European Journal of Information Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tjis20

Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling

Ersin Dincelli & InduShobha Chengalur-Smith

To cite this article: Ersin Dincelli & InduShobha Chengalur-Smith (2020) Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling, European Journal of Information Systems, 29:6, 669-687, DOI: 10.1080/0960085X.2020.1797546

To link to this article: https://doi.org/10.1080/0960085X.2020.1797546

EUROPEAN JOURNAL OF INFORMATION SYSTEMS
2020, VOL. 29, NO. 6, 669–687
https://doi.org/10.1080/0960085X.2020.1797546

THE OPERATIONAL RESEARCH SOCIETY
Taylor & Francis
Taylor & Francis Group

EMPIRICAL RESEARCH

Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling

Ersin Dincelli [a] and InduShobha Chengalur-Smith [b]

[a]Information Systems, University of Colorado Denver, Denver, CO, United States; [b]Information Systems & Business Analytics, University at Albany, Albany, NY, United States

ABSTRACT

Online self-disclosure (OSD) on social networking sites can leave individuals and organisations vulnerable to security threats. Following a design science research (DSR) method, we created a gamified, "choose your own adventure" style security education, training, and awareness (SETA) artefact using two formats: text and visual. Both artefacts were designed to identify the security threats that trainees are most susceptible to, debrief them about the threat and its potential consequences, and facilitate behaviour change by letting trainees re-evaluate their decisions. Using a longitudinal randomised controlled experiment, we compared these two artefacts to no intervention and traditional security warning emails by assessing both instrumental (changes in attitudes, intentions, and OSD behaviour) and experiential (memorability and user experience) outcomes. Our survey of 1,718 employees showed that the text-based artefact was better at improving instrumental outcomes, and the visual-based artefact was better at improving experiential outcomes. This study provides a more granular understanding of the linkages between technology artefacts and human experiences through the application of design science thinking. The findings contribute to DSR by developing design principles, testable propositions, and realistic performance evaluation metrics for gamified SETA artefacts, and present practical recommendations for regulating employees' information security and privacy behaviours inside and outside the workplace.

ARTICLE HISTORY
Received 8 March 2019
Accepted 14 July 2020

SPECIAL ISSUE EDITORS
Paul Benjamin Lowry, Stacie Petter and Jan Marco Leimeister

KEYWORDS
Gamification; security education; training; awareness; SETA; online self-disclosure; design science; design artefact; storytelling

1. Introduction

Social networking sites (SNS) are increasingly blurring the lines between personal and business networks as they enable companies to interact with consumers and government agencies to distribute information and provide services (DePaula et al., 2018). This, combined with the growing trend for employees to use their personal devices for work, and be social media friends with their co-workers, increases the potential for social engineering attacks (Acquisti et al., 2015). While the awareness of social engineering attacks over email has increased, people are less aware of the potential for social engineering attacks through SNS (Krombholz et al., 2015).

SNS are one of the most challenging avenues of information leakage for organisations due to their pervasive use and features that promote information disclosure (Cavusoglu et al., 2016). Employees' intentional or unintentional disclosure about their organisations makes them targets for highly contextualised social engineering attacks, such as targeted malware, spear phishing, vishing, and advanced persistent threats. These attacks are complicated, difficult to detect, and could result in the theft of intellectual property or confidential information, cyber industrial espionage, and sabotage of corporate networks (Vishwanath, 2015). Thus, online self-disclosure (OSD) is a pervasive and risky behaviour that can pose severe consequences and opportunities to compromise information related to both individual privacy and organisational security (Chen & Sharma, 2015).

Reconnaissance and information gathering are the first activities hackers conduct for almost any type of attack. Attackers can *passively* gather information about a target from multiple sources, including SNS, search engines, forums, and archived websites, and use it to *actively* collect information through social engineering techniques and interactions with the target or other key individuals on SNS (Garba et al., 2018). Organisations cannot entirely stop reconnaissance or employees from disclosing information (Cole, 2012), however, educating employees about the negative consequences of information disclosure can limit the sensitive information they publicly share (Spitzner, 2019) and increase the difficulty of reconnaissance efforts, thus decreasing the likelihood of an attack.

Organisations use various information security interventions, such as security education, training, and awareness (SETA) programmes and security policies, to mitigate security risks. However, most of the

CONTACT Ersin Dincelli ersin.dincelli@ucdenver.edu
The supplemental online Appendix for this article can be accessed here.

existing information security interventions are standardised and provided uniformly, which means they are designed as one-size-fits-all (D'Arcy & Hovav, 2009). Gamified systems provide a new method to design tailored programmes that not only educate users but also motivate them to learn and be engaged in tasks that they would otherwise consider tedious or difficult (Hanus & Fox, 2015). However, the efficacy of gamified SETA interventions in the context of OSD through SNS is not guaranteed for the following reasons.

Firstly, gamification has been effective in increasing engagement, changing behaviours, and learning new problem-solving skills in a variety of fields (Osatuyi et al., 2018), but not all applications are successful (Liu et al., 2017) and adding gamification concepts to IS has not always resulted in positive outcomes or behaviour changes (Hamari, 2013). Thus, IS researchers have recommended using a design science approach to develop gamified systems, combined with longitudinal and controlled experimental methods (Crossler et al., 2013) that evaluate realistic outcomes (Schöbel et al., 2020). Our investigation follows these recommendations and applies design science principles to explore the efficacy of various gamified SETA interventions in the context of OSD.

Secondly, although gamification has been successfully used to motivate users to comply with information security policies (Silic & Lowry, 2020), information security is not sufficient to safeguard information privacy (Ackerman, 2004). Traditional SETA programmes are narrowly focused on technical issues and not contextualised (D'Arcy & Hovav, 2009). Information privacy is distinct from information security (Smith et al., 2011). Information privacy preferences and OSD behaviour are malleable, and context-dependent (Acquisti et al., 2015), and privacy decisions vary extensively across individuals (Anaraky et al., 2020). Thus, our investigation applies a contextualised and participatory storytelling approach as one of the primary gamification elements of the SETA artefact. Specifically, we apply a "choose your own adventure" (CYOA) style training that allows us to identify the security threat(s) that trainees are most susceptible to, based on the type of information and the circumstances under which they are prone to disclose online, and focus the training to the relevant context.

Thirdly, one of the few studies to apply gamification to data privacy training found evidence that the gamification approach increased participants' awareness about their own data privacy, but found no evidence that gamification improved learning relative to non-gamified approaches (Baxter et al., 2016). Thus, gamified SETA interventions have the potential to improve privacy, but the appropriate mix of game design elements that can lead to success has not been established. To investigate this further, we explore a combination of various design formats for our contextualised CYOA-style, gamified SETA artefact and evaluate their impact on reducing OSD and influencing the antecedents of OSD (i.e., attitudes and intentions towards OSD).

We contribute to design science knowledge by developing design principles, testable propositions, and realistic performance evaluation metrics (Rothe et al., 2020) in the context of information security and privacy. We also contribute to the literature on SETA by addressing threat, protection and vulnerability artefacts (Lowry et al., 2017) through the development and testing of gamified SETA interventions. Specifically, we propose using CYOA-style interactive storytelling, to improve engagement and ultimately regulate employees' information security and privacy behaviours inside and outside of the workplace.

The rest of the paper is structured as follows. We begin by examining the literature on OSD, SETA programmes, and gamification. Next, we develop hypotheses about the proposed interventions using the gamified SETA artefact and follow by describing the design science research (DSR) process we used to develop the gamified SETA artefact. We then present our evaluative measures and explicate the longitudinal randomised controlled experimental design and data collection procedures used in the study. We proceed to present the results and discuss their implications. Finally, we present the limitations of the study and conclude the paper.

2. Literature review

2.1. Online self-disclosure

OSD is the disclosure of individuals' personal information to others via the Internet for either economic benefits or social support (Shih et al., 2017). Social influence has a greater impact on self-disclosure than perceived benefits in SNS (Cheung et al., 2015), suggesting that self-disclosure is reciprocal, or a learned behaviour from other users (Chen & Sharma, 2015). SNS facilitate disclosure by allowing a wide range of information to be disclosed in various forms, such as pictures, videos, and geographic locations. Personal information can also be shared by individuals' network connections using features such as "tagging" and "sharing." Group pictures that are shared on SNS are examples of "co-owned" information that could pose a risk to all those in the photo (James et al., 2017). Once the information is disclosed online, it is stored in the servers belonging to service providers and possibly third parties for unknown durations even if the disclosers delete their information from their profile. This becomes a collective privacy management issue (Jia & Xu, 2016), and individuals may lose control over who can access their personal information.

SNS encourage users to overshare through the design of their services that exploit human biases.

For example, data transactions, such as free quizzes and surveys, are structured so that the benefits of disclosure are immediate and attractive (e.g., fun), whereas the costs are vague and in the future (John, 2018). Advertisements on SNS often resemble non-commercial posts, and social and commercial transactions can be blurred (e.g., the social payments app, Venmo). Some technologies also provide an illusion of control that reduces inhibitions towards self-disclosure, by sharing information through disappearing messages (e.g., Snapchat) or with a select audience (e.g., Facebook) (Hofstetter et al., 2017). Similarly, many SNS apps have default settings that automatically share personal information, such as locations and contacts, and make it difficult to opt out.

The privacy paradox is the phenomenon where consumers express concerns about privacy, but behave contrarily by disclosing private information, perhaps for convenience (Dinev, 2014). Users' confidence about their ability to control disclosed information increases as they become habituated to using SNS (Gwebu et al., 2014), which results in increased susceptibility to social engineering attacks (Vishwanath, 2015). SNS features, such as privacy settings and policies, enhance users' feelings of being in control, and reduce their perceived privacy risk (Krasnova et al., 2010). However, SNS users often underestimate the size and scope of their audience (Bernstein et al., 2013). Additionally, the privacy settings are often complicated (Johnson et al., 2012), resulting in privacy risks of self-disclosure being underestimated and the social benefits of self-disclosure being overestimated (Brandimarte et al., 2013).

