Chapter 4

Social Networking and Trust: Is Personalisation the Only Defence Technique?

Vladlena Benson
Kingston University, UK

ABSTRACT

Based on the literature review of the theory of trust, this chapter aims to provide an insight into trust formation on social networking sites (SNS). An overview of the current state of cybercrime and known ways of threat mitigation helps shed some light on the reasons why social networks became easy targets for Internet criminals. Increasingly, personalisation is seen as a method for counteracting attacks perpetrated via phishing messages. This chapter aims to look specifically at trust in online social networks and how it influences vulnerability of users towards cybercrime. The chapter poses a question whether personalisation is the silver bullet to combat cyber threats on social networks. Further research directions are discussed.

INTRODUCTION

The notion of trust elongates from social context to human computer interactions. Much research (e.g. Beudoin, 2008; Jiang, Jones, and Javie, 2008) now recognises the importance of understanding trust and trust-building in online communication, transactions and systems. Online interactions involve various types of risks and entail presence of trust between communicating parties as well as in the applications used for these interactions (Riegelsberger, Sasse, and McCarthy, 2003). Over the past few years there has been an emergence of a number of online social networking sites, such as MySpace, Facebook, Twitter, LinkedIn, to name but a few. Social networking sites (SNS) provide a straightforward, user-friendly and convenient way to connect and share information with other users online. This explains the growing popularity of such SNS as Facebook, which counts more than
200 million active users. Over 100 million people made logging into Facebook a daily routine and the amount of content shared through the site reached one billion pieces (including web links, stories, blogs posts, photos, etc.) each week (Facebook Statistics, 2009). Features for customising personal profile and privacy settings, peer based rating system and a sense of a secure environment for sharing personal information and content made SNS immensely popular.

The nature of social interactions online forms the basis for trust building and trust-transfer between users of social networks. Online interactions are possible only when not only users trust each other, but also when they have enough faith in the systems they use to transact as well as the organisations which provide them (Riegelsberger et al., 2005). Trust in e-commerce application has attracted a significant research attention (Golbeck, 2008), the concept of trust has been linked to security and used in context of privacy, identity and authorisation. Research efforts have been directed at establishing factors influencing trust in online applications. For example, Dutton and Shepherd (2006) argue that trust on the Internet has been based on two indicators: net-confidence and net-risk. Perceptions of confidence in the Internet technology has been expressed through the level of reliability of information on the Internet, trust in the institutions running the Internet and the confidence in people with whom they conduct online communication and transactions. Net-risk was defined as the perceived exposure to risks or user perceived vulnerability to threats while using the Internet.

Earlier studies showed that those people who use the Internet more tend to gain more trust in technology. Dutton and Shepherd (2006) highlighted that education and experience determine formation of trust among Internet users. They also showed that reinforcement of the digital divides, including life stage factors, social gaps and proximity to the Internet, translates into significant differences in levels of trust developed by people.

Based on these arguments and data reported in the 2007 OxIS Survey (Dutton and Helsper, 2008) it is possible infer that higher levels of trust are developed by individuals aged between 18 and 24 that intensively use social media and have the closest proximity to technology. Monitoring the threats from Internet criminals has been the centre of attention of major information security solution providers, e.g. Symantec, MessageLabs, SANs and others. However, research literature demonstrates a lack of sustained research into how social networking users are affected by cybercrime and how they respond to the existing threats. This chapter helps fill the gap in the literature by a) providing an analysis of factors influencing formation of trust in technology in online social networks, b) identifying factors which make social networking users vulnerable to cybercrime and c) provoking a discussion on the reliability of personalisation as the mitigation instrument against social networking vulnerabilities.

The structure of the rest of the chapter is organised as follows: Section 2 provides an overview of the trust theory further linked to the discussion of trends in cybercrime in section 3. Section 4 describes scenarios of Internet attacks perpetrated through social networking sites. Section 5 summarises the factors which influence formation of trust among users of online social networks and examines the aspects of behaviour which make their users prone to cybercrime. The article concludes with the discussion about whether personalisation is the silver bullet to combat cyber threats on social networks. Further research directions are discussed.

**Critical Concepts**

Social Exchange Theory provides a framework defining trust and helps explain formation of trust in interpersonal and exchange relationships. A general definition can be given to trust as a "psychological state comprising the intentions to accept vulnerability based upon positive expecta-
Related Content

Discovering and Characterizing Places of Interest Using Flickr and Twitter
Steven Van Canneyt, Steven Schockaert and Bart Dhoedt (2013). *International Journal on Semantic Web and Information Systems* (pp. 77-104).
[www.igi-global.com/article/discovering-and-characterizing-places-of-interest-using-flickr-and-twitter/97654?camid=4v1a](www.igi-global.com/article/discovering-and-characterizing-places-of-interest-using-flickr-and-twitter/97654?camid=4v1a)

SPORTAL: Profiling the Content of Public SPARQL Endpoints
[www.igi-global.com/article/sportal/160175?camid=4v1a](www.igi-global.com/article/sportal/160175?camid=4v1a)

Fault-Tolerant Emergent Semantics in P2P Networks
[www.igi-global.com/chapter/fault-tolerant-emergent-semantics-p2p/28852?camid=4v1a](www.igi-global.com/chapter/fault-tolerant-emergent-semantics-p2p/28852?camid=4v1a)

SemDiff: An Approach to Detecting Semantic Changes to Ontologies
[www.igi-global.com/article/semdiff-approach-detecting-semantic-changes/2825?camid=4v1a](www.igi-global.com/article/semdiff-approach-detecting-semantic-changes/2825?camid=4v1a)