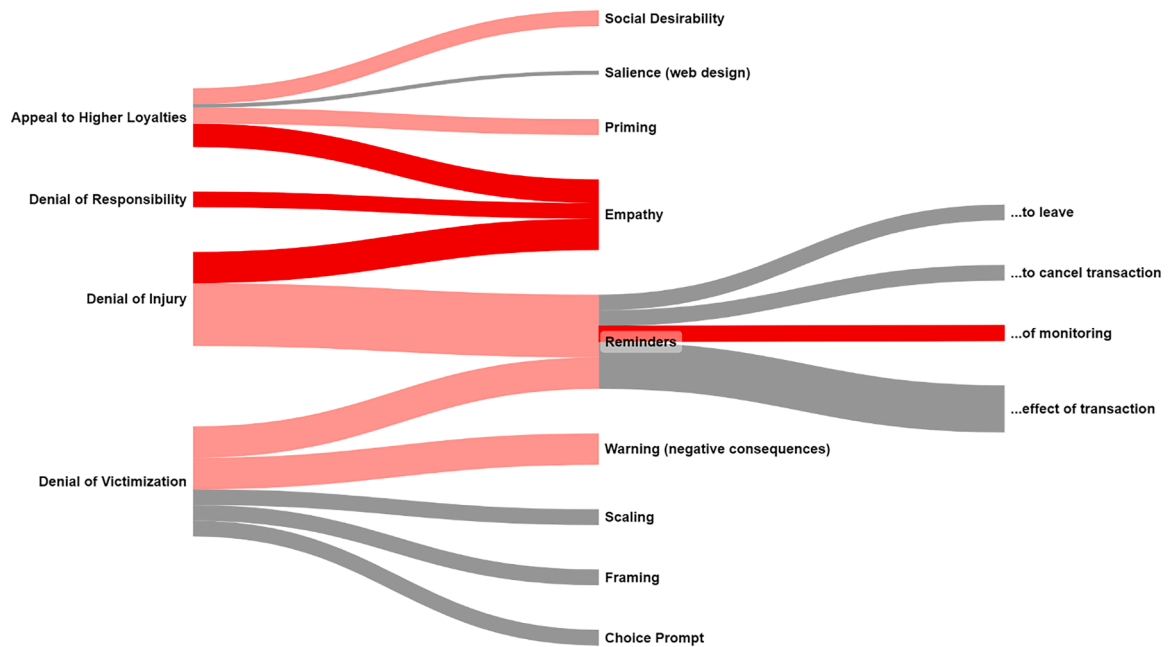


Fig. 6. Alignment of neutralisation strategies and behavioural nudges.

and by using the interview data, we calculated the frequency that the various rationalizations were mentioned in the interview transcripts. The most prominent rationalizations are illustrated in varying shades of red within Figs. 5 and 6. In doing so, indicating the relative importance of the rationalizations (and neutralisation strategies) within an e-banking context. The same applies to Fig. 6- albeit to illustrate our ranking as to the level of effectiveness of the behavioural nudges.

Importantly, the data and associated discussion of Figs. 5 and 6 enabled us to address the second research question: RQ2: Which neutralisation strategies do participants use most to rationalise committing e-banking fraud?

### 4.3. Contributions

Our findings articulate theoretical and practical contributions by providing support for the alignments illustrated in Figs. 5 and 6. We refer readers to Appendix C, which contains detailed information relating to our motivations (and empirical support for) the alignments illustrated.

#### 4.3.1. Theoretical implications

We argue that the most prominent rationalizations namely (1) crime of opportunity, (2) unlucky personal circumstances and the (3) sunk cost fallacy expand the scope of Neutralisation Theory. Traditionally, neutralisation strategies were considered a static set of techniques employed before or after an individual commits a deviant act (Siponen et al., 2020). However, these themes suggest that rationalization processes can be dynamic, evolving over time as individuals become more deeply involved in their behaviour especially, within an e-banking context. This expansion underscores the fact that neutralisation strategies are not limited to premeditated justifications but can adapt in response to changing circumstances and decisions. The emphasis on the sunk cost fallacy highlights the significance of ongoing rationalization processes in sustaining deviant behaviour. While traditional neutralisation strategies primarily address the initial rationalizations that enable deviance, this theme illustrates that individuals engaged in fraudulent activities may continually rationalise their actions to justify persisting in their pursuit to “explore” another person’s e-banking account. This temporal dimension of rationalization, where individuals rationalise their actions not just before, but also during and after deviant acts, provides a new perspective for understanding the durability of deviant behaviour within an e-banking context.

Our findings also emphasise the importance of environmental factors in shaping the rationalization processes of fraudsters. The rationalizations crime of opportunity and unlucky personal circumstances underscore how external circumstances and situational factors influence an individual’s ability to rationalise their actions. This insight suggests that Neutralisation Theory should consider the interplay between personal motivations and external context (i.e., user environment), recognizing that rationalization strategies may vary depending on the specific circumstances surrounding the deviant act. This is, however, not a new realization, with varied research into how personal motivation, and a user’s environment, influence deviant behaviour (De Bruyn et al., 2023; Ruggeri et al., 2023). Having said this, much of the latter research is scattered among a few (varied) disciplines and not focused on cybersecurity or cybercrime.

Our rationalizations also highlight the adaptability of rationalizations to individual needs and circumstances. Individuals may switch between different rationalization strategies based on their evolving situations and environmental pressures. For example, they may use crime of opportunity when explaining their initial involvement but shift to the sunk cost fallacy to rationalise their continued engagement. This adaptability suggests that Neutralisation Theory should acknowledge the flexibility of these strategies, challenging the notion that individuals adhere to a fixed set of rationalizations. Understanding the dynamic and evolving nature of rationalizations can have theoretically enhance the study of intervention and prevention strategies. Traditional approaches that focus solely on pre-emptive deterrence may miss opportunities to disrupt ongoing rationalization processes. By recognizing the temporal nature of rationalizations, interventions can be designed to address shifting cognitive patterns and motivations, potentially reducing recidivism and encouraging desistance from criminal behaviour.

#### 4.3.2. Practical implications

This study’s main practical implications include the ability to raise user knowledge of e-banking security. People frequently have a false sense of security due to traditional security measures, such as

monitoring, which are frequently undetectable to them. People are reminded of the value of security and are less inclined to participate in unsafe behaviour by seeing alerts about these safeguards. Additionally, an innovative tactic is the employment of an image of an elderly woman to arouse sympathy for e-banking customers. This not only appeals to consumers’ emotions, but it also gives victims of cybercrime a human face. Because of the potential consequences of their actions on vulnerable people, consumers may be more careful when using online banking services. By including cautionary warnings during the login and transaction processes, financial institutions can incorporate these behavioural nudges into their online banking platforms. Additionally, they might emphasise the potential repercussions of careless behaviour by using relatable imagery like the elderly woman.

Hasty actions, such as clicking on phishing links or revealing personal information, are frequently preyed upon by cybercriminals. The results of the study indicate that behavioural nudges can successfully lessen such impulsive behaviours. People are more likely to halt and consider their next move when presented with cautionary messages and empathetic visuals. This decrease in impulsive behaviour safeguards them, as a whole, while also enhancing the security of the e-banking ecosystem. Financial institutions and their clients profit when fraud efforts are less successful. To reduce impulsive actions, e-banking platforms can implement multi-step authentication processes, display warnings before critical actions, and use sympathetic imagery in security notifications. User education campaigns can further reinforce these concepts.

In order for customers to feel confident in the security of their financial transactions, building trust is essential in the e-banking industry. Financial institutions can show their dedication to user safety by using behavioural nudges successfully, which will increase trust and client loyalty. Security alerts and empathetic graphics are displayed, which not only protects consumers but also shows how committed the institution is to defend their interests. This may lead to higher customer retention rates and a favourable reputation in the cutthroat e-banking market. Financial institutions can emphasise their proactive approach to security by utilizing these insights in their marketing and communication efforts. Additionally, they can collect user feedback to continuously hone and enhance their security nudges.

The study’s findings also have ramifications for the financial industry’s compliance and regulatory systems. The prevention of fraud and cybersecurity are becoming more and more important to regulatory organisations. Effective behavioural cues that deter fraud can be in line with legislative demands, potentially lowering compliance risks for financial institutions. Financial institutions should keep up with changing legal requirements and make sure that all of their security measures, including behavioural nudges, comply with them. Compliance can give an organisation a competitive edge by showing clients that it upholds the highest security requirements.

