Chapter 1.5
How Safe Is Your Identity?
Security Threats, Data Mining, and Digital Fingerprints/Footprints

Bobbe Baggio
La Salle University, USA

Yoany Beldarrain
La Salle University, USA

ABSTRACT

Digitally mediated communications offer ease and flexibility to exchange information across a networked global community. All interactions could potentially be captured however, using different invasive technologies for spoofing, phishing, data mining, profiling, and tracking an individual's digital fingerprints and footprints. Ultimately, the exposure of private information not only compromises an individual's identity, security, and privacy, but also the security of organizations and governments. Nonetheless, these same technologies present unique opportunities for cyber educators to track and monitor, within e-learning platforms, the activities of students with the goal of using this data to improve the learning experience for the benefit of all learners.

OBJECTIVES

- Describe data mining, profiling, spoofing, phishing, digital fingerprinting, digital footprints and other terms unique to privacy and anonymity concerns in the online environment.
- Analyze the detrimental and potentially positive effects of the digital trails learners leave in online learning.
- Identify the diametrically opposing positions of FERPA and the USA PATRIOT Act
- Recognize the variety of threats that may be present to learner privacy and identity in the online environment.

DOI: 10.4018/978-1-61350-323-2.ch1.5

- Discuss security trends, threats, and safeguards that affect e-learning.

INTRODUCTION

Privacy and anonymity co-exist in the realm of digitally mediated communications. Increased connectivity increases the risks of security threats to individuals as well as organizations and governments. Besides the well known threats posed by worms, viruses, Trojans and the like, other dangers may come in the form of email spoofing and phishing or in the form of tracking an individual's whereabouts. Lack of awareness of these threats often results in breaches that affect individuals as well as organizations.

With every click, a person's digital trail is captured. These data can be gathered and analyzed for any particular intent or purpose. Aside from compromising a person's identity, the visibility brought about by social networking tools diminishes the protection that would otherwise be offered by anonymity. Anyone, including employers, collection agencies, friend or foe, could locate information about an individual and make inferences about their preferences, personality, and character. The growing digital trail may be used to conceptualize a person's morality and ethics.

These same invasive technologies that are used to pry into private information could potentially be applied to cyber education. Although the danger of misusing learner information remains a concern, the prospective benefits of data mining and tracking digital fingerprints and footprints within e-learning platforms hint at improving distance learning programs. This chapter discusses key definitions and then explores the harms as well as the potential benefits of data mining, profiling and tracking of digital fingerprints and footprints.

BACKGROUND

Privacy and anonymity are inextricably mixed. Anonymity may be defined as the absence of identity and privacy as the ability to be apart from and unidentified by, others. The right to private communications and freedom of speech is guaranteed in the United States Constitution, yet digital privacy and true anonymity remain both misleading and elusive. Donald Kerr, Deputy Director of National Intelligence in the United States tells us "privacy no longer can mean anonymity" (Bradner, 2007, p.26). Privacy is now subject to a new interpretation according to Kerr, which has impelled government and business agencies to make attempts at safeguarding our private communications. Digitally mediated communications, whether used for business, personal or educational purposes, open the door to security threats such as spoofing, phishing, data mining and the capture of digital fingerprints and footprints. There is promise that these invasive technologies may be used to capture information about the individual learner. If used properly, these same technologies may help cyber educators not only personalize the learning experience, but also focus on student achievement.

Fear, misconduct and improper use of technologies surface occasionally only to be suppressed by the mesmerizing appeal of communicating online. An overwhelming 60% of Internet users in the United States do not necessarily worry about how much of their personal information is available online (Madden, Fox, Smith, & Vitak, 2007). This lack of concern affects not only individuals, but also eventually impacts organizations and institutions. With the increased use of social networking sites, especially by the Millennials (those born between 1980 and 2000), it would be expected that it is the younger generation that is not concerned about protecting their online identity. Surprisingly, the opposite is true. According to the Pew Internet Project, 55% of teens have