Chapter 4.9
Determining the Intention to Use Biometric Devices:
An Application and Extension of the Technology Acceptance Model

Tabitha James
Virginia Polytechnic Institute & State University, USA

Taner Pirim
Mississippi Center for Supercomputing Research, USA

Katherine Boswell
Middle Tennessee State University, USA

Brian Reithel
University of Mississippi, USA

Reza Barkhi
Virginia Polytechnic Institute & State University, USA

ABSTRACT

Protection of physical assets and digital information is of growing importance to society. As with any new technology, user acceptance of new software and hardware devices is often hard to gauge, and policies to introduce and ensure adequate and correct usage of such technologies are often lacking. Security technologies have widespread applicability to different organizational contexts that may present unusual and varied adoption considerations. This study adapts the technology acceptance model (TAM) and extends it to study the intention to use biometrics devices across a wide variety of organizational contexts. Due to the use of physiological characteristics, biometrics present unique adoption concerns. TAM is extended in this study to include constructs for perceived need for privacy, perceived need for security and perceived physical invasiveness of

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

biometric devices as factors that influence intention to use. The model is shown to be a good predictor of intention to use biometric devices.

INTRODUCTION

Property theft, violent crimes, theft and misuse of digital information, terrorism, and threats to privacy, including identity fraud, in today's digitally connected, mobile society necessitate the development of tools to protect digital information and physical assets by both individuals and corporate entities. According to findings from the National Crime Victimization Survey, approximately 24 million U.S. residents were victims of crime in 2003, including both property crime and violent criminal acts (Bureau of Justice, 2003). The 2003 CSI/FBI Computer Crime and Security Survey reported that 56% of their participants reported unauthorized computer use. Out of the respondents that were willing or could quantify the financial implications, the amount of losses reported exceeded $200 million (Richardson, 2003). The Federal Trade Commission (FTC) reported 86,168 cases of identity fraud in 2001 and stated that they believe this figure does not capture all the cases (FTC, 2001). Identity fraud categories included credit card fraud, telecommunications/utility fraud, bank fraud, employment fraud, fraudulent loans, government documents or benefits fraud, evasion of legal sanctions and criminal records, medical services, opening of Internet accounts, leasing of a residence, bankruptcy filings, trading of securities or investments, among others (FTC, 2001).

The need to secure both digital and physical assets is apparent from these statistics, yet it is often difficult for technology to keep pace with the growing number of threats and the increasing number of vulnerabilities that exist in traditional methods of security. A method of identification that has been growing in popularity is the use of physical or behavioral traits, such as fingerprints or DNA, to identify and authenticate individuals. Certain physical and behavioral traits are unique to each individual and therefore may provide methods of identification that are more successful than traditional approaches. Technological devices that utilize these unique traits to identify and authenticate an individual are known as biometrics. These devices have the obvious advantage of not falling prey to many of the well known vulnerabilities of traditional methods. Since a biometric device uses a unique biological trait to distinguish an individual, it is very difficult and often impossible for the identifier to be lost, stolen, duplicated, or given away (Liu & Silverman, 2001). This advantage makes biometric devices an appealing option for individuals and corporations that wish to adopt a new security technology.

The technology acceptance model (TAM) has received wide acceptance for studying the usage behavior of new technologies (Davis, 1989). We extend TAM to determine the intention to use security technologies, specifically biometric devices. We utilize a vignette-based survey design to study the user behavior toward biometrics and the intention to use these devices. This approach provides a general overview of individual's perceptions of biometrics regardless of the application area or device type; hence, providing insight into possible barriers of adoption of biometric technologies for security purposes. By focusing on factors that influence an individual's intention to use biometric technologies, we can explore the possible modes of adoption that may smooth the transition to new forms of security and authentication technologies. The literature suggests that barriers to adoption of biometric devices can be grouped into the following categories: physical invasiveness, information invasiveness, ease of use, privacy, and the perceived level of benefit from the device (Deane, Barrelle, Henderson, & Mahar, 1995; Liu & Silverman, 2001; Woodward, 1997). We posit that an individual's need for privacy and security along with the perceived invasiveness of the device and the original TAM

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/determining-intention-use-biometric-devices/18262

Related Content

Control Supply Chain Risks in Digital Transformation: A New Way to Improve Supply Chain Resilience

Yang Gao, Yubing Lengand Biaoan Shan (2022). *Journal of Organizational and End User Computing (pp. 1-18).*

www.irma-international.org/article/control-supply-chain-risks-in-digital-transformation/298680

Educating Our Students in Computer Application Concepts: A Case for Problem-Based Learning

Peter P. Mykytyn (2007). *Journal of Organizational and End User Computing (pp. 51-61).*

www.irma-international.org/article/educating-our-students-computer-application/3822

A Generic Context Interpreter for Pervasive Context-Aware Systems

Been-Chian Chienand Shiang-Yi He (2013). *Mobile and Handheld Computing Solutions for Organizations and End-Users (pp. 308-321).*

www.irma-international.org/chapter/generic-context-interpreter-pervasive-context/73219

Privacy, Risk Perception, and Expert Online Behavior: An Exploratory Study of Household End Users

Judy Drennan, Gillian Sullivan Sullivanand Josephine Previte (2008). *End-User Computing: Concepts, Methodologies, Tools, and Applications (pp. 1-18).*

www.irma-international.org/chapter/privacy-risk-perception-expert-online/18165

A Markup Approach to Surveys and Questionnaires

Jeffrey Hsuand Murray Turoff (1996). *Journal of End User Computing (pp. 20-27).*

www.irma-international.org/article/markup-approach-surveys-questionnaires/55734