Implementation of Serious Games for Data Privacy and Protection Awareness in Cybersecurity

Siti Normaziah Ihsan
Faculty of Computing
Universiti Malaysia Pahang
Pahang, Malaysia
normaziah@ump.edu.my

Tuty Asmawaty Abd Kadir
Faculty of Computing
Universiti Malaysia Pahang
Pahang, Malaysia
tuty@ump.edu.my

Nurul Ishafira Ismail
Faculty of Computing Universiti
Malaysia Pahang
Pahang, Malaysia
ishafiraismail@gmail.com

Kerk Zhi Yuan
Teleperformance Malaysia
Selangor, Malaysia
kerkzy1999@gmail.com

Yeow Song Jie
Sim IT Sdn Bhd Johor,
Malaysia
$song_jie99@hotmail.com$

Abstract—Information security and privacy are big issues in today's digital world, and people should be aware of the risks that come with using their personal information online. There are many things that can be done to make people more aware of the importance of keeping personal information safe from attacks, such as an educational campaign, workshops and training sessions, public service announcements, and events in the community. Serious games, which are also called educational games, are a type of educational campaign activity that is meant to teach or train players about a certain subject or skill. They can play an important role in raising awareness of data privacy and information security by providing an engaging and interactive way for players to learn about these important topics. In this study, we suggest a game design architecture for protecting and keeping data private in cybersecurity. In order to validate the architecture, Datanion, a platform game, was created to educate the public on maintaining data privacy over the internet. This lack of awareness will have negative effects on mental health, private information, and computer equipment. Through these games, players can learn the basics of cybersecurity in a fun way, such as how to use strong passwords, recognise and avoid phishing websites, and how firewalls work. The advantage of playing these games is that they can help non-expert end users improve their knowledge and awareness of cybersecurity and also increase a player's motivation, engagement, and comprehension of cybersecurity knowledge.

Keywords—serious games, awareness, cybersecurity, data privacy, protection

I. INTRODUCTION

Today's digital world worries about assaults on personal gadgets that steal or safeguard private data. Cellphones, computers, and tablets hold sensitive data such login passwords, financial data, and contact information. Attackers may steal this data from these devices and exploit it for identity theft or financial crime. Data privacy and security on personal devices may be compromised in several ways. These include malware, phishing, and theft.

In this way, data privacy and security are still important issues in the digital world, even though their nature is always changing. Data breaches, in which the sensitive information of a company or organization is either exposed to the public or stolen by cybercriminals, are an example of a current issue that relates to data privacy and protection. A breach of data security can result in stolen identities, fraudulent financial transactions, and other types of illegal behavior. The Equifax breach [1], the Capital One breach [2], and the Marriott breach [3] are three of the most notable data breaches that have occurred in the past few years.

As more people use the internet and other digital devices, concerns about how businesses and other organizations use customers' personal information have grown. In response, new privacy laws like the General Data Protection Regulation (GDPR) of the European Union [4] and the California Consumer Privacy Act (CCPA) [5] give individuals more control over their personal data and require businesses to be transparent about how they collect and use it. Due to the Cambridge Analytica data leak, these laws were passed. In April 2019, Facebook announced that it had inadvertently stored the passwords of hundreds of millions of users in plain text, leaving them accessible to Facebook employees [6]. Data protection and privacy issues have also emerged due to the increased use of IoT devices like smart speakers and home security systems. Who accesses and uses the vast volumes of data captured and sent by these devices is concerning. Complex and changing are data privacy and protection problems. The confidentiality of sensitive information requires 24/7 surveillance.

In the most recent few years, the concept of using serious games as a new method that can supplement computer-based or instructor-led cybersecurity education and training has been proposed [7]. Players can learn about data privacy and information security in an engaging and interactive way. Serious games teach many data privacy and security lessons. Below are some serious gaming data privacy and security education methods. Serious games can simulate real-life events and show the risks of data privacy and system security. Players may understand the consequences of their actions and make better decisions. They may also give specific feedback on their decisions' effects, helping people understand how