Additionally, security fatigue results in individuals getting desensitised to security threats and becoming lax about maintaining security (Furnell & Thomson, 2009). It also leads to cognitive biases in decision making where people believe that they are not at risk or that no security measure they put in place will actually make a difference (Stanton et al., 2016). People get overwhelmed by the need to be constantly on the alert and choose the easiest available option, make decisions driven by immediate motivations, or behave impulsively (Stanton et al., 2016). An alternative explanation is provided by the vicious cycle of privacy erosion, which suggests that when personal information becomes public through data breaches, people value their privacy less, making them more comfortable with sharing information (John, 2018).

People may be aware that their information is being monetised, either for commercial or political purposes, however, the market power of these "essential" online services leaves consumers with little choice (Ghosh & Scott, 2018). Since the Cambridge Analytica data breach, almost three quarters of Facebook users either adjusted their privacy settings, took a break from the platform for several weeks, or deleted the app from their cell phones (Perrin, 2018). However, many of these users returned to using Facebook as they were resigned to the fact that they have little or no control over how their information is used and lacked feasible options (Guynn, 2018). Additionally, given that users often derive social status or enhanced social identity through OSD behaviour, they may feel ambivalent about reducing OSD.

Although seeking to eliminate OSD is not realistic, there is evidence that users care about protecting their privacy (Wisniewski et al., 2016) and aspire to mitigate security risks by limiting OSD, despite the pressures described above. A study of SNS users showed that over time they increased the information shared with friends in their network while simultaneously decreasing what was shared with strangers (Stutzman et al., 2012). Thus, raising awareness about the potential negative consequences of OSD along with training to limit OSD can help in changing attitudes and intentions towards OSD and reducing OSD behavior in SNS.

2.2. Attitudes and intentions towards OSD behaviour

Behaviour is a complex construct as various factors affect one's behaviour simultaneously, such as past experience, current context, and other specific stimuli (Dennis & Minas, 2018). This complexity is heightened in the case of OSD (Acquisti et al., 2015) as users rely on technical (e.g., privacy controls and settings), behavioural (e.g., self-censorship) and mental (e.g., reciprocity of trusting others) strategies to manage their privacy on SNS (Cavusoglu et al., 2016). A meta-analysis of attitude-behaviour research found a strong relationship between attitude and behaviour across varying contexts (Kim & Hunter, 1993). Researchers consider attitude as a multidimensional construct, consisting of three components: *behavioural, cognitive*, and *affective* attitude (Rosenberg, 1960).

The strongest predictor of behaviour is intention, as it captures the motivational factors that influence behaviour (Ajzen & Fishbein, 1980). Most theorists agree that the effect of attitude on behaviour is mediated by intention (Kim & Hunter, 1993). Intention is a particularly accurate predictor of behaviour when the behaviour is volitional and involves a choice among available alternatives, e.g., having an abortion or voting choice (Ajzen, 1991). Although online self-disclosure seems volitional, it can also be an unintended action performed unknowingly (e.g. when information is co-owned (James et al., 2017)) or on an impulse. Thus, intentions play an important role but are not sufficient to predict OSD behaviour.

Emotions, biases, and heuristics can affect privacy behaviour differently than privacy attitudes (Acquisti

et al., 2015). For instance, perceived inconvenience and behavioural inertia could prohibit people from adopting privacy protection behaviours (Crossler & Posey, 2017). People who care deeply about privacy, in general, may still choose to self-disclose after taking costs, benefits, and social norms into account (Acquisti et al., 2015). An additional wrinkle is that SNS users who are trying to reduce their OSD are often at the mercy of others in their network, who may continue to tag them in their online posts, location-based check-ins, and photos (James et al., 2017). Thus, existing interventions may fail due to the strength of social media habits, calling for interventions that interrupt habitual patterns of reactions by reframing users' perceptions (Vishwanath, 2015). This leads us to our research goal, which is to design and evaluate a gamified SETA artefact to reduce OSD and change attitudes and intentions towards OSD.

2.3. SETA programmes and gamification

To increase the effectiveness of SETA programmes, Karjalainen and Siponen (2011) recommend using transformation-oriented training that is directed towards changing attitudes and behaviour by connecting with the learners' experiences and allowing the learning to occur by evaluating the new knowledge they have gained and its personal relevance (Sheng et al., 2007). Gamification can be used as part of a transformation-oriented training as it heightens user experiences and allows learners to self-reflect (Osatuyi et al., 2018). Game-based learning is a technique that integrates games into instructional content by incorporating the characteristics of computer games to engage users and positively influence learning outcomes (Hamari & Nousiainen, 2015).

There are a plethora of game elements and techniques that are used for gamification, including game design principles, game dynamics, player journey, and storytelling (Kankanhalli et al., 2012). Liu et al. (2017) created a taxonomy of game elements with two broad categories: *gamification objects* and *mechanics*. Gamification objects can be used to create sensory experiences (e.g., images), cognitive experiences (e.g., narratives), or just be functional (Liu et al., 2017). Game mechanics, on the other hand, are the rules that govern the interactions between users and game objects (Teh et al., 2013). The characteristics of the context and needs of the users determine the appropriate subset of game design elements that should be applied (Schöbel et al., 2020).

Learning science research has established that games are one of the most effective learning methods and can be highly motivational if they follow certain design principles (Quinn, 2005). One such design principle, *story-based agent*, advocates for the use of agents (cartoon-like or real-life characters) as part of the story-based content to help to guide users through the learning process (Sheng et al., 2007). Many people learn about security problems and solutions by hearing warnings and stories from other people (Das et al., 2014). The use of storytelling in security gamification can stimulate curiosity and challenge users (Kapp, 2012). Exposing people to ideas about computer security through games or stories improves their understanding of the diversity of potential security threats and makes it more likely that they will invest the time and effort required for desirable security and privacy behaviours (Denning et al., 2013).

3. Hypothesis development

3.1. Gamified SETA artefact: interactive storytelling

Interactive storytelling can provide a mechanism for users to experience security threats in various contexts and learn the importance of reducing OSD. When storytelling is integrated into a gamified training, it creates an opportunity for learners to find relevance between the context and their personal experience, which is also an essential feature of transformation-oriented training (Karjalainen & Siponen, 2011). For instance, participants in a cyber-threat education programme who were provided with real-life details had improved security outcomes, relative to participants who were provided with more generic training (McCrohan et al., 2010). Thus, storytelling can help users develop strong connections to the training material, and the stories become a springboard for action (Woodside, 2010) and cause profound changes in behaviour (Drew et al., 2010). Embedding interactivity within the storylines can result in experiential narratives (Ralph & Monu, 2015) that stimulate a hedonic, game-like experience and can change the user's behaviour towards the desired outcome (Kankanhalli et al., 2012). Interactive storytelling that enables learners to make their own decisions that alter the course of the storyline and create dynamic narratives, such as CYOA-style stories, can also improve learning (Gaeta et al., 2014).

Another learning design principle, *reflection*, advocates that games should provide opportunities for the users to stop and think, i.e., reflect on the new knowledge they have gained (Sheng et al., 2007). In the context of learning, it is particularly crucial that gamification focuses on providing feedback about the user's learning progress (Cheong et al., 2014), performance, and competence (Deci & Ryan, 2000). Teaching information security is more effective in an interactive, game-like context that provides rich, unambiguous feedback (Silic & Lowry, 2020). Providing choices and informational, unambiguous feedback increases participants' sense of autonomy and rewards their competence while

promoting engagement (Silic & Lowry, 2020). Participatory storytelling approaches, such as CYOA-style stories, allow learners to become active participants who can use the feedback provided through the training for self-evaluation and ultimately change their attitudes and behaviours (Karjalainen & Siponen, 2011). Thus, we propose the following hypothesis:

H1: A gamified SETA artefact using CYOA-style interactive storytelling will be effective in (a) changing attitudes, (b) changing intentions, and (c) reducing OSD.

Interactive storytelling can also compel users to be more engaged in the training, resulting in improved memorability and positive user experiences. SETA programmes are often perceived to be boring and lack user interaction and involvement; therefore, employees usually do not pay attention to the training materials (Yoo et al., 2018). Stories can be used to encode technical knowledge as they combine events, facts, and experiences within the context of specific situations, making the information more accessible and memorable (Hayne, 2009). Game mechanics that encompass role-plays and storylines can improve learning outcomes by increasing motivation, interest, relatedness, and autonomy (Frost et al., 2015). The use of storytelling in security gamification can also stimulate curiosity and challenge users (Kapp, 2012). Stories can enhance the ability to remember and recall detailed information as individuals internalise and identify with a story (Hayne, 2009), resulting in more memorable learning outcomes (Mandler & Johnson, 1977).

User perceptions of interactivity result in increased training satisfaction (Lowry et al., 2009). Training satisfaction has been noted as an important determinant of training outcomes (Johnson et al., 2008). SETA programmes that allow users to control the pace and sequence of learning, and provide feedback, result in improved cognitive outcomes such as training performance and retention, as well as improved affective outcomes such as trainee satisfaction and self-efficacy (Abraham & Chengalur-Smith, 2019). The underlying goals of gamification are to engage users to learn, change their attitudes, and motivate desired behaviours through enjoyable user experiences (Treiblmaier et al., 2018). Thus, we hypothesise:

H2: A gamified SETA artefact using CYOA-style interactive storytelling will improve (a) memorability and (b) user experiences.

3.2. Gamified SETA artefact: text vs. visual

SETA programmes using interactive storytelling can be enhanced by using visual media, such as graphics and illustrations. Information provided through visual media is more vivid and elicits more information from memory (Thorpe et al., 1996). Textual content is stored in our short-term memory, whereas visual content goes into our long-term memory, where information is stored over an extended period of time (Burmark, 2002). The human brain processes visual information much faster (Hyerle, 2000) and more effectively (Thorpe et al., 1996) than text. Thus, visual content can lead to better comprehension and retention of the information compared to textual storytelling (Dincelli & Chengalur-Smith, 2019). Moreover, when combined with salient stimuli, it can heighten emotions and feelings, which, in turn, intensifies both cognitive and behavioural responses (Fiske & Taylor, 1984).