## 5. Limitations

Although we tried to minimise those study design aspects which may limit the applicability of our findings, there are some we would like to acknowledge. For example, we presented interviewees with different scenarios and behavioural nudges while they were exploring the various e-banking websites. This differs from traditional experiments where researchers alter only one variable while keeping the others constant to help evaluate the effect that changing that specific variable has on the results. This did not translate perfectly in this study due to time constraints. For instance, although the pre-login and post-login design conditions employed their own set of behavioural nudges at various places within the e-banking website, they obviously used aspects of the control. This aspect of the overall study design complicates direct comparisons and views of opinion. Additionally, our study participants may have diverse cultural backgrounds; all of which are underpinned by their own belief systems. This also complicates direct comparisons. Hence our avoidance of direct comparisons based on demography. We



also found indications that some interviewees were likely to behave honestly – at least based on what was discussed. This seems encouraging, but more structure, and a longitudinal approach, is required to further this field of study. In this regard, we provide scholars with several research recommendations which we argue bridges the gap between our exploratory findings and those advocated by Pawson (Pawson, 2013) on the realities of engineering true and lasting behavioural change.

The sample size of 15 participants, while adequate for studies that carry out qualitative analyses, may limit the generalizability of the findings. It is necessary to carry out further studies to confirm or deny our findings.

## 6. Recommendations

**Recommendation 1:** There is a need for researchers to conduct systematic reviews (possibly even meta-analyses) that examine how the various principles and methods of (behavioural) evaluation, can be integrated with theories about deviance. Particularly focusing on the process of rationalization. What the field really requires is an evidence-based assessment as to how effective these evaluation techniques are, and in which environments they are likely to produce such results. Supplementing these with specific interventions would further enhance the contribution. Tangentially, some researchers may wish to include a review of established ethical frameworks suited to the evaluation of behavioural interventions aimed at reducing deviant behaviour. Possibly even including elements as to how ethical considerations can be integrated into the evaluation process itself. Especially within contexts where the evaluation itself might influence the rationalization processes of individuals, such as what we found in our study. This, in turn, emphasises the importance of using a multidisciplinary strategy to treat deviance thoroughly. The goal is to increase the efficiency of interventions created to lessen deviant behaviour by integrating assessment concepts with deviance theories. Systematic evaluations of the effects of interventions within a theoretical framework can reveal tactics that successfully address the underlying reasons of deviance, hence assisting in the development of more targeted and effective preventative measures. Scholars may consult classic texts on program evaluation, such as that of Rossi et al. (Renz et al., 2023), which offers a foundation in evaluation principles and methodology, to support similar studies. Moreover, investigations of the foundational criminological literature, such as Rational Choice and Situational Crime Prevention: Theoretical Foundations by Newman and Clarke (Newman and Clarke, 2016), provide insightful information about the theoretical underpinnings of deviance, including the application of Rational Choice Theory.

**Recommendation 2:** As indicated above, there is a clear absence of longitudinal studies that examine the long-term effects of behavioural interventions that target further understanding the evolution of rationalization processes and deviant behaviour. It would be interesting to get an understanding as to how the impact of interventions are sustained over time, and whether individuals revert to previous rationalizations. In other words, further exploring those environments where the sunk cost fallacy was brought up. Although several similar longitudinal studies have been conducted, most focus on cyberbullying (Kowalski et al., 2022; Pabian and Vandebosch, 2016; You and Lim, 2016; Hemphill et al., 2012). To our knowledge, none have focused on e-banking or related contexts.

**Recommendation 3:** To further argue the influence of demography and psychological traits, we advise researchers to holistically evaluate the psychological profiles of individuals engaged in deviant behaviour within e-banking or similar contexts. This area of inquiry is motivated by the realization that interdisciplinary cooperation, particularly between criminologists and psychologists, is essential to gaining a comprehensive knowledge of deviant behaviour. Such interdisciplinary cooperation is warranted because it holds out the prospect of a more comprehensive and nuanced understanding of abnormal behaviour. The examination of

how unique personality traits, cognitive biases, and moral reasoning processes interact with particular deviant behaviours and the persistence of these behaviours across time is particularly important. We advise researchers to follow a similar approach to Abdullah & Marican (Abdullah and Marican, 2016), with the intention to study a variety of personality models and not just the Big Five. In this vein, researchers can look into the relationship between impulsivity, narcissism, or psychopathy and the propensity to commit e-banking fraud and the rationalizations provided to justify such behaviour. The tactics indicated in recommendations 1 and 2 must be used with these psychological questions as part of the recommended method. Researchers can advance the study of deviant cyber behaviour by combining insights gained from the examination of the psychological drivers of deviance and the evaluation of therapeutic effectiveness. Through this synergy, deviant e-banking behaviour can be prevented and mitigated by better understanding the complex interactions between intervention tactics and individual psychological traits. Additionally, it is crucial for researchers to think about using cross-cultural and contextual studies in order to widen the scope of their research in this field. This analytical strategy looks to see if the effects of interventions and the psychological factors that influence deviant behaviour differ depending on the cultural and situational environment. Scholars are encouraged to investigate the cultural aspects of crime and deviance (Fanghella et al., 2021). As a result, researchers may investigate how various cultural norms, beliefs, and socioeconomic characteristics affect the justification techniques used by those who commit e-banking fraud. Scholars might better understand how societal variables influence the rationalisation of antisocial behaviour by exploring these cultural and contextual components. This information is crucial for creating culturally sensitive intervention techniques that are aware of the unique demands and driving forces of various communities. Therefore, this multidisciplinary study strategy promises to deepen our understanding of problematic online behaviour and considerably advance the creation of efficient preventative and remedial strategies for e-banking and related fields.

**Recommendation 4:** Given the prevalence of artificial intelligence, we advise researchers to consider studying how these technological advancements influence behaviour change. For example, how do these advancements impact the effectiveness of behavioural interventions and the rationalization processes of individuals engaged in e-banking fraud. More importantly, do these advancements lead to behavioural change? To our knowledge no research has been conducted to investigate the latter.

**Recommendation 5:** Researchers are advised to analyse the policy and regulatory implications of our findings. Assess how insights into rationalization processes and intervention effectiveness can inform the development of policies and regulations aimed at preventing and addressing e-banking fraud.

## 7. Conclusion & future work

The objective of this study was to determine which behavioural nudges are more effective at dissuading e-banking fraud. In particular, whether they are more effective if they are placed before or after a user has logged into their e-banking portal. Importantly, the study also sought to understand how individuals rationalise their (deviant) behaviours if they do decide to go ahead and commit e-banking fraud. Using a quasi-experimental approach, we conducted 15 semi-structured interviews with e-banking customers to understand how they would use three versions of a fictitious e-banking website based on the scenarios we provided them with. One of the websites acted as a control, which incorporated no explicit nudging mechanisms. The other two websites incorporated nudges either before or after a user had logged into the fictitious e-banking portal. Our findings indicate that banks should focus on implementing nudges focused on encouraging empathy as well as those which increase awareness of e-banking security and monitoring. In terms of placement, our findings indicate that nudges are most effective

if they are placed after a user logs into an e-banking website. Our analysis further indicated that the most prominent rationalisation for committing e-banking fraud centres on the opportunity to commit such fraud.

In terms of future work, it would be advisable to carry out this study with a larger and more diverse sample of eBanking customers from various countries. Moreover, it would be advisable to carry out longitudinal studies to determine whether the nudges would retain their power as people become more familiar with their presence. Finally, it would be worth experimenting with different nudge combinations to reveal possible interplays between them.

**Funding**

This research received funding from the National Research Foundation of South Africa.

**Data availability statement**

Data not available due to ethical restrictions.

