Improving cybercrime awareness within mobile applications with the help of interactive personal data visualisation

Keywords: data visualisation, young adults, cybercrime, spyware, data breaches, data-driven design, mobile applications, awareness, knowledge, augmented reality, gamification

Anouk Vreeburg

Graduation Project DDD

22/08/2022

ABSTRACT

Mobile applications are seeing an increase in personal data attacks, and this pattern is only predicted to persist. Since the pandemic's beginning, everyone has had to communicate online, which has increased the number of opportunities for cybercriminals. The risk of harm from an cyber attack increases with the amount of personal data online. To lessen their potential for harm, vulnerable target groups need to be made aware of the problem. This study examines how data visualisation-focused augmented reality applications can aid in boosting young adults awareness and knowledge. By learning about the behaviour of the target group, design decisions can be made that as closely resemble the target group as is practical. To stay on track and assist with the development of a prototype to solve the issue, a range of theoretical research methods will be used, including the ADKAR model, Communication Privacy Management, and the Data-Driven Feedback Loop.

INTRODUCTION

Over the past few decades, digitalisation—the translation of text, images, or music into a digital format that a computer can process—has developed significantly, transforming how people interact in a constantly evolving environment (Monteith, Bauer, Alda, Geddes, Whybrow, & Glenn, 2021). Since the inception of COVID-19, the digital communication has grown remarkably more. As most individuals were ordered to stay indoors, the Internet has grown in popularity as a means of socialising, working, studying and shopping (Monteith, Bauer, Alda, Geddes, Whybrow, & Glenn, 2021). Due to the increase in Internet traffic, another aspect—cybercrime—became increasingly common. Brands, and Van Doorn (2022) describe cybercrime as *"any crime that is facilitated committed using a computer, network, or hardware device."* Cybercrime is one of the crimes with the fastest rate of growth, and COVID-19 has led to a 600% increase in its incidence (PurpleSec, 2021). Especially mobile platforms and applications could feel this impact, due to the fact that more than 24.000 harmful mobile applications are blocked daily (Rana, 2022).

While cybercrime's attack methods are constantly evolving, mobile devices and applications continue to lag behind traditional security systems (Raghavan, 2020). They are deficient in terms of technological security elements like firewalls, anti-malware protection, and encryption capabilities. In addition, mobile applications lack adequate privacy control. As a result, cybercriminals will find it easy to access the system (Raghavan, 2020). In order to build an automated assault to amass resources, a cybercriminal scans all application surfaces for automation access and gathers API

(code to identity the user) credentials (Eian, Yong, Li, & Qi, 2020). When inside, these data leaks are easily overlooked since they occur in the background and leave no traces, making it take an average of 196 days for them to be discovered (Dataprot, 2022). These outcomes could be disastrous, particularly if they are successful in stealing the victims most valuable asset—personal data (Mitrea, & Borda, 2020).

The GDPR (General Data Protection Regulation, 2019), General Data Protection Regulation, defines a personal data breach as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."* Personal data, which is any information that may be used to identify an individual, was included in 45% of breaches in 2021 (Cynixit, 2021). This percentage is high because cybercriminals can profit from this data in a variety of ways. Personal data can be used for identity theft, blackmail, opening new credit accounts, securing loans, and other types of financial fraud. It may also be sold to the highest bidder (Kimachia, 2021). Personal data is valuable information, however, 81% of users of mobile applications knowingly publish their data online without considering the hazards (Waterval, 2022).

The majority of mobile application device users are either unaware of or reluctant to address security flaws (Broadhurst, Skinner, Sifniotis, Matamoros Macias, & Ipsen, 2018). This is particularly true for "tech-savvy" young adults, who readily divulge their personal data online in search of amusement, social connections, and other requirements (Kokolakis, 2017). They overestimate their online capabilities and thereby make impulsive decisions (Kokolakis, 2017). In their study, Nzeakor, Nwokeama, and Ezeh (2020) discovered that 78% of young adults (16-24) were unaware of the various methods and reasons used in cybercrime. Young adults as a result have low levels of awareness and fear of cybercrime. Their ignorance about cybercrime is a primary source of its prevalence (Brands, & Van Doorn, 2022). As a result, young adults who are unaware of potential threats or impending attacks become the weakest link. Human error is at blame for 95% of cybersecurity problems overall (Broadhurst, Skinner, Sifniotis, Matamoros Macias, & Ipsen, 2018). Cybercriminals so attack not only security measures but also their victim perceptions (Broadhurst, Skinner, Sifniotis, Matamoros Macias, & Ipsen, 2018).

Virtual private networks, or VPNs, are one security measure that may be used to stop thieves from accessing traffic (Kimachia, 2021). The majority of young adults, though, are hesitant to pay a price

for cybersecurity (Dataprot, 2022). Other strategies include routine password changes, which just 15% of young adults now practice (Dataprot, 2022). To address the problem of human error, innovative projects have been developed. A web-based cybersecurity awareness program (WBCA), powered by blockchain, teaches users how to strengthen their security capabilities by providing cybersecurity knowledge based on actual cyberattacks and expert commentary (Razaque, Ajlan, Melaoune, Alotaibi, Alotaibi, Dias et al., 2021). It primarily focuses on studying criminal behaviour and sharing best strategies for dealing with them. The "Education as a Strategic Method against the Illegal Use of the Internet" initiative adopted a different strategy, increasing user awareness of cybercrime through cartoons, simulations, and films (Lapuh, Dime, Rozman, & Sladoje, 2014). To encourage active learning, these images depicted cybercrime encounters. Despite their disparities, the two efforts' utilisation of active learning and instructional modules proved to be a fantastic starting step in the right path for both.

Augmented reality (AR) is a technology that is acclaimed for encouraging active learning and teaching (Sidharth, 2021). With the use of technological instruments, AR is an interactive experience or enhanced representation of the real world (Sidharth, 2021). It can motivate users to actively engage with the issues at hand rather than passively reading about them on a screen (Sidharth, 2021). Therefore, young adults may become more concerned about the issue as a result. AR is helpful for a variety of purposes, including visualising material, boosting motivation and engagement, providing interactive sessions, assisting with the understanding of difficult topics, raising awareness, being available anywhere, and generally making learning more pleasurable (Alzahrani, 2020). Conserv-AR, a mobile AR application that promotes wildlife conservation, is an example of this (Alvarez, Bower, de Freitas, & Gregory, 2016). Conserv-AR students were more engaged, contented, and focused when wandering around nature and learning from their screens after incorporating components of storytelling and location awareness.

Nevertheless, there are still issues that can arise when dealing with augmented reality or cybercrime. CyberCIEGE serves as a prime illustration of such. The goal of the anti-phishing game CyberCIEGE is to help users recognise phishing websites (Alqahtani, Kavakli-Thorne, & Alrowaily, 2020). However, this initiative did not turn out well because their teaching strategies featured too much complex information, which did not pique the user's attention. Another approach was tested as part of the "SPECIAL" European research initiative. The goal of the SPECIAL project was to make users more aware of the openness of their data (Islam, Becker, Posner, Ekblom,

McGuire, Borrion et al., 2019). However, because the project was being implemented in a large setting, the voice and personality of the user were lost, and their privacy preferences were as a result disregarded. Due to this, SPECIAL was no longer compatible. The grey areas must be considered while creating a prototype for a difficult subject because any offshoot may become significant. Making a successful prototype can be challenging, but it is possible if appropriate research is done. Therefore the research questions reads: **How can augmented reality help young adults become more aware of the dangers of data theft associated with sharing personal information on mobile applications?**

THEORETICAL FRAMEWORK

This study will be carried out in accordance with the research topic, the offered methodology, the applicability of the study areas, the limitations, and the proposed approach. There are some scientific articles that address the issue and make use of techniques that could be essential to the answer. This research will examine a creative strategy to combine and work with mobile applications cybercrime, awareness and educational strategies, AR technology, and young adults' behaviour to solve the problem using models, theories, and statistics.