Media richness is the medium's capacity to process rich information. It is characterised by a multiplicity of cues (textual, verbal, visual, etc.), the immediacy of feedback, personalisation of focus (messages tailored to the current situation of the receiver), and variety in the language (Daft & Lengel, 1986). Findings from studies that investigated media richness in the training context have been mixed. A comparison of various teaching styles found that visual and participatory presentations were more effective for both short-term and long-term recall, relative to text presentations (Dale, 1969). In the security context, SETA programmes using comics or video games were found to be more effective than using plain text on webpages (Kumaraguru et al., 2007) in decreasing phishing susceptibility (Mayhorn & Nyeste, 2012).

On the other hand, when researchers compared the effectiveness of disseminating content by watching a video story to reading the script of the video, they found that the script was the most useful method for comprehension, most likely, due to its low cognitive load (Mirkovski et al., 2019). Similarly, training using rich media can be problematic for SETA programmes, particularly when the content requires high cognitive attention (Jenkins et al., 2012). A recent comparison of the benefits of communicating privacy policies using comics as opposed to text found that although comics resulted in slightly more accurate understanding, they also resulted in lower self-efficacy (Anaraky et al., 2019).

Other studies comparing security training based on different levels of media richness have also found that using rich media was less effective than using leaner media due to cognitive overload when information is provided using multiple channels (Shaw et al., 2009). There can be various reasons for these unexpected findings. For example, training videos may have narrators with distracting voices or attire or contain special effects that may be overstimulating. In such cases, using leaner media, such as a narrated slide presentation, become more effective (Jenkins et al., 2012). Nevertheless, there appears to be some consensus in the recent literature that visual cues improve memorability and user experience (Liu et al., 2017; Mayhorn

& Nyeste, 2012), while detracting from performance due to cognitive overload (Jenkins et al., 2012; Mirkovski et al., 2019). Thus, we hypothesise:

H3: CYOA-style interactive, *visual-based* storytelling will be less effective than CYOA-style interactive, *text-based* storytelling in (a) changing attitudes, (b) changing intentions, and (c) reducing OSD.

H4: CYOA-style interactive, *visual-based* storytelling will be more effective than CYOA-style interactive, *text-based* storytelling in improving (a) memorability and (b) user experiences.

4. Method: building the SETA artefact

Our DSR goals are to generate prescriptive knowledge (Gregor & Hevner, 2013), by establishing design principles for a gamified SETA artefact that can reduce OSD (Avdiji et al., 2020). In order to generate these design principles, we developed testable propositions (Gregor & Jones, 2007) – hypotheses – about what the gamified SETA artefact should enable users to do and how it should be built in order to do so. Next, we construct an innovative SETA artefact as a proof-of-concept and explore its utility as a solution in the context of reducing OSD (Iivari, 2015). We designed an objective-centred solution (Peffers et al., 2007) and relied on rigourous methods in the construction of this artefact by reviewing the gamification literature and learning about features that may work well in our context. Accordingly, we established suitable scope and boundaries and developed a prototype (Hevner et al., 2004) of a gamified SETA artefact with CYOA-style interactive storytelling.

4.1. Design of a gamified SETA artefact

Hevner et al. (2004)'s DSR guidelines provided a structured path in using DSR methodology in designing the gamified SETA artefact. Table A1 in Appendix A (see online supplement) presents an overview of the general process we followed. Figure 1 presents the research activities that we followed in designing the gamified SETA artefact. We developed a SETA artefact for reducing OSD by applying the two learning design principles described earlier, *story-based agent* and *reflection*, as well as relevant requirements for IS security training proposed by Karjalainen and Siponen (2011). For the gamification aspects, we relied on Helms et al. (2015)'s taxonomy of game elements as well as Liu et al. (2017)'s general principles for designing gamified systems.

We relied on the literature to surface the most relevant game elements for a SETA artefact, keeping in mind Liu et al. (2017)'s recommendation that game design elements should be chosen to create the desired user-system interactions and experiential and instrumental outcomes. The overarching goal of the training was to reduce OSD by alerting SNS users to the pitfalls of sharing information online. Other instrumental outcomes were changes in the antecedents of OSD behaviour, viz. attitudes, and intentions towards OSD. By considering both short- and long-term changes, these instrumental outcomes test the efficacy and effectiveness of the gamified SETA artefact (Checkland & Poulter, 2010).

In addition, we considered two experiential outcomes to evaluate our gamified SETA artefact: memorability and user experience. Most information that we learn, especially factual information, is forgotten after a short period of time (Lujan & DiCarlo, 2006), which makes retention of acquired knowledge an important topic in learning. Elegance (Checkland & Poulter, 2010) is another experiential outcome that assesses the ease of use and understanding of the artefact. Assessing user experience using reliable and valid measures is an essential step for designing and evaluating a gamified SETA artefact since user experience is an important indicator of the overall success of

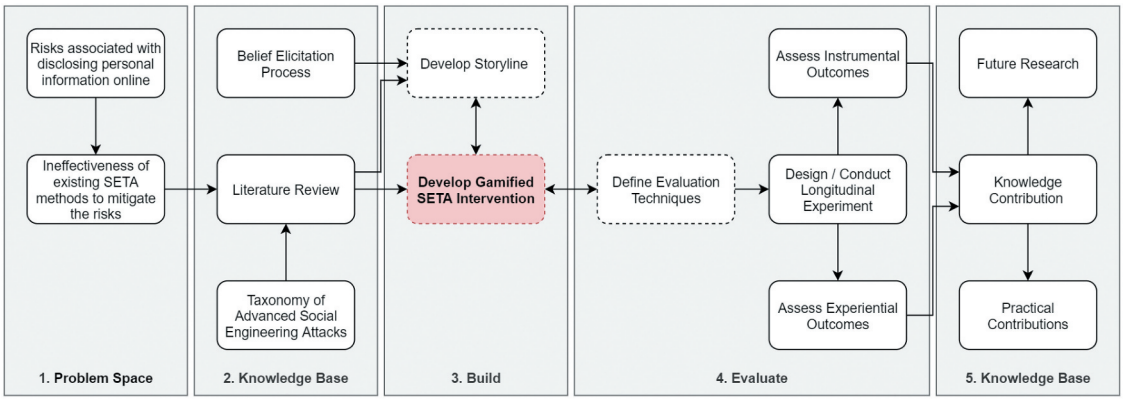

Figure 1. Design science research process for a gamified SETA artefact (Adapted from Tremblay et al. (2010) and Gregor and Hevner (2013). *The dashed boxes indicate the iterative design processes.*

any new system (Zviran & Erlich, 2003). Therefore, we aimed to create a gamified SETA artefact that would be memorable, easy to use, and result in high user satisfaction and usability.

Helms et al. (2015) identified seven categories of game elements: progression, rewards, rules, social, competition, communication, and general. We believed that progression should be an element of the gamified training, as the intrinsic motivation to progress in a story that is part of a training programme can add to the extrinsic motivation to complete the training (Pivec et al., 2004). Communication increases motivation as users can see the impact of their actions as they interact with the training material (Prensky, 2005). Therefore, we included both aspects of communication: feedback and interaction. We included rules to limit the actions of users and keep the training manageable (Kapp, 2012). Table A2 in Appendix A maps the game design elements to those used in our training.

4.2. Choose your own training adventure

Recall that our goal was to create a gamified SETA artefact that reduced OSD by contextualising the training to the participant's OSD proclivities. Thus, the gamified SETA artefact used interactive storytelling to (1) determine the security threat(s) that each participant was most susceptible to, (2) debrief the participant about each threat and its potential causes, and (3) facilitate behaviour change by letting him or her re-evaluate the decision that led to the threat. In order to achieve these three objectives, we developed a CYOA-style interactive storyline that allowed participants to explore hypothetical scenarios, make decisions about OSD in various contexts, and experience how their OSD behaviour would affect individual and organisational privacy and security.

In creating the storyline, we balanced several goals: covering essential privacy and security concepts, creating reasonably realistic scenarios, mapping game mechanics, and maintaining comprehensibility and brevity. In order to improve the relevance, validity, and generalisability of the storyline (Benbasat & Weber, 1996), we followed two approaches to generate content: a belief elicitation process (Limayem & Hirt, 2003), and a review of the literature and news articles on information security and privacy threats. Appendix B (see online supplement) presents the details of the process of generating content for the storyline.

We identified five common types of threats based on our synthesis of the literature and news articles, and the unstructured data acquired through the belief elicitation process. They were: (1) phishing, (2) spear phishing, (3) burglary, (4) password cracking, and (5) identity theft. Although users may be aware of such threats, they can still fall victim to them. Therefore, we chose these security threats to be included in the storyline.

Researchers have found that stories about negative events related to security are the most influential (Redmiles et al., 2016). Therefore, we designed our storyline to reflect the five security threats we identified as *consequences*. We recognised the social context for such scenarios by explicitly taking into account potential interactions among individuals and groups on SNS (De Leoz & Petter, 2018). Reducing OSD can have limitations due to the possibility of others in one's social network disclosing on one's behalf (James et al., 2017). To address this, we incorporated a social sub-artefact that addressed problems of third-party disclosure (De Leoz & Petter, 2018). Thus, rather than restricting the scenarios to cases where the story-based agent made decisions about OSD, we also included situations where the agent had to make decisions about permitting her friends to disclose about the focal agent online. By depicting scenarios that participants could imagine experiencing in reality, the stories offered a streamlined, surrogate experience (Sole & Wilson, 2002).

The storyline included various *decision points* where participants could alter the course of events throughout the scenario. Therefore, the participants could complete the interactive storyline following several different sequences based on their decisions. Additionally, participants' decisions shaped how the story would end. By identifying a consequence based on the participant's decision, we were able to debrief the participant on a particular security threat by providing a consequence-specific *debriefing*. After the debriefing, we took the participant to the decision point where she made a misjudgement and asked her to re-evaluate the previous decision she made. This self-re-evaluation process reinforced the feedback the participant had received in the debriefing to facilitate positive behaviour change. The storyline also included *background* information to improve the flow of the story and add context and relevance.

After outlining the complete story, we followed an iterative and incremental design process for developing the storyline in two main phases: developing the script for the text-based storyline and developing a visual-based storyline.

