Chapter 61
Cyber Security Patterns Students Behavior and Their Participation in Loyalty Programs

Witold Chmielarz
University of Warsaw, Poland

Oskar Szumski
University of Warsaw, Poland

ABSTRACT

Despite of the number of public advice campaigns, researchers have found that individuals still engage in risky cyber behaviour. The first part of this article is focused on the general approach to the cyber security and safety of personal data kept and processed by different entities from the perspective of students, while the second part is dedicated to the privacy aspects from the perspective of loyalty programs. Researchers have found that individuals are typically aware of online security and how to protect their privacy in the network, Nonetheless, individuals are still inclined to take risks because they are unrealistically optimistic and believe that negative events are less likely to happen to them. The survey also shows that even though respondents are aware that retailers collect, and process personal data and respondents feel that the amount of personal data of program members is far beyond the accepted level they still participate in such programs. Authors found also interesting patterns related to behaviour of respondents influenced by demographical data and the area of loyalty.

INTRODUCTION

Popularity of information technologies and transfer of significant part of personal and business life to virtual reality evolved a new set of dangers related to security and privacy aspects in the internet. Nowadays, the Internet has a significant role in enabling the communications, monitoring, operations, business systems and personal applications. Nowadays, serious number of countries are developing own strategies

DOI: 10.4018/978-1-5225-8897-9.ch061

securing their vital infrastructure (Azmi, Tibben & Win, 2016). People more and more often use internet as a medium to execute different activities that also bring new forms of privacy threats to the community. Despite other threats technology is not the major aspect that puts people privacy in danger. It can be noticed that human behaviour is one of the most risky elements of cyber security (Whitty, Doodson, Creese & Hodges, 2015; Wiederhold, 2014). Looking at the current situation cyberattacks become more frequent and take different forms, starting from the simplest ones e.g. phishing where attacked person is convinced to open infected attachment to serious cyber-attacks on national infrastructure (Snyder, 2014).

Also transfer of personal and business life to virtual reality moves loyalty programs, that are recognised as privacy-sensitive segment also to digital era. People more often use internet as a medium to execute different activities including loyalty programs and moving physical cards to mobile applications, that also bring other privacy threats to the community, where apart from analysis of common data used by retailers to investigate trends allows also for deeper analysis of other sensitive data collected from customers with or without their knowledge. It also puts other type of risk related to cybersecurity on participants of such programs. It can be noticed that human behaviour is one of the most risky elements of cyber security (Whitty, Doodson, Creese & Hodges, 2015; Wiederhold, 2014). As other research proves the major risk lay beneath the personal approach to cyber security and privacy protection of internet users (Winnefeld, Kirchhoff & Upton, 2015).

As other research proves the major risk lay beneath the personal approach to cyber security and privacy protection of internet users (Winnefeld, Kirchhoff & Upton, 2015). "In the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors" (Zadelhoff, 2016).

Definition of a cybersecurity can be found in many publications and standards, although in this article authors would use the definition of cyber security that was used by von Solms and van Niekerk (2013) where is defined as protection of both informational and non-informational assets through the ICT infrastructure.

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and nonrepudiation, Confidentiality" (Solms & Niekerk, 2013).

Loyalty programs, this is something that everyone have heard, and many of us are members of at least one and with time the amount on such cards in our wallet (or e-wallet) increases. The idea beneath that was to get some rewards from retailers in exchange of making purchases from them. To be a member person is requested to provide many personal information such as name, telephone number, email address, snail mail address, and possibly other defining characteristics or shopping preferences, all that allows to track our purchases and make a deep analysis of our life and patterns of behaviour. Every time a member makes a purchase, owner of a program matches the purchase information to the shopper's personal information. Shoppers' purchasing data is useful to the individual retailer, but the real revenue stream is in the world of Big Data (Rivard & Crossley, 2014).

Back in 2004, an online survey conducted by Boston University's College of Communication found that adult supermarket shoppers believed that the benefits of using a loyalty card outweighed any infringement on personal privacy (McQuivey, 2014). This research was done in 2004, so there is no doubt that