Cybercrime

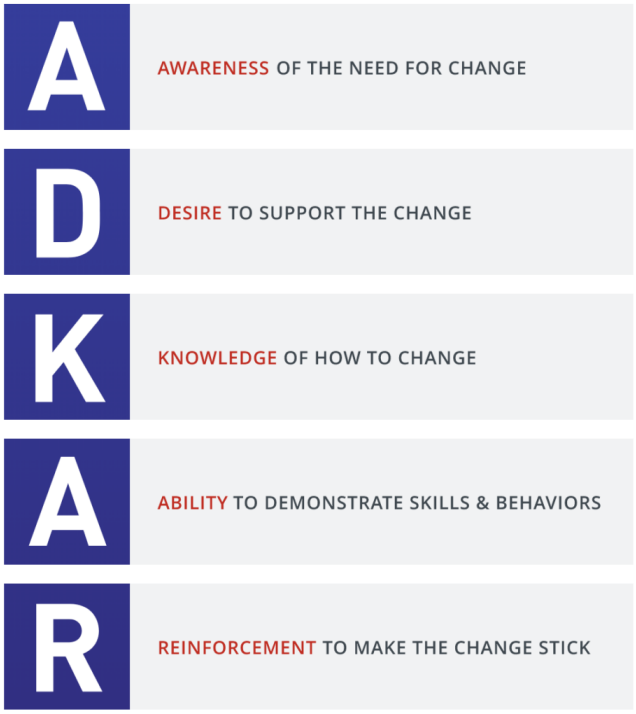
When using their phone, users may encounter a variety of cybercrime difficulties, including infected applications, risky mobile browsers, lax user logging and authentication, bad session handling, and brute force attacks (Khan, Abbas, & Al-Muhtadi, 2015). Mobile device security is notoriously inadequate, as seen by mobile devices accounting for more than 60% of digital fraud (Nelson, 2022). However, in addition to cybercriminals, manufacturers and developers also like creating holes in the system (Markelj, & Bernik, 2015). Because mobile device software manufacturers incorporate "back doors," 85% of security features are worthless on these devices (Markelj, & Bernik, 2015). These back doors provide them the ability to take control of the user's mobile device and do operations on it without the user's knowledge, such as altering software settings, receiving location data, or even sending commands. The person in charge of managing them, the mobile application developer, is likewise susceptible of misusing the user's data (Markelj, & Bernik, 2015). The personal data of the user may be taken by them if a black door was also present.

Because mobile devices have poor security and backdoors, cybercriminals can easily access applications on them by taking advantage of their vulnerability (Markelj, & Bernik, 2015). Due to their role as the central repository of user personal data, social media applications in particular suffer from this (Marttila, Koivula, & Räsänen, 2021). Name, address, date of birth, location, contacts, surfing history, banking, family, and employment information are examples of personal data (General Data Protection Regulation, 2019). In addition to personal data, sensitive data—as defined by GDPR (2019)—can also be found on applications. This data includes things like sexual orientation, political beliefs, and mental health. These data can be handled in a variety of ways, with each method pursuing a different objective when used inside the application. Malware (malicious software), phishing (email fraud), cyberstalking, social engineering, and spyware are some of the methods used (Khan, Abbas, & Al-Muhtadi, 2015). Spyware will be the main topic of this project because its sole purpose is to steal sensitive and personal data. A form of malware known as spyware can infiltrate an application with the main objective of secretly collecting user data (Khan, Abbas, & Al-Muhtadi, 2015). Once recovered, the stolen data is either sold to third parties or utilised as a form of extortion against the user (Khan, Abbas, & Al-Muhtadi, 2015).

To become more aware of this problem and to prevent it from happening, one might look at the popular Routine Activity Theory (RAT). When discussing cybercrime awareness and prevention, this theory regularly comes up. According to this situational theory of crime, a crime can only take place when there is a motivated criminal, a suitable target, and an absence of a capable guardian (Näsi, Danielsson, & Kaakinen, 2021). According to this theory, crime never occurs at random but rather always adheres to these predetermined patterns. Therefore, if the user recognised these patterns and was able to do away with one, it would lower the likelihood that they would become a victim of crime (Regalado, Timmer, & Jawaid, 2022). But RAT has also seen its share of criticism. Mikkola, Oksanen, Kaakinen, Miller, Savolainen, Sirola et al., (2020) explain that because cybercrime takes many different forms, it is challenging to compare each one using the same metrics. They say that in a technologically mediated environment context is vital. Marttila, Koivula, & Räsänen, (2021) concur, noting that her study did not indicate a difference when providing a competent guardian. Lukfeldt, & Yar, 2016 tests also show that even within the same environment, different fraud schemes had distinct results. Finally, Kikerpill (2020) concurs that the patterns are mainly meaningless and asserts that the knowledge of the individual is what matters most in the fight against cybercrime.

Awareness

Using the ADKAR model as a starting point, one can begin the process of enhancing an individual's knowledge. This model is predicated on the notion that individual change is the only way for change to occur (Goyal, & Patwardhan, 2018). The acronyms for awareness, desire, knowledge, ability, and reinforcement each stand for a stage that is necessary for transformation in that sequence. While ability and reinforcement represent the engagement zone, where action is taken, awareness, desire, and knowledge represent the enablement zone, encouraging the individual (Goyal, & Patwardhan, 2018). Only the enabling zone will be worked with because the goal of this project is awareness and information acquisition rather than taking action. To gain knowledge on the subject, one must first understand why change is necessary and then desire that change; only then are they receptive to learning and absorbing the information (Goyal, & Patwardhan, 2018). As they compared the differences between employees with and without awareness of cybercrime, the study of Alqahtani, & Kavakli-Thorne (2020) aligns with the ADKAR model. Those who were aware of cybercrime expressed greater motivation in learning how to defend against assaults when they were sent an email with information regarding cybersecurity attacks, compared to those who were unaware of the problem, who showed little to no interest at all to learn (Alqahtani, & Kavakli-Thorne, 2020). The target group of young adults fits this description because just 35% of them are aware of general cybercrime security, which is noteworthy given that 51% of them create passwords using personal information (Alzubaidi, 2021).



Situation Awareness (SA), a pathway comprising three levels of awareness, can be used to enhance the dismal awareness rates of the target group (Bolstad, & Endsley, 2006). Perception, or level 1, is an active process where the user can glean relevant information from their surroundings. Level 2 is comprehension, where the user will combine the knowledge from level 1 and discover how it affects goals and objectives in order to build a thorough understanding of the issue at hand. In level 3, referred to as projection, users consider how knowledge will affect future states depending on the current situation and their forecasts (Bolstad, & Endsley, 2006). The more of these three are present in a system, the more potent the awareness process will be (Bolstad, & Endsley, 2006). This process can be simplified by using the right delivery techniques. Alzubaidi (2021) experimented with various delivery strategies and found that texting and video for instance were the most efficient by young adults. SA is not without its challenges, though, as there are several general design factors that can impede the progress of the process. Bolstad, & Endsley (2006) lists eight examples, including out-of-loop syndrome, data overload, misplaced salience, complexity creep, workload/ anxiety stressors, and attention tunnelling.

Desire

The aforementioned theories, however, are created with the typical person in mind rather than a specific target audience, therefore they do not consider the thoughts of young adults or how they feel about cybercrime (Bolstad, & Endsley, 2006). Young individuals' awareness levels when learning were still quite low, Virtanen (2017) found, this is because they did not believe a cybercrime would at any time occur to them. An association with the Thomas (2018) research can be drawn in order to successfully raise their level of awareness. Young individuals are more likely to absorb information and be motivated to take action if they can evaluate the harm that a cyberattack can do to them. The cognitive appraisal process is influenced and stimulated by fear, and this process informs and desires the urge to wish to protect (Thomas, 2018). According to the study of Thomas (2018), this heightened incentive for protection can considerably raise users' awareness through a variety of responses. However, since victims of cybercrime already have part of that anxiety, this fear trick only works on persons who have never been the victim of a cyberattack (Virtanen, 2017). Other research supports this approach, showing that two-thirds of young individuals increased their awareness and propensity to act after hearing about potential cyberattacks (Broadhurst, Skinner, Sifniotis, Matamoros-Macias, & Ipsen, 2018). YOUN (2009) concurs and adds that emphasising one's susceptibility to threats is the best course of action because

it increases their need to become aware the most.

