Journal of Business & Leadership: Research, Practice, and Teaching (2005-2012)

Volume 3
Number 1 *Journal of Business & Leadership*

Article 26

1-1-2007

Computer Security Threats: Student Confidence In Their Knowledge of Common Threats

George Schmidt
University of Arkansas - Fort Smith

Margaret Tanner
University of Arkansas - Fort Smith

Thomas Hayes
University of Arkansas - Fort Smith

Schmidt, Tanner, Hayes
Journal of Computer Science Education, and Teaching
2007, Vol. 3, No. 1, 211-215

COMPUTER SECURITY THREATS: STUDENT CONFIDENCE IN THEIR KNOWLEDGE OF COMMON THREATS

George Schmidt, University of Arkansas - Fort Smith
Margaret Tanner, University of Arkansas - Fort Smith
Thomas Hayes, University of Arkansas - Fort Smith

This paper investigates the possible existence of overconfidence by business students in their knowledge of different types of malware that may be present in current computer information systems. This article focuses on the students' ability to understand and identify three main types: viruses, Trojans and spyware. The results are consistent with research suggesting that many students believe their computer knowledge is adequate (Weston and Barker, 2002), when the opposite may be true. Further, in an educational setting, students' overconfidence in their computer knowledge exacerbates the problem of faculty falsely assuming that students have adequate computer knowledge (Messineo and DeOllas, 2005).

INTRODUCTION

Over the past two decades, the development of computer technology has profoundly impacted virtually every part of our lives, from automobiles to education to home entertainment. For example, the proliferation of the Internet has forever changed the way we communicate. E-mails and instant messaging have replaced written memos and the telephone as the primary means of communication. At the same time, malware, such as viruses and spyware, has emerged to undermine further advancements and pose serious threats to personal and business information.

To address these concerns, it is important to have the knowledge and skills to deal with threats posed by such malicious software. Colleges and universities are a logical setting for individuals to learn about viruses and other forms of malware. Moreover, students in a college setting are expected to be proficient with computers as a necessary part of college life (Eisenberg & Johnson, 2002; Weston & Barker, 2002).

Interestingly, prior research suggests that faculty may falsely assume that students have adequate computer knowledge when in fact, the opposite may be true (Messineo and DeOllos, 2005). In turn, faculty will make assignments based on their expectations of students' technical competencies, which may negatively impact student success. To further complicate the issue, students tend to believe their computer skills are adequate to meet their instructors' needs (Weston and Barker, 2002). In other words, students may be overconfident in their abilities.

The purpose of this study is to examine whether or not students are overconfident with respect to their knowledge of various computer security threats (e.g., viruses). Students who are overconfident are more likely to be less prepared to face such threats in the workplace. Further, students' overconfidence exacerbates faculty misconceptions regarding student preparedness. Thus, results will be useful for faculty and administrators in designing curricula that adequately prepare students to enter the workforce.

Malware

Computer proficiency is essential to success at the college level (Eisenberg & Johnson, 2002; Weston & Barker, 2002). This proficiency should include a working knowledge of malware, including viruses and spyware. Several types of malware are considered in the current study; specifically, we are interested in viruses, Trojans, and spyware. A computer virus is a program that attaches itself to other computer programs, generally without the user's knowledge. Although a precise definition of computer viruses can be elusive, Crume (2000) provides a working definition of the term, which includes the following two criteria:

- the computer virus executes itself when the host program is run, and
- the computer virus replicates by attaching a copy of itself to other programs when it is executed

What makes viruses so insidious is their ability to spread throughout a host's computer before causing any noticeable damage (Hall, 2004). The type of damage varies considerably depending on the nature of the virus. Some viruses do minimal damage simply by taking up disk space or processing capacity, and that damage may even be accidental (Maximum Security, 2001). Most viruses, however, cause moderate to extensive damage. For example, boot sector viruses, spread from computer to computer via floppy disks, can ultimately prevent a host computer's operating system from working (Maximum Security, 2001). Macro viruses, which attack data files such as Microsoft Word documents, can result in significant loss of data (Maximum Security, 2001). These macro viruses are particularly damaging when sent via email. Unsuspecting users may ultimately forward the infected message to many users, making containment of such viruses difficult (Crume, 2000).