First, a script was drafted by the researchers for the text-based storyline. The script outlined all the elements (decision points, consequences, background information, characters, relationships, interactions, etc.) of the storyline. The storyline followed a three-act structure, a model used in narrative fiction that divides a storyline into three parts: *setup, confrontation*, and *resolution* (Brütsch, 2015). Act one (setup) introduced the protagonist, the main characters, the environment, and the main events. Act two (confrontation) involved the main events that led to the consequence that we had identified. In this act, we determined how the protagonist could experience or

avoid the consequence. Act three (resolution) involved the details of the debriefings following the consequence. The script went through multiple revisions and once the storyline was finalised, it was pilot tested several times to ensure it was realistic and followed a consistent logic. Figure C1 in Appendix C (see online supplement) presents the storyline logic.

Second, the text-based storyline was turned into comic scenes. A professional comic artist was hired to draw the scenes for the visual-based storyline. The visual-based storyline was finalised after multiple revisions. Both text- and visual-based storylines were pilot tested multiple times to ensure they were highly similar in terms of the three-act structure. Figure 2 presents the protagonist of the story, Jamie, and some of the scenario characters.

The final storyline consisted of five background scenes, 13 decision points (providing 41 different decision options), eight consequence scenes, and five debriefing scenes. Figure D2 in Appendix D (see online supplement) presents two decision points in the visual-based storyline. Figures D3-D8 show some of the consequence and debriefing scenes, and re-evaluation messages. For the complete visual-based storyline, we direct the readers to the following website: www.seta.games/cyoa

5. Evaluation: comparing and assessing outcomes

We compared text- and visual-based storytelling interventions to a control group that received no intervention and another group that received a set of traditional security emails warning them about OSD in an organisational context. The emails mimicked a situation where an organisation experienced a security breach due to one of its employees' disclosure of personal information online and subsequent spear phishing attacks. The messages were crafted based on typical security-related emails sent out periodically by organisations. The emails alerted employees about the breach, highlighted the security-related changes made by the organisation, provided recommendations for reducing the disclosure of personal information, improving password security and privacy settings to protect against identity theft and phishing. Thus, the email intervention contained the same essential content (i.e., the scenarios) as the gamified SETA artefact. The email messages were also presented in the same sequence as the three-act structure used in the interactive storyline. In addition, the threat consequences outlined in the email messages reflect those in the storytelling interventions. Table E1 in Appendix E (see online supplement) shows the security warning emails that we used in the email intervention.

5.1. Measures for assessing outcomes

A gamified system should result in meaningful engagement with both instrumental and experiential outcomes (Liu et al., 2017). Our overall proof-of-value of the gamified SETA artefact is demonstrated by the following performance criteria (Avdiji et al., 2020): efficacy (the intervention produces the intended outcomes), effectiveness (it can be

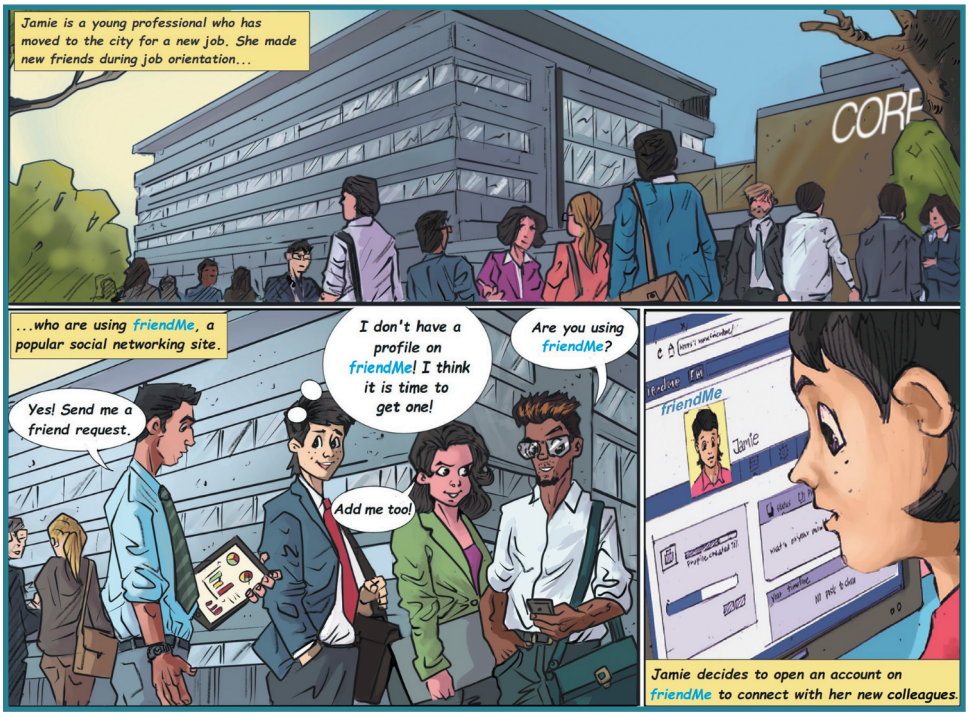

Figure 2. A background scene showing the protagonist, Jamie, during a job orientation.

successfully used to achieve higher-level or longer-term goals), efficiency (its use does not require an inappropriate amount of time or other resources), and elegance (the intervention is easy to use and understand) (Checkland & Poulter, 2010). In order to provide evidence of the rigour of our research, we needed to establish the instrumental outcomes, i.e., the efficacy of the gamified SETA artefact as well as its longer-term effectiveness in changing attitudes and intentions and reducing OSD behaviour (Venable et al., 2016). We also evaluated experiential outcomes of efficiency and elegance using memorability and user experience measures.

In order to minimise potential response bias, we used a combination of survey items and hypothetical scenarios, also known as vignettes (Weber, 1992), to assess attitudes and intentions. To measure OSD, we calculated a composite index (Petter et al., 2007) based on the availability of different types of information, weighted by the associated privacy settings on users' Facebook profiles. Although self-reported, these questions were relatively objective as the type of information and the privacy settings affiliated with them were pre-determined by Facebook and adjusted by the users. Appendix F (see online supplement) describes the process we followed to develop the measures for instrumental outcomes. Tables F1-F3 present the vignettes and survey questions for attitudes and intentions, the different types of information and the levels of privacy settings used to create the composite index for OSD, respectively.

We evaluated the experiential outcomes (efficiency and elegance) of the gamified SETA interventions using two measures: memorability and user experience. We used three measures of memorability: *recall* (retrieving information that is not currently present), *recognition* (determining whether information has been learned before) (Haist et al., 1992), and *reintegration* (restructuring a complete memory based on partial cues) (Baddeley, 2007). One month after the participants took our interventions, we asked them a series of questions to measure the memorability of each intervention. Table G1 in Appendix G (see online supplement) shows the recall, recognition, and reintegration questions.

To get a more holistic view of the overall user experience of the gamified SETA artefact, we adapted three commonly used user experience metrics to the context of our study. Specifically, we measured *satisfaction* (how satisfied users were after using the system), *usability* (to what extent the system was useful for users to achieve their goals), and *ease of learning* (whether using the system required effort to complete the training and the ease of understanding of the training material). Table G3 in Appendix G shows the satisfaction, usability, and ease of learning questions that we used to assess user experience. Appendix G presents the details of the process behind choosing and implementing our experiential measures.

Although the measurement items were adapted from previously validated instruments, we used an expert panel to test the face validity of the instruments. To establish proof-of-value of our design artefact, we conducted a series of pilot tests of the gamified SETA artefact and used the results to iteratively refine it. The final pilot data achieved excellent reliability, convergent, and discriminant validity results in all constructs. In addition, we pilot tested the entire longitudinal experiment, including all three interventions.

5.2. Longitudinal experiment design and data collection

In order to examine the potential causation between the study stimuli (gamified SETA and email interventions) and the subsequent changes in participants' attitudes, intentions, and OSD behaviour, we conducted a longitudinal randomised controlled experiment. During the first data collection period (t_1), participants were directed to the questionnaire consisting of the study constructs and demographic questions. T_1 was the baseline for the instrumental outcomes.

Data for this longitudinal experiment were collected on Amazon Mechanical Turk (mTurk), a crowdsourcing Internet marketplace that is widely used by researchers to recruit participants for online surveys and experiments (Paolacci & Chandler, 2014). MTurk was selected as the recruitment pool as a large sample could be collected in a short period of time. This is especially important for longitudinal security- and privacy-related experiments to avoid potential external causes of related behaviour change, such as the possibility of a major security breach happening during the experiment or potential security training the participants could have undergone.

MTurk has been used by researchers for various purposes and has been shown to be a reliable source for high-quality and representative datasets (Buhrmester et al., 2011). There have also been concerns associated with the use of mTurk in academic research (Peer et al., 2017). To overcome these concerns, rigourous data collection and cleaning procedures were followed, as explained in Appendix H (see online supplement). After the data cleaning processes, 1,718 employees were included in the experiment. The average age of the participants was 38.27 years. 55.5% of the participants were female, 42.3% of them male, and 0.4% of them identified as other gender.

To measure OSD behaviour as accurately as possible, we used two types of measures. The first was the OSD composite index described in section 5.1. Second, with the permission of the Institutional Review Board (IRB), we collected data on actual OSD by asking participants to provide us with the URL of their Facebook profile at

the beginning of the study (t_1), prior to the interventions. In total, 458 participants provided their Facebook profiles (26.66% of all the study participants). We calculated an actual OSD score based on the publicly visible content on participants' Facebook profiles using a self-disclosure coding scheme similar to Li et al. (2015). We identified 35 different information fields that could be made publicly available on Facebook and analysed each profile by coding the fields based on whether the participant made the information publicly available for each information field. The actual OSD score was calculated as the sum of the information made publicly available for each profile. We found that the actual OSD score was positively correlated with our composite OSD index ($r = 0.421$, $p < 0.01$). Although de-identifying the dataset to preserve the privacy of our participants (as required by IRB) did not allow us to collect further data on actual OSD after the interventions, this significant correlation shows that the composite index for OSD can be used as a surrogate for actual OSD behaviour in our study.