**Appendix A - Scenarios and interview guide**

[Table A1](#), [Table A2](#), [Table A3](#), [Table A4](#)

**CRedit authorship contribution statement**

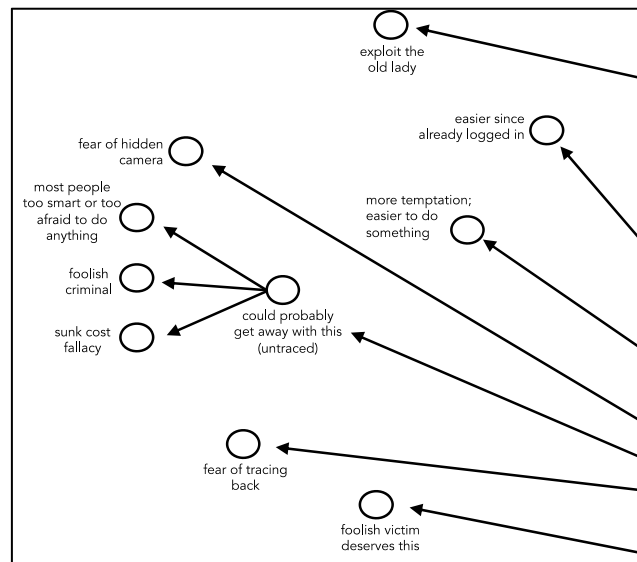
**Takudzwa Mutyavaviri:** Data curation, Formal analysis, Investigation, Visualization, Methodology. **Karl van der Schyff:** Conceptualization, Methodology, Supervision, Writing – original draft, Writing – review & editing, Visualization. **Karen Renaud:** Conceptualization, Methodology, Supervision, Visualization, Writing – original draft, Writing – review & editing.

**Declaration of competing interest**

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

**Acknowledgments**

We would like to thank Jacques Ophoff for his valuable feedback and suggestions during the development of this study.



**Fig. 7.** An extract of a larger project map visualization.



Fig. 8. An initial thematic map associated with post-login design condition (post phase 3).

Table. A.1  
Scenario 1.

| Scenario   | Question  | Motivation  | Research Alignment |
|--|---|---|--------------------|
| <p>“Jack/Jill Taylor was recently involved in a small car accident. They’ve gone to visit their local Internet café to browse the web in search of an affordable local mechanic to repair their car. Besides Jack/Jill Taylor, there isn’t another customer in the café. <u>While walking past, Jack/Jill notices one of the machines is on and has an e-banking website open. Credentials are on a sticky note under the keyboard.</u>”</p> | <p>Given what you have seen on this version of the interface, what do you think Jack/Jill would do if they encountered it along with the credentials?</p> | <p>Get a sense of what a third party may do if they encounter someone else’s e-banking credentials – establishing a baseline of behaviour, as the control version of the website is as neutral as possible.</p> | RQ1                |
|  | <p>What would Jack/Jill’s thought process (or rationalisation) be when making that decision?</p>  | <p>Get a sense of the rationalisations that a third party may go through when they make their decision about what to do on the website.</p>   | RQ2                |

Table. A.2  
Scenario 2.

| Scenario   | Question  | Motivation  | Research Alignment |
|--|---|---|--------------------|
| <p>“While walking past, Jack/Jill notices one of the machines is on and has an e-banking homepage open. Jack/Jill also notices that the e-banking credentials seem to have been saved on the machine.”</p> | <p>Jack/Jill did ____!<br/>Would they also commit an unauthorised transaction?</p>  | <p><b>General idea:</b> Based on observed behaviour while the participant is roleplaying, how would a third party on the pre-log page behave? Beyond using the credentials, would they go a further step and perform unauthorised transactions?</p> | RQ1                |
|  | <p>What was Jack/Jill’s thought process or rationalisations for deciding to do that (hit login) (or transact)?</p>  | <p>Get a sense of the rationalisations a third party may use for their behaviour.</p>   | RQ2                |
|  | <p>Going back to the homepage of the interface, what aspect(s) or feature(s) would have stood out the most to Jack/Jill?<br/>Did those aspects affect (play a role in) Jack/Jill’s decision or thought process? If so, how?</p> | <p>Get a sense of what nudge(s) the participant may have noticed on the page and, subsequently, the potential effect they may have had on the behaviour and rationalisations of a third party.</p>  | RQ1                |



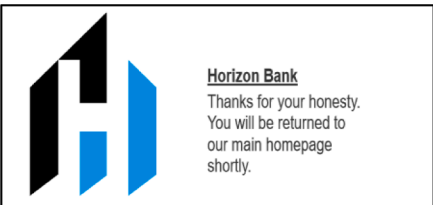
**Table A.3**  
Scenario 3.

| Scenario  | Question  | Motivation  | Research Alignment |
|---|---|---|--------------------|
| “While walking past, Jack/Jill notices one of the machines is on and has an e-banking website open. Jack/Jill also notices the previous user forgot to log out of their account!” | Jack/Jill did ___!<br>What was Jack/Jill’s thought process or rationalisations for deciding to do that click (or transact)?         | Observe what the participant roleplaying as the third party on the website would do on this version of the fictional e-banking website. Learn what a third party is likely to do in the scenario. Also, discover some of the rationalisations a third party may use if the e-banking account is open. | RQ1 & 2            |
|   | Looking back to the pages you encountered in this post-log version, would any feature(s) or aspects(s) have stood out to Jack/Jill? | Get a sense of what nudge(s) the participant may have noticed on the page and, subsequently, the potential effect they may have had on the behaviour and rationalisations of a third party.   | RQ1                |

**Table A.4**  
Scenario 4.

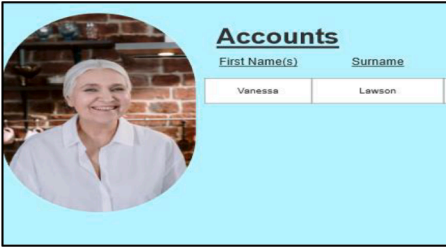
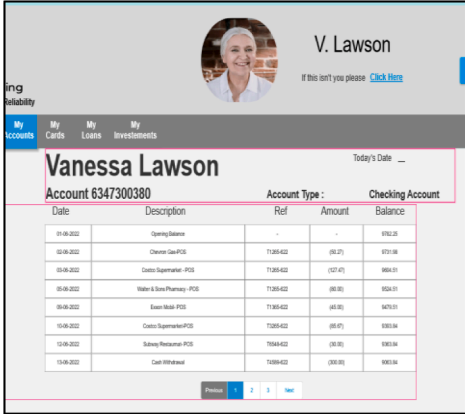
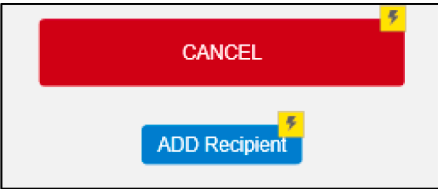
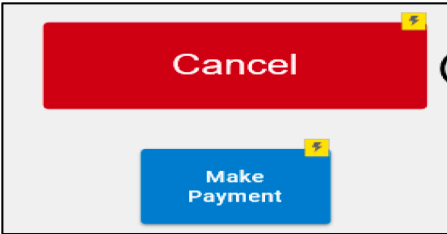

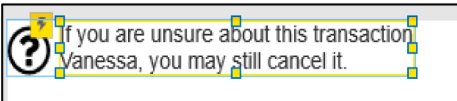
| Question  | Motivation  | Research Alignment |
|---|---|--------------------|
| Looking back between the pre-log and post-log versions, which version could have had the more significant effect on Jack/Jill’s behaviours and rationalisations? Why? | As close to a direct answer to RQ2 as we can get from the participant. It helps to get a sense of where on e-banking websites it may be more effective to place some nudging mechanisms.  | RQ1 & 2            |
| If both versions (halves) were combined, how would this impact the behaviour and rationalisations of Jack/Jill? (If it makes any difference at all?)                  | While the project may have sought to compare and contrast nudges employed at different steps/stages, in reality, nudges may be used across the whole site. The motivation for this question is to check if this would yield additional benefits in terms of dissuading e-banking fraud or if banks should instead focus on one step/ stage. | RQ2                |
| Which aspect on all three versions (specifically fraud, yes) had the most effect on Jack/Jill’s behaviour?  | Get an idea about what may overall have been the most effective nudge employed. Subsequently, gaining a sense of which was the most effective at dissuading e-banking fraud.  | RQ1                |

**Appendix B - Nudges within post-log design condition**

| Nudge (Screenshot)  | Behavioural Nudge   | Neutralisation Strategy                      |
|---|---|--|
|  | <b>Social desirability and priming:</b><br>The slogan below the company logo acts as a constant reminder to be honest. Social norm(s)/value(s) of integrity are brought up. Since it is ever present across the interface, it acts as a prime, even if only read once. Integrity is put in CAPS to stand out on this interface. | Appeal to Higher Loyalties                   |
|  | <b>Empathy, reminders to leave</b><br>The account holder’s picture in the header is a constant reminder to unauthorised visitors. “Click Here” is constant to give unauthorised people the option to leave the website at any stage.  | Appeal to Higher Loyalties, Denial of Injury |
|  | <b>Positive reinforcement</b><br>Honesty is acknowledged after they use “Click Here” in the header.   | No apparent link based on interview data     |