Some viruses are especially dangerous because of their ability to overwrite hard drives and effectively wipe clean the Basic Input/Output System (BIOS) on a user's system. On modern computers, the BIOS, which contains the necessary commands to read and write to hard drives and other auxiliary equipment (e.g., keyboard), can be upgraded to recognize new input/output devices, such as an external hard drive (Crume, 2000). Several viruses, such as the CIH virus is programmed to wipe out the BIOS on a user's system, rendering the computer

Journal of Business & Leadership: Research, Practice, and Teaching
2007, Vol. 3, No. 1, 211-215

useless (Crume, 2000).

Although they are often considered a type of virus, Trojans are different in that they do not spread on their own. Like viruses, they do contain malicious code, but unlike viruses, they cannot replicate themselves (Crume, 2000). Trojans essentially spread from computer to computer under the guise of something harmless, usually as an e-mail attachment. For example, the ILOVEYOU Trojan arrived to unsuspecting users as an e-mail attachment. Once the user opened the seemingly harmless attachment, the Trojan would mail itself to anyone in the user's address book, consuming resources, and ultimately denying service to the user (Maiwald, 2003).

Spyware refers to a variety of programs that, once loaded on a user's computer, surreptitiously collect personal information and monitor web pages accessed by the user (Carvey, 2005). These spyware programs can enter into a computer several ways, for example, as attachments to freeware or shareware (Kucera et al., 2005). While spyware does not necessarily pose the same threats as viruses and Trojans, it can still have negative consequences for the user. For instance, spyware programs have the potential to collect not only relatively innocuous personal information, such as name, gender, and marital status (Kucera et al., 2005), but also potentially harmful information, such as social security and bank account numbers (Warkentin et al., 2005). Furthermore, certain spyware programs can inundate the user with unwanted information in the form of pop-up advertisements, redirect the user to spyware-affiliated websites, and even plant viruses and Trojans on the user's computer (Warkentin et al., 2005).

Most importantly, the emergence of such spyware programs raises serious concerns about individual privacy. Indeed, research suggests that individuals are concerned about their online privacy (Kucera et al., 2005; Dinev and Hart, 2004; Sheehan, 2002; Lohr, 2000). In addition, concerns about individual privacy are such that public policymakers are abandoning their laissez-faire approach to privacy protection, recognizing that the private sector has failed in its efforts to self-regulate (Kucera et al., 2005).

Overconfidence

Overconfidence in one's ability is a phenomenon that can be found in a broad range of literature. In fact, research suggests that overconfidence is a strong human tendency. For example, Arkes et al. (1986) suggest a link between overconfidence and decision aid reliance, finding that individuals tend to ignore the results of a decision aid (e.g., checklist or decision support system) in favor of their own judgment, even when their own judgment proved to be inaccurate.

Overconfidence is also found in business settings, such as capital markets. Specifically, investors tend to be overconfident in their abilities, which ultimately create inefficient markets (Ko & Huang, 2007; Chen et al., 2007). Moreover, research suggests that even entrepreneurs exhibit overconfidence, which may attribute to the high failure rate among new business owners (Koellinger et al., 2007).

Overconfidence is also prevalent in academic settings. Prior research (Clayson, 2005; Kennedy et al., 2002) finds that students tend to be overconfident in their abilities, overestimating their performance on exams. Moreover, as Kruger and Dunning (1999) suggest, if students don't realize their lack of knowledge, then teachers are faced with a quandary since they tend to only focus on teaching their particular subject (Kennedy et al., 2002). In other words, faculty may omit coverage of necessary skills or content areas which support student learning of a particular subject.

In the present study, we look at students' overconfidence in their knowledge of various malware, including viruses, Trojans, and spyware. Since many business students will play an important role in maintaining the integrity and reliability of company data (Hall, 2004), they are expected to have adequate knowledge of such computer security threats before they enter the workplace. Thus, it is important to understand whether or not students are overconfident in their knowledge of such threats. If students are overconfident, faculty face the additional challenges of helping students recognize their lack of knowledge in that area. Accordingly, we test the following proposition:

> Business students will be overconfident in their knowledge of computer security threats, specifically, viruses, Trojans, and spyware.