There are other things than susceptibility to threats that can make one fear cybercrime. A statistic from the Virtanen (2017) study demonstrates that, in addition to prior victimisation, a variety of vulnerabilities can help increase fear and, by extension, desire. It has been discovered through testing these variables on numerous individuals from all ages that women are more likely than males to fear cybercrime . This, however, only covers offences like malware, cyberbullying, and harassment (Virtanen, 2017). As a result, the gender variable won't be used in this research because it does not affect cybercrimes where personal data is stolen through mobile applications. Due to the high expenses associated with becoming a victim of cybercrime, low socioeconomic level and/or minority status are linked to greater fear of cybercrime (Virtanen, 2017). The ability to utilise the Internet confidently comes last. Fear of cybercrime may grow as a result of one's lack of trust in one's abilities or due to one's unfamiliarity with the Internet (Virtanen, 2017). The target group, however, sees it the opposite way around since they have a false sense of confidence in their Internet skills and have grown up with it, so they do not perceive it as a foreign environment (Kokolakis, 2017) . This also works against them, as the likelihood of being a victim increases with the amount of time spent online or using mobile applications (Marttila, Koivula, & Räsänen, 2021). They need to be made aware of their true capabilities and vulnerabilities in order to heighten their fear of cybercrime. However, several studies dispute the link between internet use knowledge and the fear of cybercrime, with some arguing that higher Internet use knowledge does associates with higher fear while others suggest that there is no link at all (Virtanen, 2017).

Knowledge

The Communication Privacy Management (CPM), which may classify privacy awareness data, can be helpful in raising knowledge of Internet use (Trepte, & Reinecke, 2011). Users should have the right and knowledge to regulate their personal data, according to CPM's concept, which is centered on the process of managing and protecting data. To provide users more control over their privacy, CPM has created a management system with four categories that they can adhere to (Trepte, & Reinecke, 2011). The first step is setting privacy boundaries; users are taught how to place restrictions on the information they choose to share and why doing so is crucial. Second, the purpose of privacy rules is to assist users in making better judgments regarding their personal data by outlining all the provisions. The third category, privacy turbulence, examines potential problems that can arise while working with personal data; the user then learns how to deal with those

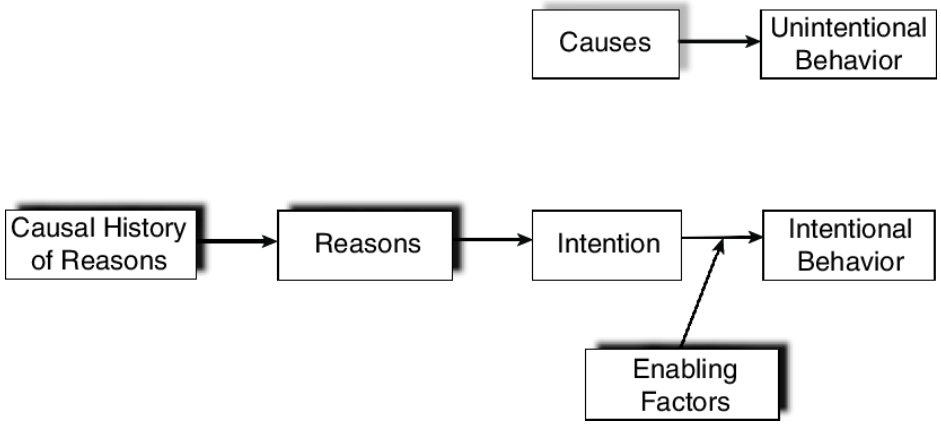
problems. And last, privacy collectives. Users who participate in privacy collectives learn how to recognise when their privacy is eroding and where their personal data may end up so they can make sure it is only utilised in appropriate and secure ways (Trepte, & Reinecke, 2011). These four categories are a useful first step in assisting users in expanding their knowledge, but changes must be made to make it more focused on mobile application cybercrime and its data.

Behaviour

Now that awareness of and attitudes about the issue may be changed, it is time for the user to start the change process in the enablement zone. Their actions, however, don't always convey this significance (Kokolakis, 2017). The privacy paradox is the name given to this phenomena. The privacy paradox is defined as *"a documented fact that users have a tendency towards privacy-compromising behaviour online which eventually results in a dichotomy between privacy attitudes and actual behaviour,"* according to Barth, & De Jong (2017). To be more specific, users spend more time worrying about their internet personal data than really taking steps to protect it. When it comes to privacy, there is a disconnect between people's attitudes and what drives them (Kokolakis, 2017). Research on this privacy conundrum has produced conflicting findings. People do care about preserving their data, according to Barth, & De Jong (2017)**,** but sadly they lack the skills to do so. Other sources claim that people can have different reactions to certain categories of personal data, for instance, feeling more protective of sensitive data than personal data, rendering the privacy paradox an incoherent concept (Kokolakis, 2017). Despite their differences, both sides agree that users require motivation in addition to awareness, desire, and knowledge in order to successfully navigate the enabling zone.

Understanding how the target groups behaviour actually functions is crucial before trying to gradually sway them to care more about the issue (Thomas, 2018). According to some theories, the reflective and impulsive information-processing brain processes govern how people use technology (Turel, & Bechara, 2016). Because they lack self-control, users of the target group tend to be more impulsive and participate in riskier behaviours (Corr, 2002). The prefrontal cortex of the brain, which is still developing in young adults and is responsible for attention, memory, decision-making, and personality, may be the root reason of this. Because of this, they frequently act inadvertently when discussing cybercrime (Mohammed, Mohamed Hussin, & Husin, 2022). Unintentional behaviour is defined as behaviour over which a person has little or no genuine control and which is influenced by their personality, upbringing, culture, and mental and emotional states (Bertram,

2011). Their impulsive thinking and thereby unintentional behaviour quickly take over when it comes to the problem of cybercrime. They expose themselves to cybercriminals as potential targets, raising their risk of becoming victims (Corr, 2002). Intentional behaviour is required to persuade the user to refrain from doing it. The ADKAR model and intentional behaviour (i.e., behaviour over which the user has control) both rely on the interaction of various mental state categories, such as belief, desire, and awareness (Bertram, 2011). By acquiring these mental states in the prototype, the user can use these categories to construct intention—a decision that comes from a cognitive process and settles on a path of action (Bertram, 2011).



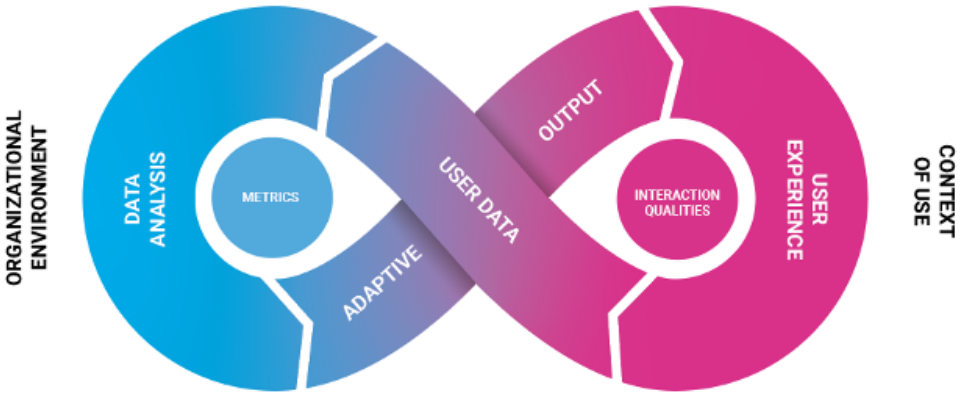
Impulsivity needs to be addressed if it were to impede the better path of action. Impulsivity causes a reduction in attention and an increase in motor activity (Corr, 2002). Therefore, the target group lack self-control and seek out instant pleasure (Corr, 2002). Smillie & Jackson (2006) talk about how a prototype would be able to leverage that to their advantage. Their research demonstrates that including gaming components can help shape how impulsive people behave. Any positive incentive event, such as prizes or a reprieve from punishment, triggers a significant reaction from impulsive users (Smillie, & Jackson, 2006). They further investigate that impulsive people also have a preference regarding these game rewards. They will always choose the first alternative when given the choice between a short-term, immediate reward and a longer-term, delayed benefit. This is due to the impulsive user finding it challenging to put off gratification (Smillie, & Jackson, 2006). Including these kinds of game components in a prototype might be advantageous.

Gamification

Gamification is another term for the addition of game components. Gamification, according to Pahlavanpour, (2022) *"is a set of activities and processes to solve problems by using or applying the characteristics of game elements."* It can enhance an experience and advance usability, productivity, and satisfaction in addition to boosting motivation (Pahlavanpour, 2022). Gamification has been increasingly common in recent years and is expected to be used in a wide range of industries, including marketing, medicine, the environment, politics, tourism, creative business, apps, and education (Alqahtani, Kavakli-Thorne, & Alrowaily, 2020). Gamification works effectively with education in particular because it helps make learning more enjoyable, simpler, and memorable (Alqahtani, Kavakli-Thorne, & Alrowaily, 2020). Serious games may spring to mind when the words "games" and "education" are used in the same phrase. Another form of gamification involves serious games, in which the subject matter is transformed into a game. It has more of a learning purpose than an entertainment one because it is frequently employed to achieve specific learning objectives, making it better for educating (Pahlavanpour, 2022). Serious games, however, take a lot of effort to build, are more challenging to understand, and once created, can only be utilised for that particular educational goal (Pahlavanpour, 2022). This is not in line with the target group, but the general gamification aspects that make content more interesting and conducive to learning are a better fit.