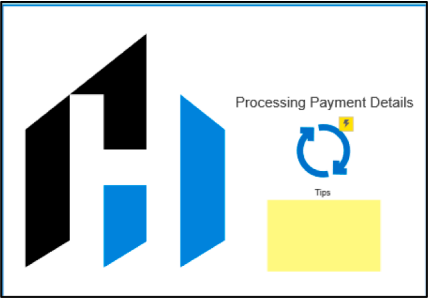
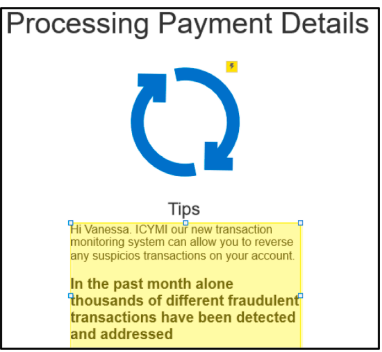

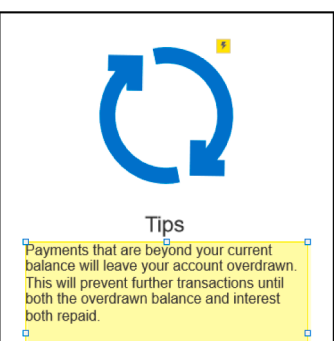
(continued on next page)

(continued)

| Nudge (Screenshot)  | Behavioural Nudge  | Neutralisation Strategy                    |
|---|--|--|
|    | <p><b>Empathy</b><br/>Picture of the account holder (full-sized now) is meant to give unauthorised people a better picture of the victim (account holder) if they do end up committing fraud. Put a face to the name they constantly see.</p>  | Denial of Injury                           |
|    | <p><b>Empathy</b><br/>Transaction history gives an insight into the account holder's life and spending patterns. While present on all three versions of the website, the empathy aspect is more apparent on the post-log design condition due to the presence of the account holder's picture.<br/>Account transactions in the post-log design condition have also been altered to generate more sympathy with "Vanessa" and her sweet old lady image.</p> | Denial of Injury, Denial of Responsibility |
|   | <p><b>Salience (ordering) and positioning.</b><br/>The cancel button is placed in a location that breaks the normal flow (reading form, then option to confirm/submit is the normal flow). Placing it before adding the recipient makes it more salient and nudges the user to cancel.</p>   | No apparent link based on interview data   |
|  | <p><b>Salience (deceptive visualisations) and positioning</b><br/>The size of the cancel button is significantly larger than the other button. It nudges the user towards cancelling the transaction or process.</p>   | No apparent link based on interview data   |
|  | <p><b>Reminder (certainty to transact)</b><br/>The user, authorised or not, always has the option to cancel a transaction. It displays when the page opens and when the question mark icon is hovered over.</p>  | Denial of Injury                           |
|  |  |  |

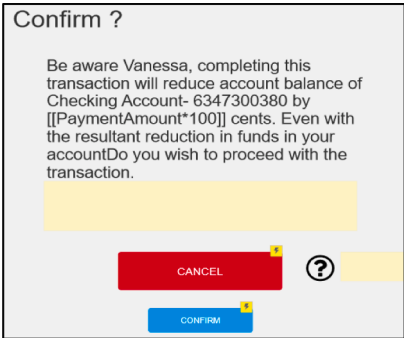
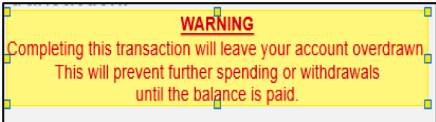
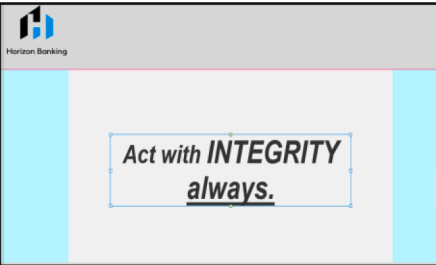
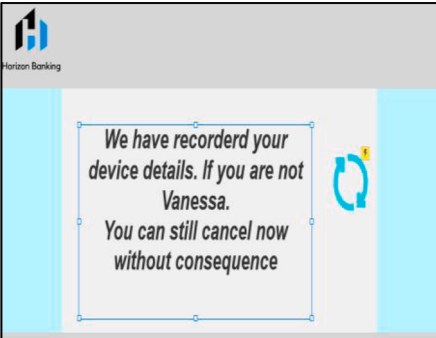
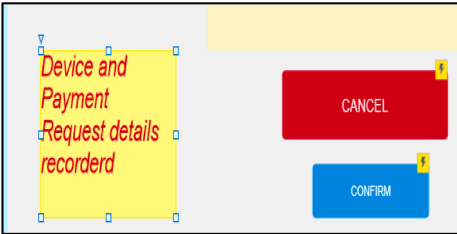
(continued on next page)

(continued)

| Nudge (Screenshot)  | Behavioural Nudge   | Neutralisation Strategy                         |
|---|---|---|
|    | <p><b>Speed bump</b><br/>The user is forced to slow down and think a little while completing a payment. Cycles through three “tip messages” as the user waits for the payment details to be processed.</p> <p><b>Friction</b><br/>Tips messages place reminders just before the user decides on the alternate path they may take; in other words, avoiding committing online banking fraud.</p> | <p>No apparent link based on interview data</p> |
|    | <p><b>Reminder (monitoring)</b><br/>One of many repeated reminders about the monitoring of transactions. It helps reduce the distance by making it more apparent that unauthorised people like the third party were detected and most likely prosecuted in the past. Hints that past unauthorised people have been caught and punished before (salience of consequences).</p>                   | <p>Denial of Injury</p>                         |
|   | <p><b>Reminder (opting out)</b><br/>Gives all users a reminder that they can opt out and stop any process/transaction.</p> <p><b>Friction</b><br/>This specific tip explicitly reminds them that they could turn back as the cancel button has been available as an option on all the pages they have encountered. The cancel button is present on the page.</p>                                | <p>No apparent link based on interview data</p> |
|  | <p><b>Warning (negative consequences) and reminder (effect of transaction).</b><br/>It makes it apparent that it is possible to deplete and overdraw the account, leaving the account holder with an overdraft.</p>   | <p>Denial of victimisation</p>                  |

(continued on next page)

(continued)

| Nudge (Screenshot)  | Behavioural Nudge   | Neutralisation Strategy                         |
|---|---|---|
|    | <p><b>Change scale</b><br/>The amount to be paid is expressed in cents to overemphasise (exaggerate) its impact.</p> <p><b>Framing and loss aversion</b><br/>Reducing the account's balance paints the payment transaction in a very negative light. Payment is phrased in such a way that the account holder is left worse off. An alternative would have been to phrase the transaction regarding what the recipient gains. Payment's impact is shown via the balance reduction aspect of the message.</p> <p><b>Prompted choice</b><br/>Users can confirm or cancel the transaction.</p> <p><b>Changing ease and convenience and enhancing or influencing active choosing</b><br/>The extra step of confirming payment is only available on the post-log design condition. The prompt forces customers to confirm their payment, unlike the control, which skips straight ahead to the recipient's page.</p> <p>Prompt combined with the other mentioned nudges.</p> | <p>Denial of victimisation</p>                  |
|    | <p><b>Warning (negative consequences) and reminder (effect of transaction)</b><br/>It should only appear when the user's transaction threatens to leave the account overdrawn.</p>  | <p>Denial of victimisation</p>                  |
|   | <p><b>Priming and social desirability</b><br/>After logging in, the message appears briefly before opening the first page (summary).</p>  | <p>Appeal to higher loyalties</p>               |
|  | <p><b>Priming, warning (transaction consequences).</b><br/>The message appears briefly (roughly 1–3 s) to try to dissuade potential fraudulent actions on the website (prime). The message pops up when first trying to access the local navigation of the post-log design condition.<br/>The message itself warns that the account's transactions are being observed. This also helps reduce distance as the message directly addresses the (unauthorised) user.<br/>Chances of being caught/detected seem much higher as the message almost directly addresses the unauthorised user.</p>   | <p>No apparent link based on interview data</p> |
|  | <p><b>Warning (transaction consequences)</b><br/>The unauthorised user should think if they have recorded my details, they can probably track me down too. The message is displayed in the style (yellow background red text) of other warnings. The style of the warning is meant to make it stand out.<br/>A message appears briefly, then disappears again. It can reappear when the confirm button is hovered over.</p>   | <p>No apparent link based on interview data</p> |