Methodology

Students in multiple sections of a junior-level Accounting Information Systems (AIS) course completed a survey and a test over malware. Sixty-four business students from a small, public University in the Mid-South participated in the study, which was conducted in two parts. First, students completed a survey that asked them to self-report their knowledge of various computer threats (e.g., viruses, spyware, etc.). Students also indicated whether or not they had taken a course that addressed computer security threats. Once they completed the first survey, students took a test to assess their actual knowledge of various computer threats. The test consisted of several multiple-choice questions related to viruses, Trojans, and spyware. In this set of questions, students were asked to recognize the characteristics and effects of trojans, spyware and viruses. The purpose was to determine if they could correctly distinguish between these three types of malware. The results of both instruments were compiled and are discussed in the next section.

Results

Table 1 presents descriptive statistics for participants' self-reported knowledge of computer threats. Although only 11% of the sample indicated they had taken an AIS class, 88% indicated they knew what viruses were and how they worked. Further, 80% indicated they knew what spyware was, and 42% said they were familiar with Trojans.

https://scholars.fhsu.edu/jbl/vol3/iss1/26
DOI: 10.58809/DPCR2816

Table 1

Survey Item	Answered "Yes"
Have you taken an AIS class before or a class that describes in detail computer malware?	11%
Are you a traditional student?	44%
Do you know what a computer virus is and what it does?	88%
Do you know what a computer Trojan is and what it does?	42%
Do you know what a computer spyware is and what it does?	80%

To test the proposition that students were overconfident with respect to their knowledge of computer threats (i.e., viruses, Trojans, and spyware), it was first necessary to develop a "passing" score for the second part of the study. For example, students answered several questions that assessed their knowledge of various computer threats, including viruses. For each type of threat, three different questions were included to test the student's knowledge. To achieve a passing score on an individual type of threat, a student had to correctly answer at least two of the three (67%) questions.

We calculated t-tests to determine if students' performance scores for viruses, Trojans, and spyware differed significantly from the passing score. Specifically, to test the overconfidence hypothesis, only those students who self-reported they knew about viruses, Trojans, and spyware were used. Table 2 below summarizes these results.

Table 2

Type of Malware	Number of students with knowledge	Mean score on test questions	Number of students without knowledge	Mean score on test questions
Virus	56	28%	8	13%
Trojans	27	9%	37	6%
Spyware	51	14%	13	10%

It is apparent that neither set of students performed particularly well on the test questions regarding computer threats. Of 64 participants, 56 (88%) indicated they knew about viruses. The average score on those test questions for those 56 students was 28%, which is significantly lower than a passing score of 67% ($t = -11.468$, $p < 0.001$). This result suggests that students were overconfident with respect to their knowledge of viruses. Further, a t-test was computed to determine if the scores of those students who indicated they knew about viruses differed from those students who indicated they did not know about viruses. The average score for those students who indicated they did not know about viruses was 13%, which does not differ significantly from the average score of those students who indicated they knew about viruses (28%; $t = 1.673$, $p = 0.099$). Namely, students who indicated they knew about viruses did not score significantly better than those students who indicated they did not know about viruses, lending additional support to the overconfidence proposition.

Of 64 participants, 27 (42%) self-reported knowledge of Trojans. The average score for those 27 students was 9%, which is significantly lower than the passing score of 67% ($t = -20.254$, $p < 0.001$). Similar to the above results for viruses, the results suggest that students were also overconfident with respect to their knowledge of Trojans. Further, a t-test was computed to determine if the scores of those students who indicated they knew about Trojans differed from those students who indicated they did not know about Trojans. The average score for those students who indicated they did not know about Trojans was 6%, which does not differ significantly from the average score of those students who indicated they knew about Trojans (9%; $t = 0.661$, $p = 0.511$). Namely, students who indicated they knew about Trojans did not score significantly better than those students who indicated they did not know about Trojans, lending additional support to the overconfidence proposition.

Of 64 participants, 51 (80%) self-reported they knew about spyware. The average score for those 51 students was 14%, which is significantly lower than the passing score of 67% ($t = -19.495$, $p < 0.001$). Similar to the above results for both viruses and Trojans, the results suggest that students were also overconfident with respect to their knowledge of spyware. Further, a t-test was computed to determine if the scores of those students who indicated they knew about spyware differed from those students who indicated they did not know about spyware. The average score for those students who indicated they did not know about spyware was 10%, which does not differ significantly from the average score of those students who indicated they knew about spyware (14%; $t = 0.679$, $p = 0.499$). Namely, students who indicated they knew about spyware did not score significantly better than those students who indicated they did not know about spyware, lending additional support to the overconfidence proposition.

