Chapter 96
The Impact of Online Training on Facebook Privacy

Karen H. Smith
Texas State University, USA

Francis A. Méndez Mediavilla
Texas State University, USA

Garry L. White
Texas State University, USA

ABSTRACT

Facebook is a major part of the lives of many consumers who share a considerable amount of information with friends, acquaintances, and commercial interests via the platform, leading to greater exposure to privacy risks. Training has been shown to be effective in reducing computer risk in a variety of contexts. This study investigates the effectiveness of training on consumer attitudes and behavioral intentions toward Facebook privacy risk. The study highlights the importance of training consumers on how and why they need to protect their privacy. Findings suggest that training can reduce consumer risk, but effectiveness can vary across types of training. For example, Facebook's Privacy Tour was less effective than third party training videos in improving consumer vigilance. Implications of the findings for consumers and privacy advocates are discussed.

INTRODUCTION

George Orwell's book *1984* (Orwell, 1949) described a society where the government constantly monitored its people, effectively eliminating citizens' privacy. Today, citizens willingly give up their privacy through social networks. In 2010 Mark Zuckerberg, founder of Facebook, declared that the "age of privacy is over" (Sarrel, 2010). Social networks have increased the amount of personal and identity information that is freely shared on the Internet. People often disclose too much personal information on social media such as Facebook, where privacy is not assured (Waters & Ackerman, 2011). People expose information about themselves by making personal information available to others to see and use. This exposure also

DOI: 10.4018/978-1-5225-7113-1.ch096

occurs by revealing preferences and habits. Knowledge of these preferences and habits allows intruders to detect behavioral patterns that can be used to predict courses of action (Shaw, 2009).

By incurring risky behavior, people do not only risk their personal information; but also information about others and perhaps even about the institutions that they represent. There is a need for better information security, especially privacy, awareness and education to improve protective behavior of users (Mensch & Wilkie, 2011; Okenyi & Owens, 2007). Therefore, it is in the best social interest that individuals are trained to protect their information. This study explores the idea that people can be trained to protect their privacy and poses the idea that peoples' attitudes and behavior intentions can be used to measure training effectiveness. Two key questions are:

- Can training reduce privacy risks?
- In addition, what attitudes and behavior intentions are impacted?

This study seeks to answer these questions.

On the Internet, there are multiple venues by which people expose private information, such as:

- Facebook,
- Twitter,
- MySpace,
- Instagram,
- Blogs, and others.

For this study, we have chosen Facebook due to its popularity (Madden, Lenhart, Cortesi, Gasser, Duggan, Smith, & Beaton, 2013), because it is a major part of many users' lives (Debatin, Lovejoy, Horn, & Hughes, 2009), and because these users share a considerable amount of information with friends, acquaintances, and commercial interests via the platform. Furthermore, Facebook has not been known as a protector of user privacy (Kuczerawy & Coudert, 2010). However, Facebook introduced a privacy education feature in 2012, the Facebook Privacy Tour (FPT), because of lawsuits and recommendations from user protections agencies in the U.S. and abroad. FTP features four screen shots about how to access privacy settings and was implemented for new users who go through the screen shots when they initially sign up for Facebook (Martinez, 2012). The research presented here tests the effectiveness of the FPT screen shots, as well as two additional training videos, in changing users' attitudes and behaviors toward protecting their privacy on Facebook.

Individuals can control disclosure and recipients of their personal information, but due to frequent modification to privacy policies, many users are unaware of who can access their information and for what purposes it can be used. One study found that if users do not take the time to investigate and educate themselves on the changes found in privacy policies, their perceived privacy settings are often times inconsistent with their actual settings (Butler, McCann, & Thomas, 2011). Furthermore, privacy policies and privacy controls may be confusing to many users. For example, Facebook's original privacy policy was written for Web-users with a minimum of two years of college education (Jafar & Abdullat, 2011). Thus, it is important to empirically investigate how users utilize social network privacy settings in order to inform the public.