Appendix C: Rationalizations with context-centric explanations and support

**Empirical support for rationalization-centric findings and alignment with Neutralization Theory (NT)**

| Rationalization                | Explanation within e-banking context  | Participant quotes  | Support for NT alignment  |
|--------------------------------|---|---|---|
| No Observers                   | As a central part of all three scenarios, and subsequently the hypothetical opportunity to commit fraud, was the assumption that the third party was alone near the computer. We thought this replicated a typical e-banking environment and could encourage fraud because of the lack of an observer. A witness could potentially help authorities and the negative impact of being labelled a thief is clearly distasteful. However, participant observations and responses were not often coded to belong to this rationalization. For this reason, it does not feature as a prominent rationalization within Fig. 1 but has been included for completeness together with two instances where a participant did bring up this line of thought. | <ul style="list-style-type: none"> <li>• “So, they’ve probably you know see if you know anyone’s around looking um, you know if there’s any cameras. Since I think if I can remember no one was around. He’d probably feel safe doing it since there was a computer there already and the credentials were already there, um, you know, I think he would feel like he would be safe in, you know, using this login information.”</li> <li>• “The first warnings that said that these transactions will be flagged. So, there’s a good possibility it would go through but that doesn’t, I don’t think that would stop it from trying. It either works or it doesn’t work. I don’t think the cameras in that coffee shop are gonna be that conclusive for any sort of investigation.”</li> </ul>   | The third party may argue that they were compelled to engage in the account takeover due to circumstances beyond their control. They might claim that the online environment provided an opportunity that was too tempting to resist. This was certainly what we were trying to convey within the scenarios we provided the participants. Based on the above, our scenarios, and the quote on the left, we aligned this rationalization with <i>Denial of Responsibility</i> . Based on the fact that the information was already there, and the participant is not responsible for the safety of the credentials.  |
| Crime of Opportunity           | All the scenarios presented participants with opportunities to commit e-banking fraud, but this may not have been perceived as such. A third party may decide to take advantage of certain opportunities based on their perceptions. To some extent this rationalization can be linked to the lack of observers, as public venues such as Internet cafés often have other people around. Having said that, they are unlikely to be fixated on a specific person. More than half of the participants brought this up as a rationalization making it one of the three most prominent rationalizations.  | <ul style="list-style-type: none"> <li>• “Well, curiosity, obviously theft, maybe you know, need what do you call it? Crime of opportunity? I suppose someone could just leave that open and continue with their own work.”</li> <li>• “There’s a crime of opportunity, some...they, they see an easy something that seems easy to use on this easy and simple. They might take advantage of that.”</li> <li>• “...I would be interested to see; you know how much. Did this person save this much money. What are the expenses? How did they spend the [eir] money? I Would be interested in that.”</li> </ul>   | When individuals commit a cybercrime as a crime of opportunity, they often rationalize their actions by claiming that they stumbled upon a vulnerable situation and were intrigued (even compelled) to take advantage of it due to the lack of security measures or the negligence of the account holder. In other words, they may argue that they had no responsibility for creating the opportunity; it was merely presented to them, and they were acting on an impulse or curiosity. Hence the alignment with <i>Denial of Responsibility</i> .   |
| Unlucky Personal Circumstances | A third party might use any recent misfortune or financial setback to justify committing fraud. In the provided scenario, this could be a car accident and subsequent repair costs that need to be covered. This suggests that third parties are in dire financial straits at the time and will be more likely to be tempted. The high number of occurrences of this fraud-enabling rationalisation suggests that third parties may prefer such a rationalisation to commit e-banking fraud.  | <ul style="list-style-type: none"> <li>• “Well, I would think well if this person was dumb enough to actually save their credentials in there then they deserve what, what they’re going to get, and hey I’m, you know maybe going through some financial struggles myself and so this is just an easy way to maybe buy something that I can’t afford to buy or something like that.”</li> <li>• “We’re doing the transaction. Well, probably because you may not feel like he’ll pay. Especially if it’s [an] expensive car bill I mean they’re never cheap. But probably would think it’s you know it’s one, might as well as one off. I will never have an opportunity to like [to] do this again, probably...I’ll probably never get a shot to like to do this again.”</li> <li>• “Well, there’s money there, you know. I mean people down on their luck. People with not so high of a moral compass. People, you know, opportunist[s]...”</li> </ul> | When individuals rationalize their involvement in a cybercrime like account takeover as a result of unlucky circumstances, they are essentially claiming that the circumstances led them to engage in the crime. They may argue that they found themselves in a once off situation where the opportunity presented itself, and they had little control over whether they would commit the crime or not. This rationalization is used to shift blame away from themselves and onto external factors (e.g., the expensive car bill). By portraying themselves as victims of circumstances, third parties may therefore attempt to shift the blame for their actions away from themselves and onto external factors. We therefore aligned this with <i>Denial of Victimization</i> in the sense that they do not acknowledge the gravity of the harm they may cause (e.g., to the account holders) and claim that they, too, were victims of unlucky personal circumstances. Theory suggests that such forms of rationalization enable third parties to distance themselves from the ethical and legal consequences of their actions. Sympathy may also play a role as they use their unlucky personal circumstances narrative to elicit leniency from others, including law enforcement, legal authorities, or society. |
| Dishonest Nature               | The idea of inherent nature dictates how people responded to similar scenarios where there was an opportunity to commit fraud. Some third parties may lean towards a more dishonest nature and subsequently have fewer qualms. Changing the behavior of such individuals would be much more difficult, which suggests that nudging may exert limited influence, as their focus would be on what they could gain from the opportunity. While the question of intrinsic nature did arise, few participants explicitly mentioned this.   | <ul style="list-style-type: none"> <li>• “You’re talking about people that I think are not concerned by warnings. They’re gonna do stuff anyway. It’s more in their nature and character to go as far as they can...”</li> </ul>  | Elements of human nature, such as our capacity for self-deception, rationalization, and the ability to adapt our moral beliefs to fit our actions, can potentially relate to multiple strategies. We argue that <i>Denial of Responsibility</i> and <i>Condemnation of the Condemners</i> is relevant if individuals argue that their dishonesty is a result of external pressures (as is sketched in the scenarios) or that those condemning them are hypocritical.  |
| Greed                          | It is conceivable that even when not in dire need, a third party may commit fraud simply due to their greedy nature. Such cases imply that an individual does not necessarily need a reason to justify stealing from someone else, despite any laws or adverse social norms. This can be linked   | <ul style="list-style-type: none"> <li>• “Personal need, greed. I’ll teach them...”</li> <li>• “Free money. So, it’s essentially an opportunity to enrich themselves.”</li> </ul>   | Participants who attribute their actions to greed may use this rationalization to criticize those who condemn them. They might argue that those who are quick to condemn them are hypocritical or morally judgmental, implying that they themselves are not immune to greed or unethical  |

(continued on next page)



(continued)