Gamification can take many different shapes and sizes, each of which has advantages for a particular target group. One may look at adaptive gamification to get the most out of the potential for young adults motivation and engagement (Pahlavanpour, 2022). Adaptive gaming is a cutting-edge and constantly growing research area. It seeks to incorporate more custom-made and used-entered game elements, which are necessary to support the target groups behaviour (Pahlavanpour, 2022). Personalisation can make it easier to tailor solutions to the user and contextualise them in light of the specifics of the cybercrimes when it comes to mobile applications cybercrime (Kalatha, Aliprantis, Konstantakis, Michalakis, Moraitou, & Caridakis, 2018). The data-driven feedback loop is a component that has the potential to further enhance this personalisation. When a data-driven feedback loop is implemented, the system will automatically learn from the user's input and provide an adaptable output for them (Islam, Becker, Posner, Ekblom, McGuire, Borrion et al., 2019). A prototype with a closed feedback loop will display each user the same personalisation possibilities. Letting the prototype handle the work relieves some of the pressure, especially for the impulsive target group who are easily sidetracked (Corr, 2002). By responding to the needs of the user and

defeating the "bad" actors, this framework can help all "good" actors in the system improve and the system as a whole once again (Islam, Becker, Posner, Ekblom, McGuire, Borrion et al., 2019). This is supported by a recent study by Hwang, & Helser, (2022), which found that personalising exercises and customising content to the target group can make it easier for users to increase their awareness.



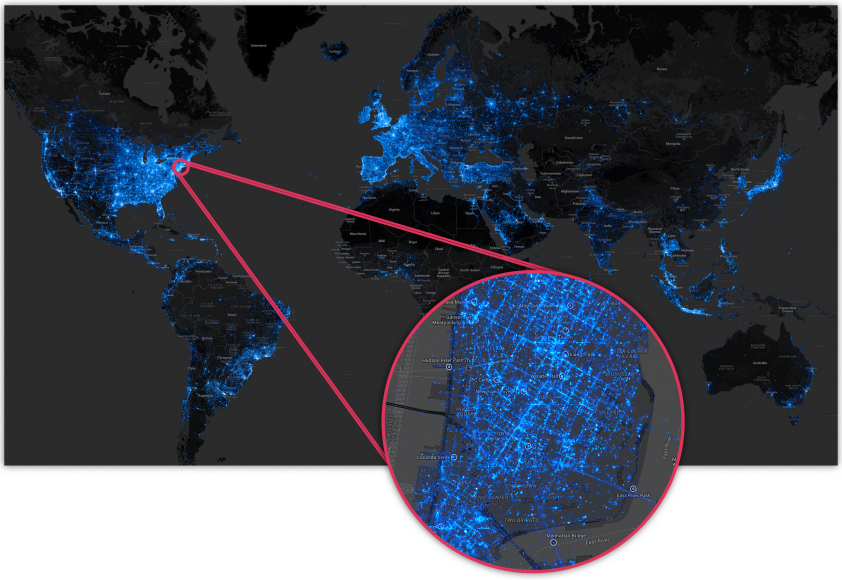
Augmented reality

Augmented reality is a technology that can effectively represent educational gamification and personalisation (Cabero-Almenara, Barroso-Osuna, Llorente-Cejudo, & Martínez, 2019). Since AR can provide knowledge in a variety of ways, using it in education offers several advantages. It can eliminate tough content, only provide understandable content, allow users to view information from a variety of angles, provide tools for everywhere learning, immerse users in information, produce a variety of resources, and enhance learning through incentive (Cabero-Almenara, Barroso-Osuna, Llorente-Cejudo, & Martínez, 2019). These are advantageous consequences for the target group, who has a hard time understanding the subject since they find it tough and overwhelming (Nzeakor, Nwokeoma, & Ezeh, 2020). It also encourages collaboration, interaction, and long-term memory retention (Cabero-Almenara, Barroso-Osuna, Llorente-Cejudo, & Martínez, 2019). Due to its fascinating hardware and software design, AR can produce this impression. An AR application is able to process this data and return to the user a customised visual transformation through keeping track of the user's movements and reactions, input recognition, and sensors (Dissanayake, 2018). Additionally, the CybAR project used this knowledge (Alqahtani, Kavakli, & Alrowaily, 2020). With the aid of augmented reality, they were able to replicate real cybersecurity threats after creating a cybersecurity awareness program. One might advance and earn points by selecting the appropriate strategies to defend yourself from these attacks. Users became more engaged in the

technology and learnt more than they would have otherwise since AR can provide a realistic scenario and a personal progress bar that adapts (Alqahtani, Kavakli, & Alrowaily, 2020).

Visuals

This visual transformation can be displayed in a variety of ways, such by combining overview and detail, focus and context, alternative visualisations, user interface elements, and/or overlay 3D visualisations, each of which has a unique strategy for illustrating context (Langner, Satkowski, Büschel, & Dachselt, 2021). It is crucial to consider the space the user will have around and/or above them when utilising the prototype when choosing which one to work with (Langner, Satkowski, Büschel, & Dachselt, 2021). Focus & Context argues that all informational elements should be immediately visible, however the target audience's attention span may make it difficult for them to focus. Alternative visualisation allows users the option to decide for themselves how they would like to view the information (Langner, Satkowski, Büschel, & Dachselt, 2021); still, as the target audience has trouble comprehending the subject, it would be better if the system could make that decision on their behalf (Brands, & Van Doorn, 2022). This is why this project will work with overview & detail, *"the simultaneous display of both an overview and detailed view, each in a distinct presentation space"* (Langner, Satkowski, Büschel, & Dachselt, 2021). The user can explore data, relate views, and make better use of a mobile device's limited display with the aid of a large visualisation in AR. Afterward, a more in-depth view of a portion of the visualisation can be viewed while engaging with the data.



Even when the information is appropriately displayed on a mobile device and the prototype is personalised, it is crucial that the target group cannot misinterpret the content. Data visualisation, often known as the visualisation of information, is a tool created to help users comprehend the data that they are viewing (Langner, Satkowski, Büschel, & Dachselt, 2021). Data visualisation has three benefits: it makes for quick analyses, increases awareness and knowledge through visual information, and is an accessible approach to take in information (Langner, Satkowski, Büschel, & Dachselt, 2021). Mavrikis, Geraniou, Gutierrez Santos, & Poulovassilis (2019) have studied the Exploration Learning Environment, a topic that focuses on deeper learning and engagement, and they concur that visualising material is the key to comprehending it better. Bhattacharjee, Chen, and Dasgupta (2020), who created their own privacy-preserving data visualisation and provided users with methods for addressing data privacy, are further advocates. The pivotal phase in their prototype was when they began to explain through images. While using images to communicate can be useful, it is crucial to do it effectively because the working memory can only keep four pieces of information at once (Zentner, Covid, & Guevarra, 2019). Visuals can be examined from several perspectives by examining various colours, forms, and sizes. These signs can change based on the target group; for instance, green could indicate profit to financial managers but infection to healthcare professionals (Zentner, Covid, & Guevarra, 2019).

Restrictions

But there are some drawbacks and restrictions to this project's design as well as advantages, which should be taken into consideration. The main drawbacks of AR are the challenges of retaining imposed information, focusing too much on virtual information, and the perception of AR as an invasive technology (Tezer, Yildiz, Masalimova, Fatkhutdinova, Zheltukhina, & Khairullina, 2019). One of the biggest problems AR has is that it is viewed as an invasive technology. As was already mentioned, when AR is activated, it continuously monitors user data (Tezer, Yildiz, Masalimova, Fatkhutdinova, Zheltukhina, & Khairullina, 2019). As the intermediary between the developer and the user in a general application, third party organisations will keep and use this data (Markelj, & Bernik, 2015). As a result, users are typically unaware of these transactions' privacy policies because they are typically not apparent to them (Markelj, & Bernik, 2015). If someone were aware, they would need to place a lot of trust in these third-party organisations. Since discussing data leaks on applications is one of the project's main objectives, it is crucial that the prototype implement a secure approach and an augmenting module for the input and output to demonstrate to the target group that they can put their trust in it.