A month later (t_2), 1,718 employees were invited to the second part of the experiment. Participants were randomly assigned to either the control (no intervention), email, text-based, or visual-based storytelling groups at t_2. Participants who were in the control group were directed to the questionnaire consisting of the measurements for the instrumental outcomes without receiving any intervention. Participants in the email, text-based and visual-based groups were first directed to the email, text-based, and visual-based storytelling interventions, respectively. Subsequently, all three intervention groups were directed to the questionnaire consisting of the measurements for the instrumental outcomes and user experience. User experience metrics were measured at t_2, right after the participants received the interventions so that they would provide more accurate evaluations of the intervention they had received.

In order to avoid potential recency and demand effects (Zizzo, 2010) when measuring the memorability of each intervention and the stickiness of the results, we measured memorability and the instrumental outcomes a month later (t_3). We collected data for the instrumental outcomes at t_1, t_2, and t_3 to examine both the short- and long-term effects of the interventions. Table 1 summarises the times at which each measurement was taken during the experiment. Table 2 presents the number of participants for each group at each stage of the experiment.

Table 1. Measurement timeline for the longitudinal experiment.

Measurements	t_1	t_2	t_3
Attitude	x	x	x
Intention	x	x	x
OSD (Actual Score)	x		
OSD (Composite Index)	x	x	x
Memorability			x
User Experience		x	
Treatment Check		x	
Instructional Manipulation Check	x	x	x

Table 2. Number of participants in the longitudinal study at t_1, t_2, and t_3.

Experiment Group	t_1	t_2	t_3
Control	428	294	212
Email	430	287	211
Text	430	303	206
Visual	430	308	209
Total	1,718	1,192	838

6. Data analysis and results

We first established the psychometric properties of the measurement scales used in the study. Scale reliabilities were measured using *Cronbach's alpha* (α), and scale validities were measured using *convergent* and *discriminant* validities. The factor loadings of each measurement item were above 0.60 on their hypothesised constructs, and the average variance extracted (AVEs) values were greater than 0.80 across all constructs. These results show that the measurement items had strong convergent validity (Gefen & Straub, 2005). We examined the cross-loadings of each measurement item for discriminant validity. All the items loaded at least 0.10 higher on their respective factors than other factors (Gefen & Straub, 2005). Additionally, all the inter-construct correlations were less than the square root of the AVEs of each construct. These results demonstrate that the measurement items also had strong discriminant validity (Fornell & Larcker, 1981). The Cronbach's α for all the constructs were greater than 0.70, providing a satisfactory level of reliability (Field, 2013). Factor loadings, Cronbach's α, and inter-construct correlations with square roots of AVEs for each construct can be seen in Tables I1 to I4 in Appendix I (see online supplement).

6.1. Evaluating the gamified SETA interventions

1,718 participants were randomly assigned to either the control (no intervention), email, text-based, or visual-based storytelling groups. A one-way ANOVA was first conducted to ensure that the randomisation was effective. As shown in Table J1 in Appendix J (see online supplement), there were no significant differences ($p > 0.05$) in study constructs among the four groups before the experiment, establishing that the randomisation was successful.

6.1.1. Evaluating instrumental outcomes

In order to avoid potential recency and demand effects (Zizzo, 2010), we evaluated our instrumental outcomes in both the *short-term* (t_2-t_1) and *long-term* (t_3-t_1).

Short-term Results (t_2-t_1): Immediately following the intervention, 1,192 participants completed the second survey at t_2. To test for significant differences in the instrumental outcomes among the four groups, we conducted a series of one-way ANOVA tests. The dependent variable was the change in each outcome, which was calculated by subtracting the average score of each construct in t_1 from t_2. As shown in Table J2 in Appendix J, other than affective attitude (AAFF), there were significant differences in changes in online self-disclosure (OSD composite index), intention to disclose (INT), behavioural attitude (ABEH), and cognitive attitude (ACOG). This means that the email, text-based, and visual-based interventions were effective in changing OSD, INT, ABEH, and ACOG in the short term, but not AAFF.

Table 3 summarises the results of the post hoc analysis by first comparing the relevant short-term instrumental outcomes of the three interventions to the control and then comparing the short-term instrumental outcomes of the gamified interventions to the email intervention.

Both gamified SETA interventions were significantly better than the control group in terms of reducing OSD, and the text-based intervention achieved slightly better results compared to the visual-based intervention in the short term. However, their impact on OSD was not significantly different from that of the email intervention. Both gamified SETA interventions were significantly better than both the control and email groups in terms of their impact on changing INT. Finally, both gamified interventions were significantly better than the control for changing ABEH and ACOG but performed better than the email intervention only in terms of changing ABEH.

Long-term Results (t_3-t_1): We collected data one month after the interventions to examine their long-term effects on the instrumental outcomes. 838 participants completed the third survey. The dependent variable was calculated by subtracting the average score of each construct in t_1 from t_3. As shown in Table J3 in Appendix J, like the short-term results, there were significant differences in changes in OSD, INT, and ABEH. However, the changes in ACOG and AAFF were not significant. Table 4 summarises the results of the post hoc analyses.

Table 3. Post hoc analysis of the short-term effects.

Constructs (changes in)	Better than control	Better than email
OSD	Text*** Visual**	*No significant difference*
INT	Text*** Visual*** Email***	Text*** Visual***
ABEH	Text*** Visual***	Text*** Visual***
ACOG	Text* Visual*	*No significant difference*

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$.

Table 4. Post-hoc analysis of the long-term effects.

Constructs (changes in)	Better than control	Better than email
OSD	Text*** Visual**	Text*
INT	Text*** Visual***	Text*** Visual***
ABEH	Text*** Visual*** Email*	Text* Visual*

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$.

The long-term results demonstrate the continuing impact of the gamified SETA interventions a month later. Like the short-term results, long-term results show that both gamified SETA interventions were significantly better than the control group, with the text-based intervention slightly outperforming the visual-based intervention in terms of reducing OSD. In addition, the text-based intervention was an improvement over email for reducing OSD in the long-term. Again, both gamified SETA interventions outdid the control and email groups in terms of their long-term influence on changing INT and ABEH.

6.1.2. Evaluating experiential outcomes

We conducted a series of one-way ANOVA tests to examine if there were significant differences in memorability and user experiences among the three interventions. As shown in Table J4 in Appendix J, there were significant differences in all the measures of memorability and user experience across the three interventions. Table 5 summarises the results of the post hoc analyses.

The results show that the visual-based intervention was more memorable than the email intervention on two measures (recall and redintegration) and more memorable than the text-based intervention on two measures (recognition and redintegration). Participants were significantly more satisfied with the training provided by the visual-based intervention relative to the email intervention but seemed to be equally satisfied with the visual- and text-based interventions. The training provided using the visual- and text-based interventions were consistently rated higher than that of the email intervention in terms of usability. Finally, users found the training with the visual-based intervention to be significantly easier to learn than that with the text-based intervention.

Table 5. Post hoc analysis of the experiential outcomes.

Experiential Outcomes	Better than email	Better than text
Recall	Visual*	*No significant difference*
Recognition	*No significant difference*	Visual***
Redintegration	Visual**	Visual***
Satisfaction	Visual***	*No significant difference*
Usability	Visual*** Text***	*No significant difference*
Ease of Learning	*No significant difference*	Visual***

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$.

6.1.3. Summary of the results

Given the complexity of our study and its measures, we summarise the results of our analyses for the instrumental and experiential outcomes for both the short- and long-term in Table 6. We show these results in the context of the hypothesis tests by aligning the results with the hypotheses that they pertain to. We explain our findings further in the Discussion section.

7. Discussion

Reducing OSD is a "wicked problem" (Buchanan, 1992) – one that is hard to define and has no true-or-false solution – and is exactly the kind of complex socio-technical problem that DSR can address (Gregor & Hevner, 2013). The primary goal of the CYOA-style gamified SETA artefact was to reduce OSD. We created two versions of the gamified SETA artefact (text-based and visual-based) that allowed participants to hypothetically experience how their OSD behaviour could expose themselves and others to various security threats. We compared them to a control group that received no intervention and another group that received traditional security warning emails about OSD.

We found that both gamified SETA interventions achieved this goal, but the email intervention worked equally well in the short-term. In the long-term, however, only the text-based intervention continued to influence users a month later. Thus, the text-based intervention had a greater and longer-lasting impact than the visual-based intervention. This finding is consistent with the prior research on communicating privacy policies using comics (Anaraky et al., 2019) and training programmes using rich media, which were found to be less effective due to cognitive overload when the information was provided using multiple channels (Jenkins et al., 2012; Shaw et al., 2009).

We also aimed to change intentions and attitudes towards OSD with the gamified SETA interventions. Both gamified SETA interventions were equally good and more effective than the email intervention in changing intentions in both the short- and long-term. The extent of personal information that participants intended to disclose was reduced following both gamified SETA interventions, indicating their success in instigating a negative shift in users' intentions towards OSD. As intention is an important predictor of behaviour, this bodes well for such gamified SETA interventions, particularly when organisations cannot readily target employees' behaviours.

The impact of the gamified SETA interventions on changing attitudes, however, was mixed. Behavioural attitude was the only attitudinal component that was amenable to change in both the short- and long-term, with both gamified SETA interventions outperforming the email intervention. Both the gamified SETA interventions had a short-term impact on changing cognitive attitude, but their impact did not exceed that of the email intervention. Finally, affective attitude was completely resistant to change.

Recall that cognitive attitude measured beliefs about OSD, and affective attitude reflected the emotional responses evoked by OSD. Beliefs and emotions may be more hard-wired into individual psyches and, therefore, more difficult to change (Rokeach, 1968). Behavioural attitude is the tendency towards a particular behaviour, and we measured it as the likelihood that a SNS user would permit someone else to disclose about them online. A reduction in behavioural attitude may reflect the fact that it is easier to control other users' online disclosure about oneself, relative to changing one's own beliefs and emotions about OSD. Regardless, inducing a change in behavioural attitude is important for the following reason. Although the collective privacy management of co-owned information can be contentious, when explicitly requested by others, people tend to respond by complying with the request (Anaraky et al., 2020). Thus, discouraging their peers from sharing information about them online can be an effective strategy in limiting the information about them that is available online and thus decreasing privacy risks (James et al., 2017).