---

**Empirical support for rationalization-centric findings and alignment with Neutralization Theory (NT)**


---

|                        |   |   |   |
|------------------------|---|---|---|
|                        | <p>to the situational cue of financial incentives brought up by multiple studies (Gneezy et al., 2018; Gerlach et al., 2019). However, the size of the incentive itself did not seem to be a factor. While the fraud-enabling rationalisation itself is unsurprising, what was surprising was how rarely participants responses could be linked to this rationalizations.</p>   |   | <p>behavior in other aspects of their lives. Additionally, they might suggest that society, in general, is driven by various forms of self-interest, including financial gain, and that they are simply more honest about their motivations. greed can serve to relativize morality, implying that moral standards are arbitrary or flexible. Participants may argue that society often rewards financial success and that they are merely taking advantage of an opportunity to achieve financial gain, much like others in the business world. They might suggest that their actions are not outliers but rather a reflection of broader societal tendencies, making it more difficult for others to single them out for moral condemnation. As such we aligned this rationalization with <i>Condemnation of the Condemners</i>.</p> <p>Participants who downplay the severity of accessing an open account may use this rationalization to minimize the moral judgment of their actions. They might argue that those who condemn them are overly judgmental or harsh, implying that their actions are relatively benign compared to more serious crimes. Individuals may compare their actions to those of others, suggesting that their behavior is no worse than what they perceive as common or accepted practices. They might contend that many people engage in ethically questionable activities, and their actions are no different. This rationalization can serve to relativize ethical standards, implying that what is considered "bad" or "good" is subjective and open to interpretation. Participants may argue that different individuals or cultures have varying views on what constitutes unethical behavior. Participants may convince themselves that their actions are ethically acceptable because they perceive them as not causing significant harm to the victims. Based on the above motivations, we aligned this rationalization with both <i>Denial of Injury</i> and <i>Condemnation of Condemners</i>.</p> |
| Accessing Open Account | <p>The scenarios specifies that a third party would stumble upon someone else's e-banking credentials. This could be used as a potential rationalisation as there was no active breach or deliberate search for the account holder's credentials. This could be used to reduce any negative impact on their self-image, as they positively compared themselves to cybercriminals. To some extent, this was an example of the theory of self-concept maintenance described by Mazar et al. (2008), Ariely (2012), Gneezy et al. (2018), and Shalvi et al. (2015). Given how common this theory is in the literature, it was surprising that this rationalisation was only mentioned by two participants.</p>   | <ul style="list-style-type: none"> <li>• "Yeah, and like said it was already logged in, I think he might feel like he's not really, you know, breaking into this person's account because it was already locked [logged] into the account..."</li> <li>• "Since it was already logged in...I think he'll definitely be more inclined to, you know, use it and make a payment."</li> </ul> | <p>Participants who are overconfident in not being caught may rationalize their actions by minimizing the perceived harm caused by e-banking fraud. They might argue that since they believe they won't be caught, the harm inflicted on the victims is minimal or inconsequential. Additionally, overconfidence in avoiding detection can serve as a way to reduce feelings of guilt. Individuals might convince themselves that if they believe they can escape consequences, the victims won't suffer significant harm, and therefore, their actions are less morally objectionable. Participants may argue that because they are confident in their evasion of punishment, the victims won't experience substantial or lasting harm, thus justifying their actions. Hence its alignment with <i>Denial of Injury</i>.</p>   |
| Overconfidence         | <p>Our findings indicate that when participants believed their chances of evading detection was high, they may be unreasonably confident regarding their chances of escaping detection and thus decide to commit fraud. A similar bias was found in other studies for both nudging (Mongin and Cozic, 2014; Acquisti et al., 2017) and deterrence theory (Piquero et al., 2011). This was a relatively common fraud-enabling rationalization and was explicitly mentioned by several participants.</p>  | <ul style="list-style-type: none"> <li>• "Essentially yeah, I mean if you gonna be a thief and I'm dumb enough to go into a transaction on an Internet café. Probably not smart enough to realize that what's going on is going to be as easy as they think it is, and they just..., think they would sho[o]t straight to the end."</li> </ul>  | <p>As stated in these quotes, third parties may argue that since they have already invested significant time and effort into their behavior, the harm inflicted on the victims is justified or inconsequential. This makes the sunk cost fallacy a means to "cope" with or reduce feelings of guilt. Individuals may convince themselves that they must continue their fraudulent activities to recoup their supposed "losses" and that doing so won't lead to significant harm to the victims. Based on the above, we aligned this rationalization with <i>Denial of Injury</i>.</p>   |
| Sunk Cost Fallacy      | <p>A relatively common idea among the participants was that third parties would explore the website first before deciding on a course of action. A third party visiting the website may not immediately log out or attempt to transact or tamper with an account. This is not always motivated by malice or greed, and individuals may well log out without causing financial harm. Curiosity may lead to a sense of sunk cost fallacy. In such a case, they might as well go "all the way" and commit fraud, i.e., "I have already used someone else's credentials to log in, which is wrong, so I might as well also get some money". This is similar to the findings of Amigud and Lancaster (2019) and Gravert (2013), who found that prior effort exerted was often used to justify dishonest behavior. Across all three design conditions</p> | <ul style="list-style-type: none"> <li>• "They probably would have had second thoughts it looks like somebody's going to be able to track me and tag me, and maybe, I shouldn't have done this. But I'm this far, so I might as well..."</li> <li>• "Yeah like if you jump in the water. It's cold doesn't make a difference you're already in the water."</li> </ul>                     |   |

(continued on next page)

(continued)

---

**Empirical support for rationalization-centric findings and alignment with Neutralization Theory (NT)**


---

several participants' responses involved an element of sunk cost fallacy.