METHODOLOGY

The goal of this study is to develop a mobile-based solution that can educate young adults about the risks associated with revealing their personal information on mobile applications. In the next step, the process will make use of a persona, use case, well-explained prototype, and testing and final prototype findings.

DataSee is a program that was made with the aid of research. DataSee was created using Figma and Unity's programming language. The final product prototype was created using an action research methodology that involved five iteration cycles. To answer the research topic, the application focuses on augmented reality, user privacy, data-driven design, and theoretical research support.

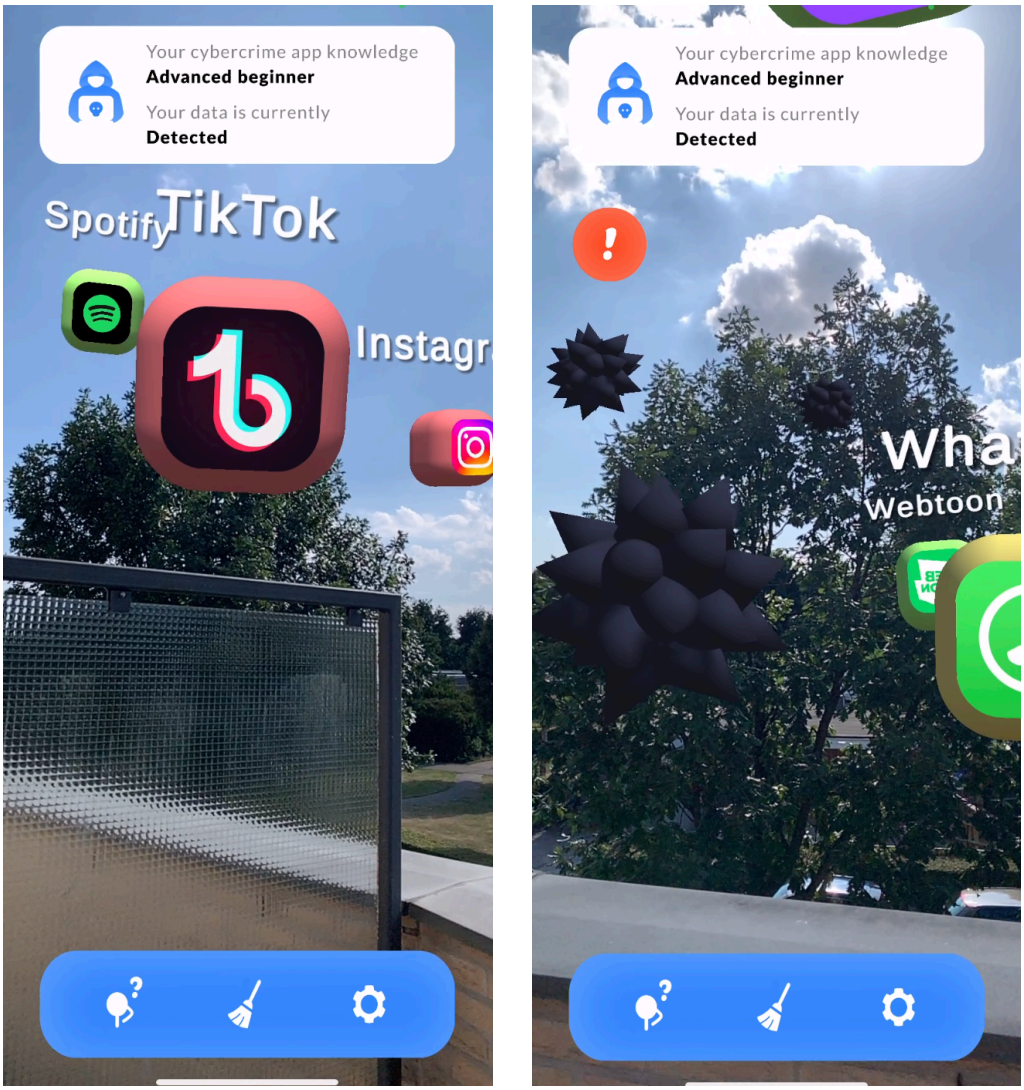
Prototype front-end

Before beginning the data visualisation, useful information is displayed on the welcome screen. This screen serves two purposes, first, it looks back at the target groups behaviour. Due to their impulsiveness and by finding the topic of cybercrime complex to understand, a little explanation in the beginning can help lessen the fall when entering the data visualisation part. Second, this screen also explains to the user how it will deal with their personal information. It explains why some of their personal information is required and makes it clear that it will only be used for this application and no other purposes. This is a crucial component because it could reassure the user that nothing improper will happen to their data.

The data visualisation screen, which shows the user's personal data, is the core component of the application. Their 10 most-used applications for the last seven days are listed in this personal data, with each application having its own data point. The size of the data point increases with the user's usage of the application. The colour of the data points depends on how much personal data each application requests, as well as on which applications cybercriminals specifically target. Safe is denoted by green, normal by orange, and dangerous by red. The user can throw their data points around in the world, simply by clicking in their surroundings. By implementing this AR feature, the user can get a clear overview of how vulnerable some applications can make them out to be.

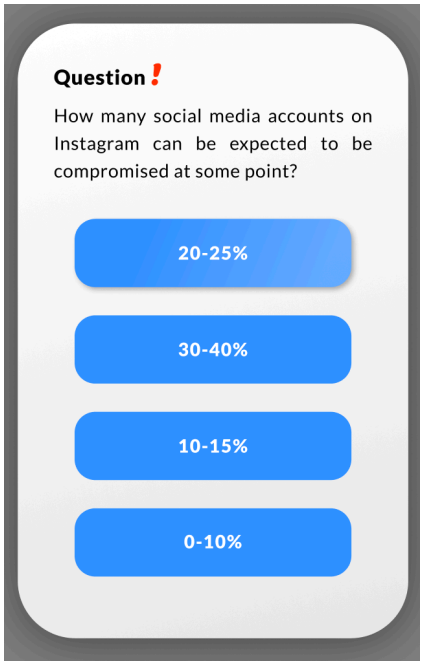
With the aid of the three situational awareness levels, this data visualisation screen also emphasises the first component of the ADKAR model, awareness. Level 1 of SA is successful with the aid of data visualisation since the user may gather pertinent information by simply observing their data

points. Only when all 10 data points are displayed on the screen do levels 2 (comprehension) and 3 (projection) also become apparent.

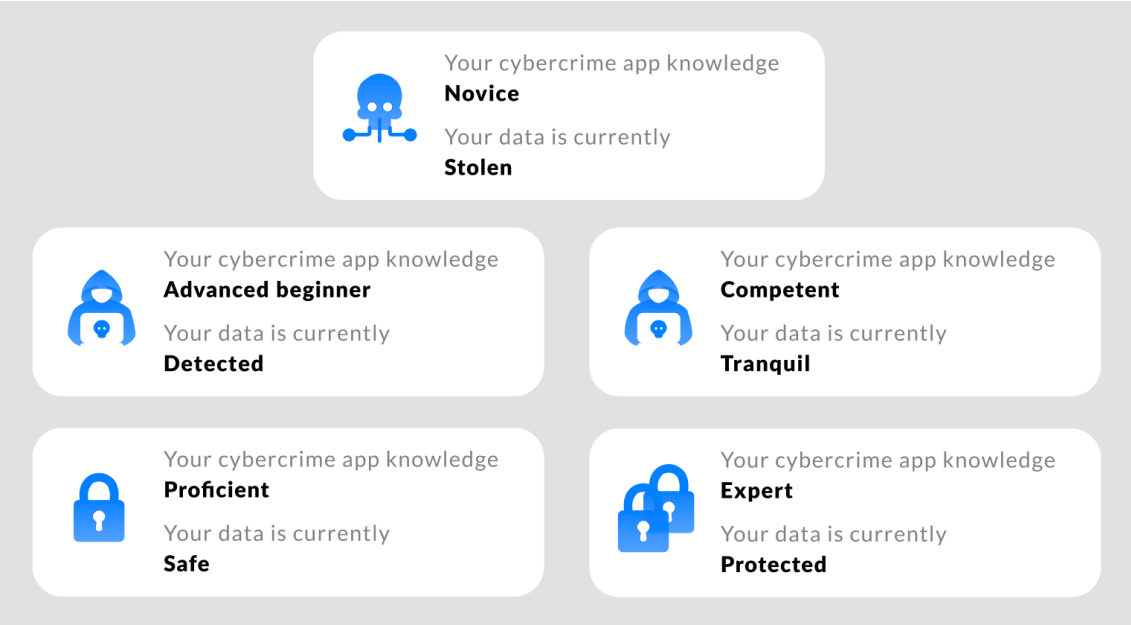


When all 10 data points are available, cyberattacks start to proliferate. This pertains to desire, the ADKAR model's second component. A cyberattack occurs every twenty seconds, though the user can alter this setting in the settings area. A virus-like blob will appear at random and there's a chance it might pay attention to a user data point. If not, it will only wander around for the user to see before disappearing, giving them the impression that cyberattacks are occurring all around them even if they are not the target. The user's data point will be attacked if the virus does concentrate on it. A sizeable red exclamation button will show up when they make contact. This button will trigger an impromptu multiple-choice question on the users familiarity with mobile applications cybercrime. If the question is correctly answered, the virus's cyberattack will not have been effective, and the data point will still be complete. If the question was incorrectly answered, the

cyberattack would have been successful, and the data point would have shown a fracture. By displaying this crack to the user, they may see that their data is no longer protected.