We also evaluated our gamified interventions on experiential outcomes, i.e., memorability and user experience. We assessed memorability using three measures: recall (retrieving information without any cues), recognition (determining whether information has been learned before), and redintegration (restructuring a complete memory based on partial cues). As expected, the text-based intervention suffered in comparison to the visual-based intervention with respect to memorability. The visual-based intervention improved recall and redintegration relative to the email intervention but was not significantly better at prompting recognition.

Note that redintegration is particularly relevant for SETA programmes as most of the common security and privacy threats come with cues that users can recognise. For example, phishing emails often come from an email domain that the target user is not familiar with, include suspicious attachments and visual cues, such as misspellings and poorly written messages (Goel et al., 2017). Such cues remind users about potential security issues and alert them without having them think about their security or privacy actively (Puhakainen & Siponen, 2010). This makes redintegration an important aspect of memorability in the context of SETA, and it can be enhanced by incorporating visual cues in SETA programmes to improve the memorability of the training content.

We assessed three measures of user experience (satisfaction, usability, and ease of learning). Users found the content of all three interventions equally

Table 6. Summary results of the analyses and hypothesis tests.

Hypotheses			Conclusion	Support
H1: A gamified SETA artefact using CYOA-style interactive storytelling will be effective in	(a) changing attitudes	*Behavioural*	Visual and text are better than email and control in the short- and long-term	Supported
		Cognitive	Visual and text are better than control in the short-term only	Partially supported
		Affective	No significant differences in the short- or long-term	Not supported
	(b) changing intentions		Visual and text are better than email and control in the short- and long-term	Supported
	(c) reducing OSD		Visual and text are better than control in the short- and long-term, and text is better than email in the long-term	Supported
H2: A gamified SETA artefact using CYOA-style interactive storytelling will improve	(a) memorability	*Recall*	Visual is better than email	Supported
		Recognition	No significant differences	Not supported
		Redintegration	Visual is better than email	Supported
	(b) user experiences	*Satisfaction*	Visual is better than email	Supported
		Usability	Visual and text are better than email	Supported
		Ease of Learning	No significant differences	Not supported
H3: Visual-based storytelling will be less effective than text-based storytelling in	(a) changing attitudes	*Behavioural*	Visual and text are equally good	Not supported
		Cognitive	Visual and text are equally good in the short term	Not supported
		Affective	Visual and text are no different	Not supported
	(b) changing intentions		Visual and text are equally good	Not supported
	(c) reducing OSD		Text is better than visual in the short- and long-term	Supported
H4: Visual-based storytelling will be more effective than text-based storytelling in improving	(a) memorability	*Recall*	Visual and text are no different	Not supported
		Recognition	Visual is better than text	Supported
		Redintegration	Visual is better than text	Supported
	(b) user experiences	*Satisfaction*	Visual and text are no different	Not supported
		Usability	Visual and text are no different	Not supported
		Ease of Learning	Visual is better than text	Supported

easy to learn. However, they rated both gamified SETA interventions more usable than the email intervention and were most satisfied with the visual-based intervention. Although a format that is universally optimal for all outcomes remains elusive, the gamified SETA intervention with visual-based, interactive storytelling had the best experiential outcomes, overall. Given that many SETA interventions are not effective due to low engagement and narrow technical focus (D'Arcy & Hovav, 2009), delivering interventions using visuals can make people more engaged with the SETA programme and less likely to skim the materials.

The visual-based intervention was more vivid and enjoyable to watch due to its richness in visual cues; however, this might have resulted in distracting the participants from the message itself and nullifying the effect of pictorial cues. Our study shows that SETA interventions should also consider potential cognitive load that may result in inefficiencies. Our overall findings suggest that providing immediate and contextualised feedback, rather than providing additional visual cues, should be emphasised in SETA interventions to change the behaviour in question effectively. Thus, the interactivity of the intervention is more important than whether it was text- or visual-based when the primary goal is behaviour change. This finding is particularly important for the design of SETA interventions as text-based interventions would be less resource intensive and more affordable, which is critical for businesses that have limited resources for educating their employees to mitigate security threats.

7.1. Limitations of the study and future research

Despite our efforts at rigour, our study has several limitations that present opportunities for future research. First, the study sample drew from employees within the United States. Previous studies (e.g., Posey et al. (2010) and Lowry et al. (2011)) showed that different societies might exhibit distinct behavioural patterns in the context of online self-disclosure. Therefore, the results of our study may not be generalisable outside of the United States population. Future studies can examine the effects of similar gamified SETA artefacts in different cultures.

Second, the effect of the visual-based intervention was not more effective than the text-based intervention. Although this finding was consistent with the previous research, visual-based interventions might still be more effective for particular populations, such as young adults (Liang & Xue, 2010), senior citizens (Carpenter & Buday, 2007), or gamers (Baxter et al., 2016). These populations are disproportionately more likely to fall prey to social engineering scams for the following reasons. Senior citizens are often the most susceptible targets of online financial scams as they are less tech-savvy, less knowledgeable about online threats, and more trusting than younger individuals when it comes to revealing personal information. Younger individuals and gamers, on the other hand, are more likely to be online and confident in their ability to protect themselves as compared to older adults (Miltgen & Peyrat-Guillard, 2014). Thus, they are more likely to fall victim to threats, such as identity theft. A gamified SETA artefact might be a better alternative for such vulnerable populations, which future research can investigate.

Third, while the text-based intervention performed better overall at instrumental outcomes, the visual-based intervention performed better overall at experiential outcomes. Future studies can test different versions of a gamified SETA artefact that combines the strengths of both text- and visual-based interventions. One example of such an intervention is *text comics*, which is a type of comic in which the narrative is delivered in captions below the illustrations instead of speech bubbles. Text comics might be more effective than both text- and visual-based presentation methods as the emphasis can be placed on the text while removing the potentially distracting visual cues (e.g., speech bubbles) from the intervention.

Fourth, artificial intelligence (AI) -supported scenario building tools are used for risk management in security and finance (Sohrabi et al., 2018). Organisations can leverage AI and machine learning (ML) techniques to better structure storylines that are tailored to their employers' behavioural patterns and computer logs. For example, employers that use simpler passwords or leave their workstation without locking their computers can be identified by an AI designed to capture employee behaviour and presented with contextualised scenarios that are designed by the AI. Such AI and ML supported scenarios can learn from the targeted learner's actual behaviour and improve the efficiency of gamified SETA.

Finally, in some instances, we found that the salutary effects of the gamified interventions dissipated over the course of a month. Security training is often conducted annually, and sometimes biannually, but our results suggest that even a six-month period may be too long for individuals to retain the effects of a SETA programme. Another avenue for future research would be to investigate the frequency at which training should be provided to maintain its benefits.

8. Conclusion

This study focuses on reducing online self-disclosure, as it can expose both individuals and organisations to various potential security and privacy threats (Chen & Sharma, 2015). We drew on the SETA and gamification literature and followed an iterative design process to create a gamified SETA artefact using interactive

storytelling. We contribute to design science research through the novelty of our artefact and by establishing the utility of our interventions at reducing OSD and changing attitudes and intentions (March & Storey, 2008). Our gamified SETA intervention is an improvement (Gregor & Hevner, 2013), as it is an innovative solution to the problem of OSD that is more effective than current solutions, as evidenced by the instrumental outcomes mentioned above as well as the experiential outcomes we evaluated viz., memorability and user experience. Thus, our research generated prescriptive knowledge by establishing design principles that were material and action-oriented (Avdiji et al., 2020; Chandra et al., 2015).

Methodologically, our study responded to calls for using DSR in gamification research (Schöbel et al., 2020) and applying longitudinal, randomised controlled experiments in SETA research (Lowry et al., 2017). Thus, we could empirically establish that the interventions we developed were an improvement. Additionally, in order to better understand the decision-making process for OSD our study went beyond the intentions construct and triangulated data about intentions with actual and self-reported behaviours (Lowry et al., 2017). Our hypotheses served as testable propositions (Gregor & Jones, 2007) about our interventions and their effects, and along with the results of our evaluation metrics, they added to the knowledge contributions of our research (Rothe et al., 2020; Venable et al., 2016).

Although this study focuses on online self-disclosure, we believe that understanding the mechanism of behaviour change can provide insights for identifying key determinants of behaviour change for other security behaviours, such as security and privacy policy compliance, use of protective information technologies, and stronger passwords.

Practically, our study provides empirical evidence to support the importance of gamified interventions in the context of information security. Additionally, it provides guidelines for the design and implementation of gamified SETA interventions for the promotion of better security behaviours. Implementing such interventions not only helps to mitigate security incidents but also helps organisations to allocate their resources more efficiently. Contextualised interventions, comprising gamified components such as the ones described in this study, also have the potential to reduce the time that employees spend on SETA programmes. Thus, our study meets the needs of business and society, addresses rigour and relevance, and is novel and interesting (Gregor & Hevner, 2013; Rothe et al., 2020).

Acknowledgments

We are grateful for the research funding provided by the Office of Research Services at the University of Colorado Denver to support this study. We appreciate the feedback we received on portions of this work from Izak Benbasat and H. Raghav Rao at the International Conference on Information Systems Doctoral Consortium (2018) and Anthony Vance, Ryan Wright, Jason Thatcher, and Monica Tremblay at the pre-AMCIS MIS Quarterly Author Development Workshop (2019). We are also grateful for the constructive feedback provided by Dawn Gregg, Alper Yayla, and Xin Zhou. Finally, we greatly appreciate the development and support we received from the senior editor, Paul Benjamin Lowry, and the work of the anonymous review team, in significantly improving this paper.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Ersin Dincelli http://orcid.org/0000-0002-8773-4714
InduShobha Chengalur-Smith http://orcid.org/0000-0002-5327-0915

References

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers & Security*, *87*, 101586. https://doi.org/10.1016/j.cose.2019.101586

Ackerman, M. S. (2004). Privacy in pervasive environments: Next generation labeling protocols. *Personal and Ubiquitous Computing*, *8*(6), 430–439. https://doi.org/10.1007/s00779-004-0305-8

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Prentice-Hall.