---

**References**

- Abdullah, A., Marican, S., 2016. The effects of big-five personality traits on deviant behavior. *Procedia-Soc. Behav. Sci.* 219, 19–25. <https://doi.org/10.1016/j.sbspro.2016.04.027>.
- Addo, K.O., 2023. An exploratory study of police corruption in Ghana: why does it exist? *Int. Criminol.* 3 (1), 52–62. <https://doi.org/10.1007/s43576-022-00078-7>.
- Aguiler, M. Here's why your bank account is less secure than your gmail. <https://gizmodo.com/heres-why-your-bank-account-is-less-secure-than-your-gm-1683777281> 2015. Accessed 14 March 2023.
- Ahmad, I., Iqbal, S., Jamil, S., Kamran, M., 2021. A systematic literature review of E-banking frauds: current scenario and security techniques. *Linguistica Antverpiensia* (2), 3509–3517.
- Alkassim, R.S., Tran, X., 2016. Comparison of convenience sampling and purposive sampling. *Am. J. Theor. Appl. Stat.* 5 (1), 1–4. <https://doi.org/10.11648/j.ajtas.20160501.11>.
- Alshaiikh, M., Maynard, S.B., Ahmad, A., 2021. Applying social marketing to evaluate current security education training and awareness programs in organisations. *Comp. Secur.* 100, 102090 <https://doi.org/10.1016/j.cose.2020.102090>.
- Alm, J., Burgstaller, L., Domi, A., März, A., Kasper, M., Nudges, 2023. Boosts, and sludge: using new behavioral approaches to improve tax compliance. *Economies* 11 (9), 223. <https://doi.org/10.3390/economies11090223>.
- Aravind, A., Mishra, S., Meservy, M., 2024. Nudging towards sustainable urban mobility: exploring behavioral interventions for promoting public transit. *Transpor. Res. Part D: Trans. Environ.* 129, 104130 <https://doi.org/10.1016/j.trd.2024.104130>.
- Banerjee, S., John, P., 2024. Nudge plus: incorporating reflection into behavioral public policy. *Behav. Public Policy* 8 (1), 69–84. <https://doi.org/10.1017/bpp.2021.6>.
- Belás, J., Korauš, M., Kombo, F., Korauš, A., 2016. Electronic banking security and customer satisfaction in commercial banks. *J. Secur. Sustainab. Issues* 5 (3), 411–422. [https://doi.org/10.9770/jssi.2016.5.3\(9\)](https://doi.org/10.9770/jssi.2016.5.3(9)).
- Bilz, A., Shepherd, L.A., Johnson, G., 2023. I Tainted Love: a systematic review of online romance fraud. *arXiv preprint arXiv:2303.00070*.
- Boddy, C.R., 2016. Sample size for qualitative research. *Qualit. Market Res.* 19 (4), 426–432. <https://doi.org/10.1108/QMR-06-2016-0053>.
- Boothroyd, V., Chiasson, S., 2013. Writing down your password: does it help?. In: 11th Annual Conference on Privacy, Security and Trust, PST 2013, pp. 267–274. <https://doi.org/10.1109/PST.2013.6596062>.
- Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. *Qualit. Res. Psych.* 3 (2), 77–101. <https://doi.org/10.1191/1478088706qp0630a>.
- Broers, V.J.V., De Breucker, C., Van Den Broucke, S., Luminet, O., 2017. A systematic review and meta-analysis of the effectiveness of nudging to increase fruit and vegetable choice. *Europ. J. Publ. Health* 27 (5), 912–920. <https://doi.org/10.1093/eurpub/ckx085>.
- Bryman, A., 2016. *Social Research Methods*. Oxford University Press.
- Castleman, B.L., Page, L.C., 2015. Summer nudging: can personalized text messages and peer mentor outreach increase college going among low-income high school graduates? *J. Econ. Behav. Organiz.* 115, 144–160. <https://doi.org/10.1016/j.jebo.2014.12.008>.
- Choe, E.K., Jung, J., Lee, B., Fisher, K., 2013. Nudging people away from privacy-invasive mobile apps through visual framing. *Lect. Notes Comp. Sci. (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 8119 LNCS (PART 3), 74–91. [https://doi.org/10.1007/978-3-642-40477-1\\_5](https://doi.org/10.1007/978-3-642-40477-1_5).
- Choubey, J., Choubey, B., 2013. Secure user authentication in internet banking: a qualitative survey. *Int. J. Innov., Manage. Technol.* 4 (2) <https://doi.org/10.7763/ijimt.2013.v4.391>.
- Claessens, J., Valentin, D., De Cock, D., Preneel, B., Vandewalle, J., 2002. On the security of today's online electronic banking systems. *Comp. Secur.* 21 (3), 253–265. [https://doi.org/10.1016/S0167-4048\(02\)00312-7](https://doi.org/10.1016/S0167-4048(02)00312-7).
- Colbert, Y., 2019. Why is this online banking security feature common in other countries, but not Canada? | CBC News. <https://www.cbc.ca/news/canada/nova-scotia/two-factor-verification-online-banking-security-1.5306052>. Accessed 14 March 2023.
- Collins English Dictionary. Third party definition and meaning. <https://www.collinsdictionary.com/dictionary/english/third-party> 2021.
- David Deng. 12 stats about banking fraud to make that impacts businesses. 2022. <https://entrepreneurshipfacts.com/12-stats-about-banking-fraud-to-make-that-impact-s-businesses/#8> Online banking accounted for 33 of US banks fraud costs in 2021 Accessed 14 March 2023.
- De Bruyn, S., Wouters, E., Ponnet, K., Tholen, R., Van Hal, G., 2023. Subtypes of prescription stimulant misuse among students: a nuanced story. *Stud. Higher Educ.* 1–15. <https://doi.org/10.1080/03075079.2023.2215272>.
- De Sutter, E., Borry, P., Geerts, D., Huys, I., 2021. Personalized and long-term electronic informed consent in clinical research: stakeholder views. *BMC Med. Ethics* 22, 1–12. <https://doi.org/10.1186/s12910-021-00675-7>.
- Despard, M., Roll, S., Grinstein-Weiss, M., Hardy, B., Oliphant, J., 2023. Can behavioral nudges and incentives help lower-income households build emergency savings with tax refunds? Evidence from field and survey experiments. *J. Consum. Affairs* 57 (1), 245–263. <https://doi.org/10.1111/joca.12498>.
- Edwards, M., Williams, E., Peersman, C., Rashid, A., 2022. Characterising cybercriminals: a review. *arXiv preprint arXiv:2202.07419*.
- Egelman, S., Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., 2011. Of passwords and people: measuring the effect of password-composition policies. In: *Proceedings of the SigCHI Conference on Human Factors in Computing Systems*, pp. 2595–2604. <https://doi.org/10.1145/1978942.1979321>.
- Fanghella, V., Ploner, M., Tavoni, M., 2021. Energy saving in a simulated environment: an online experiment of the interplay between nudges and financial incentives. *J. Behav. Exper. Econ* 93, 101709. <https://doi.org/10.1016/j.jsocec.2021.101709>.
- Florêncio, D., Herley, C., Oorschot, P., 2014a. An administrator's guide to internet password research this paper is included in the proceedings of the. In: *Proceedings of the 28th Large Installation System Administration Conference (LISA14)*, pp. 33–52. <https://www.usenix.org/conference/lisa14/conference-program/presentation/florencio>.
- Florêncio, D., Herley, C., Oorschot, P.C.Van, Oorschot, P.C.Van, 2014b. Password portfolios and the finite-effort user: sustainably managing large numbers of accounts. In: *Proceedings of the 23rd USENIX Security Symposium*.
- French, A.M., 2012. A case study on E-banking security. When security becomes too sophisticated for the user to access their information. *J. Inter. Bank. Commerce* 17 (2), 2–14.
- Gehring, E.F., 2002. Choosing passwords: security and human factors. *Int. Sympos. Technol. Soc.* January, 369–373. <https://doi.org/10.1109/istas.2002.1013839>.
- Groff Networks. Cyber-thieves exploit online banking weaknesses. <https://groffnetworks.com/cyber-thieves-exploit-online-banking-weaknesses/2023>. Accessed 11 September 2023.
- Hakimi, H., Joolae, S., Ashghali Farahani, M., Rodney, P., Ranjbar, H., 2020. Moral neutralization: nurses' evolution in unethical climate workplaces. *BMC Med. Eth.* 21, 1–10. <https://doi.org/10.1186/s12910-020-00558-3>.
- Hartl, V.M.I.A., Schmutzsch, U., 2016. Fraud protection for online banking: a user-centered approach on detecting typical double-dealings due to social engineering and inobservance whilst operating with personal login credentials. In: Tryfonas, T. (Ed.), *Proceedings 4th International Conference, HAS 2016, Held as Part of HCI International, Toronto, ON, Canada*. [https://doi.org/10.1007/978-3-319-39381-0\\_4](https://doi.org/10.1007/978-3-319-39381-0_4). July 17–22, 2016.
- Hartwig, K., Reuter, C., 2021. Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. *Behav. Inform. Technol.* 41 (7), 1357–1380. <https://doi.org/10.1080/0144929X.2021.1876167>.
- Hemphill, S.A., Kotevski, A., Tollit, M., Smith, R., Herrenkohl, T.I., Toumbourou, J.W., Catalano, R.F., 2012. Longitudinal predictors of cyber and traditional bullying perpetration in Australian secondary school students. *J. Adolescent Health* 51 (1), 59–65.
- Hillman, J. MTurk vs. qualtrics vs. Prolific: whose survey participants are best? [online] Available at: <https://www.prolific.co/blog/mturk-qualtrics-prolific-best-survey-p-articipants2022> [Accessed 18 Oct. 2022].
- Horowitz, M. Financial firms not offering two factor authentication | Computerworld. <https://www.computerworld.com/article/2476642/financial-firms-not-offering-two-factor-authentication.html> 2014. Accessed 14 March 2023.
- Inglesant, P.G., Sasse, M.A., 2010. The true cost of unusable password policies: password use in the wild. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Association for Computing Machinery*, pp. 383–392. <https://doi.org/10.1145/1753326.1753384>.
- Ioannou, A., Tussayadiah, I., Miller, G., Li, S., Weick, M., 2021. Privacy nudges for disclosure of personal information: a systematic literature review and meta-analysis. *PLoS One* 16 (8), e0256822. <https://doi.org/10.1371/journal.pone.0256822>.
- Jager, J., Putnick, D.L., Bornstein, M.H., 2017. More than just convenient: the scientific merits of homogeneous convenience samples. *Monogr. Soc. Res. Child Develop.* 82 (2), 13–30.
- Jeske, D., Coventry, L., Briggs, P., van Moorsel, A., 2014. Nudging whom how: nudging whom how: IT proficiency, impulse control and secure behavior. *Personal. Behav. Change Technol. CHI Workshop* 49 (18). [http://nrl.northumbria.ac.uk/17996/1/Jeske et al 2014 CHI Personalised Nudges.pdf](http://nrl.northumbria.ac.uk/17996/1/Jeske%20et%20al%202014%20CHI%20Personalised%20Nudges.pdf).
- Kenton, W. Triple bottom line (TBL) definition. <https://www.investopedia.com/terms/t/triple-bottom-line.asp> 2020 Accessed 14 March 2023.
- Kowalski, R.M., Giumentti, G.W., Feinn, R.S., 2022. Is cyberbullying an extension of traditional bullying or a unique phenomenon? A longitudinal investigation among college students. *Int. J. Bully. Preven.* 1–18.
- KPMG. The multi-faceted threat of fraud: are banks up to the challenge? <https://kpmg.com/xx/en/home/insights/2019/05/the-multi-faceted-threat-of-fraud-are-banks-up-to-the-challenge-fs.html> 2019 Accessed 11 September 2023.