The question has more repercussions because it targets user behaviour and incorporates a gamification system of rewards and punishments. The primary data visualisation screen also displays the users' level of knowledge and how it affects their data. In addition to the cracks that form when an answer is incorrect, the user may lose levels and transition from being an expert with protected data to a novice with stolen data, or vice versa. There are a total of 5 levels, from novice to expert. The levels range from advanced beginner to competent to proficient. The usage of this simple reward and punishment system plays into users' impulsive desire to click on it for a quick reward. The user is thus encouraged to strive for a higher level since they feel rewarded for doing so. This rewards and punishment system can help with the third letter of the ADKAR model by incorporating education as well.



The user can click on their data points in addition to the question to get more knowledge. There are four sides to each data point, and each side has a separate CPM category of information. Users can learn more about the kind of sensitive and personal data that these programs acquire from them by looking at these categories. Additionally, it describes how cybercriminals might use this application, what to watch out for, how to stay safe, and other general facts.

Both the questions and these data points adapt to the user's input and given data. The system will try to entice the user to interact with certain data points by drawing their attention, for instance by bouncing or flashing, especially particularly large and red data points that are not being used. The system can also adjusts the questions so that for instance B questions appear more frequently if it becomes clear that a user does well on category A questions but poorly on category B ones. This way, the users will be pushed to learn every aspect of mobile application cybercrime.

Prototype back-end

The prototype's back end ensures that the data-driven feedback loop can function. The system must initially gather numerous datapoints before proceeding. The user generates the initial data points. The application asks the user if it can "screenshot" their screen time statistics when they first launch it. Screen time data shows which applications the user has used that day and for how long. After obtaining this permission from the user, the system will take a screenshot of the screen time data each day. Multiple data points can be obtained from this screenshot. The system focuses on the application's name and the time that stands behind that. The screenshot and its contents must first be cleansed before this information is collected. The image can be read with the aid of programming, and just the relevant components can be removed. It is then added to a dataset after being extracted.

Web scraping is used to gather more data points. The AppStore will be searched for every application that stood on the screen time data. What type of data the application will need from the user must be specified in a part of the AppStore. This data, which includes everything from browsing history to medical information, may be gathered with the aid of webscraping and coding. It is then combined with the other points in the dataset after being extracted.

App	Amount of time app used (minutes)	SENSITIVE - Identification method	SENSITIVE - Usage data	SENSITIVE - Purchases	SENSITIVE - Location	SENSITIVE - Contact details	SENSITIVE - User cont
TikTok	523.0	1.0	1.0	1.0	1.0	1.0	1.0
Twitch	474.0	1.0	1.0	1.0	0.0	1.0	1.0
YouTube	268.0	1.0	1.0	1.0	1.0	1.0	1.0
WhatsApp	238.0	1.0	1.0	1.0	1.0	1.0	1.0
Discord	160.0	1.0	1.0	1.0	0.0	1.0	1.0
Chrome	114.0	1.0	1.0	0.0	1.0	1.0	1.0
WEBTOON	107.0	1.0	1.0	1.0	0.0	1.0	1.0
Zalando	56.0	1.0	1.0	1.0	0.0	1.0	1.0
Twitter	44.0	0.0	0.0	0.0	0.0	0.0	0.0
Snapchat	29.0	1.0	1.0	1.0	1.0	1.0	1.0
Notities	24.0	0.0	0.0	0.0	0.0	0.0	0.0
TicketSwap	22.0	1.0	1.0	0.0	0.0	0.0	0.0
Thuisbezorgd.nl	19.0	1.0	1.0	1.0	1.0	1.0	1.0
Camera	14.0	0.0	0.0	0.0	0.0	0.0	0.0
Facebook	8.0	1.0	1.0	1.0	1.0	1.0	1.0
Instagram	7.0	1.0	1.0	1.0	1.0	1.0	1.0
Spotify	6.0	1.0	1.0	1.0	1.0	1.0	1.0
Instellingen	4.0	0.0	0.0	0.0	0.0	0.0	0.0
AllAppsTogether	2117.0	14.0	14.0	12.0	9.0	13.0	13.0

These data points must be gathered in order to give the user an experience that is as knowledgeable and personalised as feasible. It increases the user's curiosity and fear levels to have their personal data points displayed. It can help users understand which applications are more vulnerable to cybercrime by informing them of the kind of personal information those applications (sneakily) request from them.

The data-driven feedback loop became a crucial feat in order to enhance the experience and highlight the ADKAR model even more. The data-driven feedback loop enables the user to experience the changes even more effectively by showing them the information they require. It would draw attention to a particular application that the user used frequently and encourage them to learn more about its risks. More viruses might be sent to it in an effort to raise particular queries about that application. The user can be directed to the areas that require the most awareness by the data-driven feedback loop. As a result, it may be trained using only user input.

Testing - participant sampling

There are several objectives that need to be analysed when testing the final prototype. Examining how awareness has been raised, whether fear appeal played a significant role, and whether their knowledge has improved. As a result, it is also crucial to recognise the role that gamification and its environment played in raising the awareness.

The final prototype was created in Figma and Unity. One participant's seven days of screen time, which they voluntarily offered to help with the test, will be used. The final prototype will be put to the test by a total of four people. Each participant is within the target group's age range and has some college experience. All four tests were conducted offline so that the participant could hold the phone that was running the project. Each person took the test knowing that their responses would only be utilised and seen by the project leader, in order to safeguard their privacy. During the exam, participants are instructed to speak aloud while also being assigned random tasks to go from A to B. Following the test, the participants underwent an interview with a few questions.

Results

Awareness

On a scale of 1 to 5, each participant was asked to indicate how much their understanding of mobile application cybercrime has grown. Three participants gave four stars, while one gave five. All

appeared surprised after learning more about the subject, with one commenting, *"I had always seen viruses on computers; I never made the connection that it also occurred on mobile apps."* The majority concur that awareness was rapidly picked up; however, one participant did appear to struggle more and indicated that the prototype's intended aim was somewhat obscured by the initial visual overload. The participant whose data was used as an example was more taken aback than the rest. She did acknowledge that she thought the way her data was presented to her was highly fascinating when questioned. *"Gives a completely another perspective."*

Visuals

Positive feedback was heard when the application's overall layout and data visualisation were questioned. A brief statement was made on how a mobile device might become too cluttered if more than 10 data points were required and what would happen if they were. Additionally, nobody considered the designs to be obtrusive, and the icons were simple to grasp. Almost everyone immediately began pushing on the screens while eagerly scanning the area while looking at the data points. The data point, which one participant attempted to move to, sadly vanished into a wall.

Desire

The most effective fear technique had to be selected by each participant. The data points' information is chosen by two. One emphasised his worry on the questions and their replies, while the other pointed at the viruses that she could see. There were a few modest yes responses when asked if fear affected them, but no one could give a strong affirmative. They did admit that they found it unsettling to think that it might also happen to them. However, one claims that it actively converted into motivation rather than fear. *"I suppose that is a little frightening to think about, but it more drives me to make sure it never occurs."* Last but not least, a participant said that after reading about the types of personal information cybercriminals are after, it made her want to use less of it online.