Anaraky, R. G., Cherry, D., Jarrell, M., & Knijnenburg, B. (2019). Testing a comic-based privacy policy. In *The 15th Symposium on Usable Privacy and Security*, Santa Clara, CA.

Anaraky, R. G., Knijnenburg, B. P., & Risius, M. (2020). Exacerbating mindless compliance: The danger of justifications during privacy decision making in the context of Facebook applications. *AIS Transactions on Human-Computer Interaction*, *12*(2), 70–95. https://doi.org/10.17705/1thci.00129

Avdiji, H., Elikan, D., Missonier, S., & Pigneur, Y. (2020). A design theory for visual inquiry tools. *Journal of the Association for Information Systems*, *21*(3), 695–734. https://doi.org/10.17705/1jais.00617

Baddeley, A. (2007). *Working memory, thought, and action*. Oxford University Press.

Baxter, R. J., Holderness, D. K., Jr, & Wood, D. A. (2016). Applying basic gamification techniques to IT compliance training: Evidence from the lab and field. *Journal of Information Systems*, *30*(3), 119–133. https://doi.org/10.2308/isys-51341

Benbasat, I., & Weber, R. (1996). Research commentary: Rethinking "diversity" in information systems research. *Information Systems Research*, *7*(4), 389–399. https://doi.org/10.1287/isre.7.4.389

Bernstein, M. S., Bakshy, E., Burke, M., & Karrer, B. (2013). Quantifying the invisible audience in social networks. In *The SIGCHI Conference on Human Factors in Computing Systems* (pp. 21–30), Paris, France.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Brütsch, M. (2015). The three-act structure: Myth or magical formula? *Journal of Screenwriting*, *6*(3), 301–326. https://doi.org/10.1386/josc.6.3.301_1

Buchanan, R. (1992). Wicked problems in design thinking. *Design Issues*, *8*(2), 5–21. https://doi.org/10.2307/1511637

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, *6*(1), 3–5. https://doi.org/10.1177/1745691610393980

Burmark, L. (2002). *Visual literacy: Learn to see, see to learn*. Association for Supervision and Curriculum Development.

Carpenter, B. D., & Buday, S. (2007). Computer use among older adults in a naturally occurring retirement community. *Computers in Human Behavior*, *23*(6), 3012–3024. https://doi.org/10.1016/j.chb.2006.08.015

Cavusoglu, H., Phan, T. Q., Cavusoglu, H., & Airoldi, E. M. (2016). Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook. *Information Systems Research*, *27*(4), 848–879. https://doi.org/10.1287/isre.2016.0672

Chandra, L., Seidel, S., & Gregor, S. (2015). Prescriptive knowledge in IS research: Conceptualizing design principles in terms of materiality, action, and boundary conditions. In *The 48th Hawaii International Conference on System Sciences* (pp. 4039–4048), Kauai, HI.

Checkland, P., & Poulter, J. (2010). Soft systems methodology. In M. Reynolds & S. Holwell (Eds.), *Systems approaches to making change: A practical guide* (pp. 191–242). Springer.

Chen, R., & Sharma, S. K. (2015). Learning and self-disclosure behavior on social networking sites: The case of Facebook users. *European Journal of Information Systems*, *24*(1), 93–106. https://doi.org/10.1057/ejis.2013.31

Cheong, C., Filippou, J., & Cheong, F. (2014). Towards the gamification of learning: Investigating student perceptions of game elements. *Journal of Information Systems Education*, *25*(3), 233–244. https://jise.org/volume25/n3/JISEv25n3p233.html

Cheung, C., Lee, Z. W., & Chan, T. K. (2015). Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. *Internet Research*, *25*(2), 279–299. https://doi.org/10.1108/IntR-09-2013-0192

Cole, E. (2012). *Advanced persistent threat: Understanding the danger and how to protect your organization*. Syngress.

Crossler, R., & Posey, C. (2017). Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of the Association for Information Systems*, *18*(7), 487–515. https://doi.org/10.17705/1jais.00463

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, *89*(1), 59–71. https://doi.org/10.1007/s10551-008-9909-7

Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management Science*, *32*(5), 554–571. https://doi.org/10.1287/mnsc.32.5.554

Dale, E. (1969). *Audio-visual methods in teaching* (3rd ed.). Dryden Press.

Das, S., Kim, T. H.-J., Dabbish, L. A., & Hong, J. I. (2014). The effect of social influence on security sensitivity. In *The 10th Symposium on Usable Privacy and Security* (pp. 143–157), Menlo Park, CA.

De Leoz, G., & Petter, S. (2018). Considering the social impacts of artefacts in information systems design science research. *European Journal of Information Systems*, *27*(2), 154–170. https://doi.org/10.1080/0960085X.2018.1445462

Deci, E. L., & Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry*, *11*(4), 227–268. https://doi.org/10.1207/S15327965PLI1104_01

Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013). Control-Alt-Hack: The design and evaluation of a card game for computer security awareness and education. In *ACM SIGSAC Conference on Computer & Communications Security* (pp. 915–928), Berlin, Germany.

Dennis, A. R., & Minas, R. K. (2018). Security on autopilot: Why current security theories hijack our thinking and lead us astray. *The DATA BASE for Advances in Information Systems*, *49*(SI), 15–37. https://doi.org/10.1145/3210530.3210533

DePaula, N., Dincelli, E., & Harrison, T. M. (2018). Toward a typology of government social media communication: Democratic goals, symbolic acts and self-presentation. *Government Information Quarterly*, *35*(1), 98–108. https://doi.org/10.1016/j.giq.2017.10.003

Dincelli, E., & Chengalur-Smith, I. (2019). Choose your own hacking adventure: Contextualized storytelling to enhance security education and training. In *The 15th Symposium on Usable Privacy and Security*, Santa Clara, CA.

Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems*, *23*(2), 97–102. https://doi.org/10.1057/ejis.2014.1

Drew, S. E., Duncan, R. E., & Sawyer, S. M. (2010). Visual storytelling: A beneficial but challenging method for health research with young people. *Qualitative Health Research*, *20*(12), 1677–1688. https://doi.org/10.1177/1049732310377455

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). Sage.

Fiske, S. T., & Taylor, S. E. (1984). *Social cognition*. Random House.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Frost, R. D., Matta, V., & MacIvor, E. (2015). Assessing the efficacy of incorporating game dynamics in a learning management system. *Journal of Information Systems Education*, *26*(1), 59–70. https://aisel.aisnet.org/jise/vol26/iss1/6/

Furnell, S., & Thomson, K.-L. (2009). Recognising and addressing 'security fatigue'. *Computer Fraud & Security*, *2009*(11), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

Gaeta, M., Loia, V., Mangione, G. R., Orciuoli, F., Ritrovato, P., & Salerno, S. (2014). A methodology and an authoring tool for creating complex learning objects to support interactive storytelling. *Computers in Human Behavior*, *31*, 620–637. https://doi.org/10.1016/j.chb.2013.07.011

Garba, F. A., Junaidu, S. B., Ahmad, I., & Tekanyi, M. (2018). Proposed framework for effective detection and prediction of advanced persistent threats based on the cyber kill chain. *Scientific and Practical Cyber Security Journal*, *3*(3), 1–11. https://journal.scsa.ge/papers/proposed-framework-for-effective-detection-and-prediction-of-advanced-persistent-threats-based-on-the-cyber-kill-chain/

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*, 91–109. https://doi.org/10.17705/1CAIS.01605

Ghosh, D., & Scott, B. (2018, September 24). *Digital deceit II: A policy agenda to fight disinformation on the Internet*. Harvard Shorenstein Center on Media, Politics, and Public Policy. https://www.newamerica.org/public-interest-technology/reports/digital-deceit-ii/

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. Journal of the Association for Information Systems, 18(1), 22-44. https://doi.org/10.17705/1jais.00447

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, *37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, *8*(5), 312–335. https://doi.org/10.17705/1jais.00129

Guynn, J. (2018, March 8). Delete Facebook? It's a lot more complicated than that. *USA Today*. https://www.usatoday.com/story/tech/news/2018/03/28/people-really-deleting-their-facebook-accounts-its-complicated/464109002/

Gwebu, K. L., Wang, J., & Guo, L. (2014). Continued usage intention of multifunctional friend networking services: A test of a dual-process model using Facebook. *Decision Support Systems*, *67*, 66–77. https://doi.org/10.1016/j.dss.2014.08.004

Haist, F., Shimamura, A. P., & Squire, L. R. (1992). On the relationship between recall and recognition memory. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, *18*(4), 691–702. https://doi.org/10.1037//0278-7393.18.4.691

Hamari, J. (2013). Transforming homo economicus into homo ludens: A field experiment on gamification in a utilitarian peer-to-peer trading service. *Electronic Commerce Research and Applications*, *12*(4), 236–245. https://doi.org/10.1016/j.elerap.2013.01.004

Hamari, J., & Nousiainen, T. (2015). Why do teachers use game-based learning technologies? The role of individual and institutional ICT readiness. In *The 48th Hawaii International Conference on System Sciences* (pp. 682–691), Kauai, HI.

Hanus, M. D., & Fox, J. (2015). Assessing the effects of gamification in the classroom: A longitudinal study on intrinsic motivation, social comparison, satisfaction, effort, and academic performance. *Computers & Education*, *80*, 152–161. https://doi.org/10.1016/j.compedu.2014.08.019

Hayne, S. C. (2009). Using storytelling to enhance information systems knowledge transfer. In *ISOneWorld Conference*, Las Vegas, NV.

Helms, R. W., Barneveld, R., & Dalpiaz, F. (2015). A method for the design of gamified trainings. In *The 19th Pacific Asia Conference on Information Systems*, Singapore.

Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hofstetter, R., Rüppell, R., & John, L. K. (2017). Temporary sharing prompts unrestrained disclosures that leave lasting negative impressions. *Proceedings of the National Academy of Sciences*, *114*(45), 11902–11907. https://doi.org/10.1073/pnas.1706913114

Hyerle, D. (2000). *A field guide to using visual tools*. Association for Supervision and Curriculum Development.