- KrebsSecurity. Report: big U.S. banks are stiffing account takeover victims 2022. Accessed 11 September 2023 <https://krebsonsecurity.com/2022/10/report-big-u-s-banks-are-stiffing-account-takeover-victims/>.
- Kroese, F.M., Machiori, D.R., de Ridder, D.T.D., 2015. Nudging healthy food choices—a field experiment at the train station. *J. Public Health* 38 (2), e133–e137. <https://doi.org/10.1093/pubmed/fdv096>.
- Kuhfuss, L., Préget, R., Thoyer, S., Hanley, N., 2016. Nudging farmers to enrol land into agri-environmental schemes: the role of a collective bonus. *Europ. Rev. Agricul. Econom.* 43 (4), 609–636. <https://doi.org/10.1093/erae/jbv031>.
- Lee, M.C., 2009. Understanding the behavioral intention to play online games: an extension of the theory of planned behavior. *Online Inform. Rev.* 33 (5), 849–872. <https://doi.org/10.1108/14684520911001873>.
- Maruna, S., Copes, H., 2005. What have we learned from five decades of neutralization research? *Crime Justice* 32, 221–320. <https://doi.org/10.1086/655355>.
- Mason, R. and Farah, H. Electoral commission apologises for security breach involving UK voters' data. <https://www.theguardian.com/technology/2023/aug/08/uk-electoral-commission-registers-targeted-by-hostile-hackers> 2023.
- Matza, D., 2018. *Delinquency and Drift*. Routledge.
- McLeod, S. The interview research method | simply psychology. <https://www.simplypsychology.org/interviews.html> 2014.
- Melissa Sanchez. Why you should never write down your passwords - whiteOut press. <https://www.whiteoutpress.com/why-you-should-never-write-down-your-password-s/> 2019, March 15.
- Newman, G., Clarke, R.V., 2016. *Rational Choice and Situational Crime prevention: Theoretical foundations*. Routledge.
- Nilsson, M., Adams, A., Herd, S., 2005. Building security and trust in online banking. In: *Proceedings Conference on Human Factors in Computing Systems*, pp. 1701–1704. <https://doi.org/10.1145/1056808.1057001>.
- Olimpi, E.M., Baur, P., Echeverri, A., Gonthier, D., Karp, D.S., Kremen, C., Sciligo, A., De Master, K.T., 2019. Evolving food safety pressures in California's Central Coast Region. *Front. Sustain. Food Syst.* 3, 102. <https://doi.org/10.3389/fsufs.2019.00102>.
- Omariba, Z.B., Masee, N.B., Wanyembi, G., 2012. Security and privacy of electronic banking. *Int. J. Comp. Sci. Issues* 9 (4), 432–446.
- Pabian, S., Vandebosch, H., 2016. Short-term longitudinal relationships between adolescents' (cyber) bullying perpetration and bonding to school and teachers. *Int. J. Behav. Develop.* 40 (2), 162–172.
- Patton, M.Q., 2014. *Qualitative research & evaluation methods: integrating theory and practice*. Sage.
- Pawson, R., 2013. *The Science of evaluation: A realist Manifesto*. Sage.
- Pilcher, J. Infographic: the history of internet banking (1983 - 2012). <https://thefinancialbrand.com/25380/yodlee-history-of-internet-banking/2020>. Accessed 14 March 2023.
- Renaud, K., Zimmermann, V., Maguire, J., Draper, S., 2017. Lessons learned from evaluating eight password nudges in the wild. *LASER Workshop - Learn. Authorit. Secur. Experim. Results*.
- Renz, E., Müller, M.M., Böhm, K.L., 2023. When nudges promote neutral behavior: an experimental study of managerial decisions under risk and uncertainty. *J. Busin. Econom.* 93 (8), 1309–1354.
- Rubin, H.J., Rubin, I.S., 2011. *Qualitative interviewing: the art of hearing data*. Sage.
- Ruggeri, K.A.I., Benzerga, A., Verra, S., Folke, T., 2023. *A Behavioral Approach to Personalizing Public Health, 7. Behavioural Public Policy*, pp. 457–469.
- Sakala, L.C., Chigona, W., 2020. How lecturers neutralize resistance to the implementation of learning management systems in higher education. *J. Comput. Higher Educ.* 32 (2), 365–388. <https://doi.org/10.1007/s12528-019-09238-7>.
- Sarreal, R. History of online banking: how internet banking went Mainstream | GOBankingRates. Available online: <https://www.gobankingrates.com/banking/banks/history-online-banking/2019>.
- Saunders, M., Lewis, P., Thornhill, A., 2016. *Research Methods for Business Students, 7th ed.* Pearson Education Limited.
- Shah, S., Shah, B., Amin, A., Al-Obeidat, F., Chow, F., Moreira, F.J.L., Anwar, S., 2019. Compromised user credentials detection in a digital enterprise using behavioral analytics. *Fut. Gener. Comp. Syst.* 93, 407–417. <https://doi.org/10.1016/j.future.2018.09.064>.
- Siponen, M., Puhakainen, P., Vance, A., 2020. Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Comp. Secur.* 88, 101617.
- South African banking risk information centre. *Ann. Crime Stats*, 2019. <https://www.sabric.co.za/2020>.
- Statista. Number of active online banking users worldwide in 2020 with forecasts from 2021 to 2024, by region. <https://www.statista.com/statistics/1228757/online-banking-users-worldwide/2023> Accessed 11 September 2023.
- Statista. Share of population using digital banking in the United States from 2018 to 2022. <https://www.statista.com/statistics/946109/digital-banking-users-usa/2022>. Accessed 11 September 2023.
- Stobert, E., 2014. The agony of passwords: can we learn from user coping strategies? CHI '14 Extended Abstr. *Human Factors in Comp. Syst.* 975–980. <https://doi.org/10.1145/2559206.2579421>.
- Stobert, E., Biddle, R., 2014. The password life cycle: user behavior in managing passwords. In: *SOUPS '14: Proceedings of the Tenth Symposium on Usable Privacy and Security*, pp. 243–255.
- Sykes, G.M., Matza, D., 2017. *Techniques of neutralization: a theory of delinquency. In: Delinquency and Drift Revisited*, 21. Routledge, pp. 33–41.
- Syniavskaya, O., Dekhtyar, N., Deyneka, O., Zhukova, T., Syniavskaya, O., 2019. Security of e-banking systems: modeling the process of counteracting fraud in e-banking. In: *SHS Web of Conferences*, p. 65.
- Tambe Ebot, A.C., Siponen, M., Topalli, V., 2023. Towards a cybercontextual transmission model for online scamming. *Europ. J. Inform. Syst.* 1–26. <https://doi.org/10.1080/0960085X.2023.2210772>.
- Thaler, R.H., Sunstein, C.R., 2008. *Nudge: Improving Decisions About Health, Wealth and Happiness*. Yale University Press.
- Toubba, K. Security incident update and recommended actions. <https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/2023>.
- Turland, J., Coventry, L., Jeske, D., Briggs, P., van Moorsel, A., 2015. Nudging towards security: developing an application for wireless network selection for android phones. In: *British HCI '15: Proceedings of the 2015 British HCI Conference*, pp. 193–201. <https://doi.org/10.1145/2783446.2783588>.
- Wang, D., Davis, R., 2023. The impact of behavioral nudges on consumer choice and decision-making processes. *Res. Stud. Busin.* 1 (01), 109–118.
- Yazdanifard, R., Wanyusoff, W.F., Behora, A.C., Sade, A.B., 2011. Electronic banking fraud; the need to enhance security and customer trust in online banking. *Adv. Infor. Sci. Service Sci.* 3 (10), 505–509. <https://doi.org/10.4156/AISS.vol3.issue10.61>.
- You, S., Lim, S.A., 2016. Longitudinal predictors of cyberbullying perpetration: evidence from Korean middle school students. *Personal. Individ. Differ.* 89, 172–176.
- Zeke Franco. Choice architecture: introduction to designing for decision making | by Zeke Franco | medium. <https://medium.com/@Zekefranco/choice-architecture-introduction-to-designing-for-decision-making-3c2fd32c32> 2018 Accessed 14 March 2023.
- Zelle Report. Facilitating fraud: how consumers defrauded on Zelle are left high and dry by the banks that created it. <https://www.warren.senate.gov/imo/media/doc/ZELLE20REPORT20OCTOBER2022.pdf> 2022 Accessed 11 September 2023.
- Zhang, B., Xu, H., 2016. Privacy nudges for mobile applications: effects on the creepiness emotion and privacy attitudes. In: *Proceedings of the ACM Conference on Computer Supported Cooperative Work*, 27. CSCW, pp. 1676–1690. <https://doi.org/10.1145/2818048.2820073>.