Introduction

In the wake of privacy controversies at Facebook, Google and other Internet service companies, this research attempts to better understand the importance of identity protection and privacy for consumers when using social media tools such as social networks, social messaging or texting, social video and so forth. In the context of this research social media is defined as media used to converse and interact with groups of people (a.k.a. communities) online. Here, media means digital words, pictures, video and even sound shared via the Internet.

About our study

Our study focuses on adult-aged consumers who use social media tools. We examine the importance of privacy and concerns about identity theft while using social media. Our study examines two independent samples: One representing adult Internet users residing in the United States; the other includes known identity theft victims also residing in the United States. Using a web-based survey instrument, we completed this research on June 2, 2010. Our general sample of consumers contains 698 respondents and the ID theft sample contains 567 respondents, for a total combined sample of 1,265.

Key findings

- We anticipated that individuals experiencing identity theft would be more cautious users of social media tools such as social networks, social messaging or texting, location tracking applications and many others. However, in our study, consumers who experienced identity theft crimes behave no differently when using social media than ordinary US consumers.
- Respondents who are heavy users of social media are less likely to see the protection of privacy and security as more important than light social media users.
- In general, respondents are complacent about protecting their privacy and security when using social media. About 40 percent of respondents admit they do not take any steps to protect their privacy or security when using social media.
- Many respondents share sensitive pieces of information about themselves in social media, such as hobbies and interests, photos, video, names of friends and so forth.
- Despite the lack of precautions taken to protect privacy and security, respondents generally see identity theft as a severe consequence of insecure social media. Of least concern are Internet ads, spam and virus or malware infections.
- With respect to identity theft, respondents see online banking and Internet purchases as more dangerous environments for identity theft than social media environments such as location tracking, social networking, uploading video and so forth.
- A majority of respondents do have confidence that the social media provider will adequately protect their identity. They also lack confidence that the social media provider will limit or curtail imposters from joining network applications.
- A majority of respondents see the pitfalls of social media, especially including the revelation of secrets, the disclosure of unflattering facts with a present or future employer, and data helpful to would-be stalkers.
- Only a small number of respondents believe information shared within social media domains will be used to steal identity.
- Despite a lack of confidence in the social media provider’s ability to protect data, respondents see the social media company or government as the two most responsible parties for ensuring privacy and security. Only a small number of respondents believe it is their responsibility to protect themselves from privacy or security abuses.
- As another indication of complacency, most respondents say they would most likely continue using their favorite social media tools even if they learned that the company did not adequately protect their privacy or security.
Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.