Knowledge

Everybody had a wonderful experience with knowledge. When discovering the results, the arbitrary questions about cybercrime on mobile applications were amusing and unexpected. Each person went through the CPM categories inside the data point and expressed satisfaction with how clear and concise each category was. They all gave affirmative answers when asked if they felt more knowledgeable regarding the topic. One user did, however, provide some insightful input, stating

that when, for example, an Instagram data point was targeted, an Instagram question would then follow, rather than a random one

Gamification

One of the aspects that the participants liked best was the notion of rewards and punishments. It was enjoyable to interact with the questions and observe how the answers affected the data visualisation. "This is more entertaining than the last test, because then I was just staring at the data," said a participant who took part in other tests. Another participant even started getting competitive, because they wanted to reach the highest and most secure level. When there, the application's fun did, however, seem to lose some of its appeal.

Data-driven feedback loop

It became challenging to test because the data-driven feedback loop was not incorporated in the Unity software. It changed into a word op word feedback in order to still get some comments. All agreed that making it more flexible and personable would keep their interest for a longer period of time. Three out of four participants responded positively when asked if they would spend their leisure time considering the application, adding that they would come back each week to see how things had evolved. The one of the four participants who said "no" said it was amusing for once but would get old.

DISCUSSION

Some of the project's results were anticipated, while others came as a bit of a surprise. The ADKAR model performed as instructed. However, motivation—an unanticipated component that emerged in addition to desire and fear—came into play. Some participants rather felt strongly motivated when they encountered the fear factors. This aspect of change might be related to the ADKAR paradigm, where the ability, the fourth element, is positioned in the engagement zone and has to do with motivation. Potentially, this could imply that the participant is driven to participate because awareness, desire, and knowledge were all attained. The ADKAR paradigm does not necessarily need to be applied in the order of awareness, desire, and knowledge. This is due to the fact that the motivated feelings the participant experienced took place prior to the knowledge components. It is undoubtedly an intriguing angle for additional study.

As a result, one might conclude from these findings that the privacy paradox is a mythical occurrence. Some of the participants' attitudes and motivations appear to be ready for action. It appears that it gives people the motivation to modify their attitude by raising their awareness, desire, and knowledge. However, since this project did not follow up on the participants, it is unclear to say with certainty if that is the case.

Continuing on, YOUN (2009) tells that susceptibility to threats makes users fear the topic the most, however, one could argue that fear is more personal dependent than originally thought. One participant exclaimed that the aftermath of a cybercrime would scare her the most, while another participant told that the level of fear for her would dependent on the type of cybercrime. This in an interesting topic, and could definitely be seen as an update for the data-driven feedback loop. Letting the system learn the users weaknesses and exploiting them, thereby increasing their fear and desire.

In addition, YOUN (2009) claims that users fear the topic the most since they are vulnerable to attacks. However, one may counter that fear is more individualised than first believed. Another participant said that her level of dread would depend on the sort of cybercrime, while another participant said that the aftermath of a cybercrime would terrify her the most. This is a fascinating subject that undoubtedly warrants updating the data-driven feedback loop. Letting the system identify the user's fear points and exploiting them to heighten their desire and thereby awareness.

Other elements did seem to completely agree with the theories and models, for instance, gamification. Gamification was really able to help bring out the enthusiasm and interest from the target group into using the application. It also kept them busy in the application, wanting to fulfil questions and seeing how that would impact their title. It was however difficult to detect if a participant was using their impulsive unintentional behaviour or their new intentional behaviour, as it seems that the use of rewards and punishment fell in favour with both behaviours. Overall, gamification is definitely an interesting topic to discover how other gamification elements could impact the user.

Other components, such as gamification, did appear to align with the theories and models in every way. Gamification was highly successful in igniting the target group's passion and interest in utilising the program. Additionally, it kept them occupied in the application because they were eager

to answer questions and determine the influence on their title. However, it was challenging to tell whether a participant was engaging in their old unintentional impulsive behaviour or their new intentional behaviour. This is owing to the fact that both behaviours seemed to favour the application of rewards and penalties, since it focuses on both impulsive behaviour and knowledge due to the questions. Overall, exploring the idea of gamification and learning how various gamification components could impact the user are fascinating.

CONCLUSION

The research question, "can augmented reality help young adults become more aware of the dangers of data theft associated with sharing personal information on mobile applications?" can be answered with a positive affirmative. More so than that, this study appears to have had other advantageous outcomes. Along with increasing their knowledge and awareness, users' motivation and enthusiasm in the subject also increased. The ADKAR model has shown to be an effective tool for assisting users in achieving their objectives. Furthermore, the prototype might display even more interaction by including particular components catered to the users' behaviour. Although there were several benefits, one participant concluded that they would not use the application again. However, this is fine because the application still succeeded in raising their awareness, which can be seen as a job well done.

LIMITATIONS

When the project reached the final testing phase, it did have certain drawbacks. The first issue was that there weren't enough people assembled for the test. A larger participant sample would aid in the collection of more trustworthy data. Unfortunately, it was not feasible due to the time of year the testing were conducted. Second, it is regrettable that the data-driven feedback loop was unable to be field-tested. Since the prototype relies on the data-driven feedback loop, a lot of feedback was lost. This is as a result of how challenging it is to integrate it with Unity.

REFERENCES

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR). Information, 11(2), 121. https://doi.org/10.3390/info11020121

Alqahtani, H., Kavakli-Thorne, M., & Alrowaily, M. (2020). The Impact of Gamification Factor in the Acceptance of Cybersecurity Awareness Augmented Reality Game (CybAR). HCI for Cybersecurity, Privacy and Trust, 16–31. https://doi.org/10.1007/978-3-030-50309-3_2

Alvarez, V., Bower, M., de Freitas, S., & Gregory, S. (2016, October). The Use of Wearable Technologies in Australian Universities: Examples from Environmental Science, Cognitive and Brain Sciences and Teacher Training. https://www.researchgate.net/publication/309485997_The_Use_of_Wearable_Technologies_in_Australian_Universities_Examples_from_Environmental_Science_Cognitive_and_Brain_Sciences_and_Teacher_Training

Alzahrani, N. M. (2020). Augmented Reality: A Systematic Review of Its Benefits and Challenges in E-learning Contexts. Applied Sciences, 10(16), 5660. https://doi.org/ 10.3390/app10165660

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Barth, S., & De Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telematics and Informatics, 34(7), 1038–1058. https://doi.org/10.1016/ j.tele.2017.04.013

Bhattacharjee, K., Chen, M., & Dasgupta, A. (2020). Privacy-Preserving Data Visualization: Reflections on the State of the Art and Research Opportunities. Computer Graphics Forum, 39(3), 675–692. https://doi.org/10.1111/cgf.14032

Bertram, M. (2011, January). Attribution theories: How people make sense of behavior. https://www.researchgate.net/publication/302951702_Attribution_theories_How_people_make_sense_of_behavior

Bolstad, C., & Endsley, M. (2006, august). Bad situation awareness designs: What went wrong and why. https://www.researchgate.net/publication/238777577

Brands, J., & Van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. Computers in Human Behavior, 127, 107082. https://doi.org/10.1016/j.chb.2021.107082

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018). Phishing and Cybercrime Risks in a University Student Community. https:// papers.ssrn.com/sol3/papers.cfm?abstract_id=3176319

Cabero-Almenara, J., Barroso-Osuna, J., Llorente-Cejudo, C., & Fernández Martínez, M. D. M. (2019). Educational Uses of Augmented Reality (AR): Experiences in Educational Science. Sustainability, 11(18), 4990. https://doi.org/10.3390/su11184990

Corr, P. J. (2002). J. A. Gray's reinforcement sensitivity theory: tests of the joint subsystems hypothesis of anxiety and impulsivity. *Personality and Individual Differences*, *33*(4), 511–532. https://doi.org/10.1016/s0191-8869(01)00170-2

Cynixit, S. (2021, 12 december). The Dangers of Hacking and What a Hacker Can Do to Your Computer? Medium. Geraadpleegd op 21 augustus 2022, van https://medium.com/quick-code/the-dangers-of-hacking-and-what-a-hacker-can-do-to-your-computer-38d3f683a95

Dataprot. (2022, 8 juli). More Than 70 Cybercrime Statistics - A $6 Trillion Problem. Geraadpleegd op 21 augustus 2022, van https://dataprot.net/statistics/cybercrime-statistics/

Dissanayake, V. (2018, October). A review of Cyber security risks in an Augmented reality world. https://www.researchgate.net/profile/Viraj-Dissanayake/publication/339941469_A_review_of_Cyber_security_risks_in_an_Augmented_reality_world/links/5e6e3c2a299bf12e23c8ba56/A-review-of-Cyber-security-risks-in-an-Augmented-reality-world.pdf

Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Z, F. (2020). Cyber Attacks in the Era of COVID-19 and Possible Solution Domains. Cyber Attacks in the Era of COVID-19 and Possible Solution Domains. https://doi.org/10.20944/preprints202009.0630.v1

General Data Protection Regulation (GDPR) – Official Legal Text. (2019, 2 september). General Data Protection Regulation (GDPR). Van https://gdpr-info.eu

Goyal, C., & Patwardhan, M. (2018). Role of change management using ADKAR model: a study of the gender perspective in a leading bank organisation of India. International Journal of Human Resources Development and Management, 18(3/4), 297. https://doi.org/10.1504/ijhrdm.2018.093442

Hwang, M., & Helser, S. (2022, march). Cybersecurity educational games: a theoretical framework. https://www.emerald.com/insight/content/doi/10.1108/ICS-10-2020-0173/full/html

Islam, T., Becker, I., Posner, R., Ekblom, P., McGuire, M., Borrion, H., & Li, S. (2019). A Socio-Technical and Co-evolutionary Framework for Reducing Human-Related Risks in Cyber Security and Cybercrime Ecosystems. Communications in Computer and Information Science, 277–293. https://doi.org/10.1007/978-981-15-1304-6_22 (data-driven feedback loop)

Kalatha, Aliprantis, Konstantakis, Michalakis, Moraitou, & Caridakis. (2018, may). Cultural heritage engagement via serious games: the arcade augmented reality, context aware, linked open data personalised ecosystem. https://www.researchgate.net/profile/Aysen-Kovan/publication/351102549_Universite_Ogrencilerinin_Iletisim_Becerileri_Acisindan_Bazi_Degiskenler_ile_Incelenmesi_Egitim_ve_Saglik_Bilimleri_Fakultelerinin_Karsilastirilmasi/links/6086fc4c907dcf667bc6fa3d/Ueniversite-Oegrencilerinin-Iletisim-Becerileri-Acisindan-Bazi-Degiskenler-ile-Incelenmesi-Egitim-ve-Saglik-Bilimleri-Fakueltelerinin-Karsilastirilmasi.pdf#page=309

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. Procedia Computer Science, 56, 376–383. https://doi.org/10.1016/j.procs.2015.07.223

Kikerpill, K. (2020). The individual's role in cybercrime prevention: internal spheres of protection and our ability to safeguard them. Kybernetes, 50(4), 1015–1026. https:// doi.org/10.1108/k-06-2020-0335

Kimachia, K. (2021, 10 augustus). Here are five mobile attack surfaces targeted by cybercriminals with tips on how app developers can improve cybersecurity. IT Business Edge. Geraadpleegd op 21 augustus 2022, van https://www.itbusinessedge.com/mobile/5-mobile-attack-surfaces-targeted-by-cybercriminals/

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134. https:// doi.org/10.1016/j.cose.2015.07.002

Langner, R., Satkowski, M., Büschel, W., & Dachselt, R. (2021). MARVIS: Combining Mobile Devices and Augmented Reality for Visual Data Analysis. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3411764.3445593

Lapuh, J., Dime, M., Rozman, D., & Sladoje, A. (2014). Raising awareness of cybercrime - the use of education as a means of prevention and protection. https://files.eric.ed.gov/ fulltext/ED557216.pdf

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. Deviant Behavior, 37(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Markelj, B., & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. Journal of Information Security and Applications, 20, 84–89. https://doi.org/10.1016/j.jisa.2014.11.001

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime Victimization and Problematic Social Media Use: Findings from a Nationally Representative Panel Study. American Journal of Criminal Justice, 46(6), 862–881. https://doi.org/10.1007/s12103-021-09665-2

Mavrikis, M., Geraniou, E., Gutierrez Santos, S., & Poulovassilis, A. (2019). Intelligent analysis and data visualisation for teacher assistance tools: The case of exploratory learning. British Journal of Educational Technology, 50(6), 2920–2942. https://doi.org/ 10.1111/bjet.12876

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., Zych, I., & Paek, H. J. (2020). Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context. International Journal of Offender Therapy and Comparative Criminology, 0306624X2098104. https://doi.org/10.1177/0306624x20981041

Mitrea, T., & Borda, M. (2020). Mobile Security Threats: A Survey on Protection and Mitigation Strategies. International conference KNOWLEDGE-BASED ORGANIZATION, 26(3), 131–135. https://doi.org/10.2478/kbo-2020-0127

Mohammad, T., Mohamed Hussin, N. A., & Husin, M. H. (2022). Online safety awareness and human factors: An application of the theory of human ecology. Technology in Society, 68, 101823. https://doi.org/10.1016/j.techsoc.2021.101823

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Current Psychiatry Reports, 23(4). https://doi.org/10.1007/s11920-021-01228-w

Näsi, M., Danielsson, P., & Kaakinen, M. (2021). Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors. European Journal on Criminal Policy and Research. https://doi.org/10.1007/s10610-021-09497-0

Nelson, B. (2022, 27 juli). Top Security Threats of Smartphones (2022). Reader's Digest. Geraadpleegd op 21 augustus 2022, van https://www.rd.com/article/mobile-security-threats/

Nzeakor, O., Nwokeoma, B., & Ezeh, P. (2020). Pattern of Cybercrime Awareness in Imo State, Nigeria: An Empirical Assessment. https://www.proquest.com/docview/ 2404396076?fromopenview=true&pq-origsite=gscholar

Pahlavanpour, O. (2022). Gamification within information security awareness programs:. https://www.diva-portal.org/smash/get/diva2:1679503/FULLTEXT01.pdf

PurpleSec. (2021, 6 augustus). 2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends. Van https://purplesec.us/resources/cyber-security-statistics/

Raghavan, R. (2020, 26 mei). All About Cyber-Attacks on Mobile Devices and How to Protect Against Them? Web Solutions Blog. Geraadpleegd op 21 augustus 2022, van https://acodez.in/cyber-attacks-on-mobile-devices/

Rana, O. (2022, 13 februari). 10 Concerning Cybercrime Statistics For 2022 - Rogue Logics. Rogue Logics - Security Is NOT Optional. Geraadpleegd op 21 augustus 2022, van https://www.roguelogics.com/10-concerning-cybercrime-statistics-for-2022/

Razaque, A., Al Ajlan, A., Melaoune, N., Alotaibi, M., Alotaibi, B., Dias, I., Oad, A., Hariri, S., & Zhao, C. (2021). Avoidance of Cybersecurity Threats with the Deployment of a Web-Based Blockchain-Enabled Cybersecurity Awareness System. Applied Sciences, 11(17), 7880. https://doi.org/10.3390/app11177880

Regalado, J., Timmer, A., & Jawaid, A. (2022). Crime and deviance during the COVID-19 pandemic. Sociology Compass. https://doi.org/10.1111/soc4.12974

Sidharth, J. (2021). Benefits of Augmented and Virtual Reality for Constructing Top Mobile App. https://www.europeanbusinessreview.com/benefits-of-augmented-and-virtualreality-for-constructing-top-mobile-app/

Smillie, L. D., & Jackson, C. J. (2006). Functional Impulsivity and Reinforcement Sensitivity Theory. *Journal of Personality*, *74*(1), 47–84. https://doi.org/10.1111/ j.1467-6494.2005.00369.x

Tezer, M., Yildiz, E., Masalimova, A., Fatkhutdinova, A., Zheltukhina, M., & Khairullina, E. (2019). Trends of Augmented Reality Applications and Research throughout the World: Meta-Analysis of Theses, Articles and Papers between 2001-2019 Years. https://www.learntechlib.org/p/217151/

Thomas, J. E. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. International Journal of Business and Management, 13(6), 1. https://doi.org/10.5539/ijbm.v13n6p1

Turel, O., & Bechara, A. (2016). A Triadic Reflective-Impulsive-Interoceptive Awareness Model of General and Impulsive Information System Use: Behavioral Tests of Neuro-Cognitive Theory. Frontiers in Psychology, 7. https://doi.org/10.3389/fpsyg.2016.00601

Virtanen, S. M. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. Psychiatry, Psychology and Law, 24(3), 323–338. https://doi.org/10.1080/13218719.2017.1315785

Waterval, R. (2022). How information sharing on online social networks may allow for personalized cyberattacks - University of Twente Student Theses. Van http:// essay.utwente.nl/89460/

YOUN, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. Journal of Consumer Affairs, 43(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x 27

Zentner, A., Covit, R., & Guevarra, D. (2019). Exploring Effective Data Visualization Strategies in Higher Education. *SSRN Electronic Journal*. https://doi.org/10.2139/ ssrn.3322856