Iivari, J. (2015). Distinguishing and contrasting two strategies for design science research. *European Journal of Information Systems*, *24*(1), 107–115. https://doi.org/10.1057/ejis.2013.35

James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management*, *54*(7), 851–865. https://doi.org/10.1016/j.im.2017.01.001

Jenkins, J., Durcikova, A., & Burns, M. B. (2012). Forget the fluff: Examining how media richness influences the impact of information security training on secure behavior. In *The 45th Hawaii International Conference on System Sciences* (pp. 3288–3296), Maui, HI.

Jia, H., & Xu, H. (2016). Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1). https://doi.org/10.5817/CP2016-1-4

John, L. K. (2018, September). Uninformed consent. *Harvard Business Review*. https://hbr.org/cover-story/2018/09/uninformed-consent

Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and privacy: It's complicated. In *The 8th Symposium on Usable Privacy and Security*, New York, NY.

Johnson, R. D., Hornik, S., & Salas, E. (2008). An empirical examination of factors contributing to the creation of successful e-learning environments. *International Journal of Human-Computer Studies*, *66*(5), 356–369. https://doi.org/10.1016/j.ijhcs.2007.11.003

Kankanhalli, A., Taher, M., Cavusoglu, H., & Kim, S. H. (2012). Gamification: A new paradigm for online user engagement. In *The 33rd International Conference on Information Systems*, Orlando, FL.

Kapp, K. M. (2012). *The gamification of learning and instruction: Game-based methods and strategies for training and education*. John Wiley & Sons.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518–555. https://doi.org/10.17705/1jais.00274

Kim, M.-S., & Hunter, J. E. (1993). Relationships among attitudes, behavioral intentions, and behavior: A meta-analysis of past research, part 2. *Communication Research*, *20*(3), 331–364. https://doi.org/10.1177/009365093020003001

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of*

Information Security and Applications, *22*(C), 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In *The 2nd Annual eCrime Researchers Summit* (pp. 70–81), Pittsburgh, PA.

Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & Management*, *52*(7), 882–891. https://doi.org/10.1016/j.im.2015.07.006

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems*, *4*(1), 65–97. https://doi.org/10.17705/1jais.00030

Liu, D., Santhanam, R., & Webster, J. (2017). Toward meaningful engagement: A framework for design and research of gamified information systems. *MIS Quarterly*, *41*(4), 1011–1034. https://doi.org/10.25300/MISQ/2017/41.4.01

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163–200. https://doi.org/10.2753/MIS0742-1222270406

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems*, *26*(6), 546–563. https://doi.org/10.1057/s41303-017-0066-x

Lowry, P. B., Romano, N. C., Jenkins, J. L., & Guthrie, R. W. (2009). The CMC interactivity model: How interactivity enhances communication quality and process satisfaction in lean-media groups. *Journal of Management Information Systems*, *26*(1), 155–196. https://doi.org/10.2753/MIS0742-1222260107

Lujan, H. L., & DiCarlo, S. E. (2006). Too much teaching, not enough learning: What is the solution? *Advances in Physiology Education*, *30*(1), 17–22. https://doi.org/10.1152/advan.00061.2005

Mandler, J. M., & Johnson, N. S. (1977). Remembrance of things parsed: Story structure and recall. *Cognitive Psychology*, *9*(1), 111–151. https://doi.org/10.1016/0010-0285(77)90006-8

March, S. T., & Storey, V. C. (2008). Design science in the information systems discipline: An introduction to the special issue on design science research. *MIS Quarterly*, *32*(4), 725–730. https://doi.org/10.2307/25148869

Mayhorn, C. B., & Nyeste, P. G. (2012). Training users to counteract phishing. *Work*, *41*, 3549–3552. https://doi.org/10.3233/WOR-2012-1054-3549

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23–41. https://doi.org/10.1080/15332861.2010.487415

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103–125. https://doi.org/10.1057/ejis.2013.17

Mirkovski, K., Gaskin, J. E., Hull, D. M., & Lowry, P. B. (2019). Visual storytelling for improving the dissemination and consumption of information systems research: Evidence from a quasi-experiment. *Information Systems Journal*, *26*(6), 1153–1177. https://doi.org/10.1111/isj.12240

Osatuyi, B., Osatuyi, T., & de la Rosa, R. (2018). Systematic review of gamification research in is education: A multi-method approach. *Communications of the Association for Information Systems*, *42*, 95–104. https://doi.org/10.17705/1CAIS.04205

Paolacci, G., & Chandler, J. (2014). Inside the turk: Understanding mechanical turk as a participant pool. *Current Directions in Psychological Science*, *23*(3), 184–188. https://doi.org/10.1177/0963721414531598

Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, *70*, 153–163. https://doi.org/10.1016/j.jesp.2017.01.006

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Perrin, A. (2018, September 5). *Americans are changing their relationship with Facebook*. Pew Research Center. http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, *31*(4), 623–656. https://doi.org/10.2307/25148814

Pivec, M., Dziabenko, O., & Schinnerl, I. (2004). Game-based learning in universities and lifelong learning: "UniGame: Social skills and knowledge training" game concept. *Journal of Universal Computer Science*, *10*(1), 14–26. https://doi.org/10.3217/jucs-010-01-0014

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems*, *19*(2), 181–195. https://doi.org/10.1057/ejis.2010.15

Prensky, M. (2005). *Computer games and learning: Digital game-based learning. Handbook of computer game studies*. MIT Press.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778. https://doi.org/10.2307/25750704

Quinn, C. N. (2005). *Engaging learning: Designing e-learning simulation games*. John Wiley & Sons.

Ralph, P., & Monu, K. (2015). Toward a unified theory of digital games. *The Computer Games Journal*, *4*(1–2), 81–100. https://doi.org/10.1007/s40869-015-0007-7

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2016). How I learned to be secure: A census-representative survey of security advice sources and behavior. In *ACM SIGSAC Conference on Computer and Communications Security* (pp. 666–677), Vienna, Austria.

Rokeach, M. (1968). *Beliefs, attitudes and values; A theory of organization and change*. Jossey-Bass.

Rosenberg, M. J. (1960). Cognitive, affective, and behavioral components of attitudes. In C. I. Hovland & M. J. Rosenberg (Eds.), *Attitude organization and change* (pp. 1-14). Yale University Press.

Rothe, H., Wessel, L., & Barquet, A. P. (2020). Accumulating design knowledge: A mechanisms-based approach. *Journal of the Association for Information Systems*, *21*(3), 771–810. https://aisel.aisnet.org/jais/vol21/iss3/1/

Schöbel, S., Janson, A., Jahn, K., Kordyaka, B., Turetken, O., Djafarova, N., Saqr, M., Wu, D.,

Söllner, M., & Adam, M. (2020). A research agenda for the why, what, and how of gamification designs results on an ECIS 2019 panel. *Communications of the Association for Information Systems*, *46*, 706–721. https://aisel.aisnet.org/cais/vol46/iss1/30/

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In *The 3rd Symposium on Usable Privacy and Security* (pp. 88–99), Pittsburgh, PA.

Shih, H.-P., Lai, K.-H., & Cheng, T. C. E. (2017). Constraint-based and dedication-based mechanisms for encouraging online self-disclosure: Is personalization the only thing that matters? *European Journal of Information Systems*, *26*(4), 432–450. https://doi.org/10.1057/s41303-016-0031-0

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, *37*(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1016. https://doi.org/10.2307/41409970

Sohrabi, S., Riabov, A. V., Katz, M., & Udrea, O. (2018). An AI planning solution to scenario generation for enterprise risk management. In *The 32nd AAAI Conference on Artificial Intelligence* (pp. 160–167), New Orleans, LA.

Sole, D., & Wilson, D. G. (2002). *Storytelling in organizations: The power and traps of using stories to share knowledge in organizations*. Learning Innovations Laboratory, Graduate School of Education.

Spitzner, L. (2019, May 31). *Applying security awareness to the cyber kill chain*. SANS Institute. https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional*, *18*(5), 26–32. https://doi.org/10.1109/MITP.2016.84

Stutzman, F. D., Gross, R., & Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 7–41. https://doi.org/10.29012/jpc.v4i2.620

Teh, N., Schuff, D., Johnson, S., & Geddes, D. (2013). Can work be fun? Improving task motivation and help-seeking through game mechanics. In *The 34th International Conference on Information Systems*, Milano, Italy.

Thorpe, S., Fize, D., & Marlot, C. (1996). Speed of processing in the human visual system. *Nature*, *381*(6582), 520–522. https://doi.org/10.1038/381520a0

Treiblmaier, H., Putz, L.-M., & Lowry, P. B. (2018). Setting a definition, context, and theory-based research agenda for the gamification of non-gaming applications. *AIS Transactions on Human-Computer Interaction*, *10*(3), 129–163. https://doi.org/10.17705/1thci.00107

Tremblay, M. C., Hevner, A. R., & Berndt, D. J. (2010). The use of focus groups in design science research. In A. Hevner & S. Chatterjee (Eds.), *Design research in information systems* (pp. 121–143). Springer.

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A framework for evaluation in design science research. *European Journal of Information Systems*, *25*(1), 77–89. https://doi.org/10.1057/ejis.2014.36

Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, *20*(1), 83–98. https://doi.org/10.1111/jcc4.12100

Weber, J. (1992). Scenarios in business ethics research: Review, critical assessment, and recommendations. *Business Ethics Quarterly*, *2*(2), 137–160. https://doi.org/10.2307/3857568

Wisniewski, P., Islam, A., Richter Lipford, H., & Wilson, D. C. (2016). Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users. *Communications of the Association for Information Systems*, *38*, 235–258. https://doi.org/10.17705/1CAIS.03810

Woodside, A. G. (2010). Brand-consumer storytelling theory and research: Introduction to a psychology & marketing special issue. *Psychology & Marketing*, *27*(6), 531–540. https://doi.org/10.1002/mar.20342

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107–118. https://doi.org/10.1016/j.dss.2018.02.009

Zizzo, D. J. (2010). Experimenter demand effects in economic experiments. *Experimental Economics*, *13*(1), 75–98. https://doi.org/10.1007/s10683-009-9230-z

Zviran, M., & Erlich, Z. (2003). Measuring IS user satisfaction: Review and implications. *Communications of the Association for Information Systems*, *12*, 81–103. https://doi.org/10.17705/1CAIS.01205