Discussion and Implications

As the above results suggest, students tend to be overconfident with respect to their knowledge of several computer threats, namely, viruses, Trojans, and spyware. In fact, their performance on a test designed to assess their knowledge of such threats does not differ significantly from those students who indicated they did not know about these common types of computer security threats. These results are consistent with prior research that finds that individuals tend to be overconfident in many contexts. Additionally, the results are consistent with research suggesting that many students believe their computer knowledge is adequate (Weston and

Barker, 2002), when the opposite may be true.

Further, in an educational setting, students' overconfidence in their computer knowledge exacerbates the problem of faculty falsely assuming that students have adequate computer knowledge (Messineo and DeOllas, 2005). Specifically, if a faculty member assumes incorrectly that students have an adequate understanding of computer security threats, the students and/or their institutions may be vulnerable to costly security breaches. In addition, student learning will not be maximized if these threats and possible consequences are not discussed in the classroom.

If this lack of knowledge persists until such time that students are employed, further consequences may be realized in the business world. Larger companies typically have the resources to engage experts to help safeguard their computer systems. However, smaller businesses tend to rely on the knowledge of existing and new employees. If these employees do not have the requisite knowledge of such security threats, then their employers may face significant losses from damaged computer systems. Given that such overconfidence exists in potential new hires, small businesses would likely benefit from computer security services offered in their communities. This issue may provide an opportunity for computer security professionals to increase their range of services and clients.

Limitations and Future Research

Research in overconfidence (Kruger and Dunning, 1999) suggests that poor performance can be overcome by improving the skill level of participants. In future research, this proposition can be tested by conducting pre- and post-tests of the knowledge of computer security issues. In addition, it might be interesting to examine student overconfidence in other business disciplines. Does the degree of overconfidence vary across subject matter, for example? The answer to this question could have important implications for the content and pedagogy used within our programs.

Furthermore, because of the potential threats to small business computer systems, we plan to extend this research to determine if this overconfidence carries into the workplace. For example, do business owners or managers understand common computer security threats, or do they rely on others to protect their systems? In addition, one limitation of the present study is that we examined student knowledge with respect to only a few potential threats to computer security. There are other threats which could be examined as well. For example, do students and business people understand the threats that phishing or war driving attacks can pose? Furthermore, do they know how to protect their computers or systems from such attacks? Currently, there is no one piece of software that can detect all computer malware. Therefore, data and system security will continue to be a concern to individuals and businesses. Are we sure our students are adequately prepared to deal with these challenges?

REFERENCES

Arkes, H., Dawes, R., & Christensen, C. 1986. Factors influencing the use of a decision rule in a probabilistic task. **Organizational Behavior and Human Decision Processes,** 37: 93-110.

Carvey, H. 2005. **Windows forensics and incident recovery.** Boston, MA: Addison-Wesley.

Chen, G., Kim, K., Nofsinger, J., & Rui, O. 2007. Trading performance, disposition effect, overconfidence, representativeness bias, and experience of emerging market investors. **Journal of Behavioral Decision Making,** 20: 425-451.

Clayson, D. 2005. Performance overconfidence: Metacognitive effects or misplaced student expectations? **Journal of Marketing Education,** 27: 122-129.

Crume, J. 2000. **Inside internet security.** London: Addison-Wesley.

Dinev, T., & Hart, P. 2004. Internet privacy concerns and their antecedents - measurement validity and a regression model. **Behaviour & Information Technology,** 23: 413-422.

Eisenberg, M., & Johnson, D. 2002. **Learning and teaching information technology - computer skills in context.** ERIC Document Reproduction Service No. ED465377.

Hall, J. 2004. **Accounting information systems**. Mason, OH: Thomson South-Western.

Kennedy, E., Lawton, L., & Plumlee, E. 2002. Blissful ignorance: The problem of unrecognized incompetence and academic performance. **Journal of Marketing Education,** 24: 243-252.

Kruger, J., & Dunning, D. 1999. Unskillled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. **Journal of Personality and Social Psychology,** 77: 1121-1134.

Ko, K., & Huang, Z. 2007. Arrogance can be a virtue: Overconfidence, information acquisition, and market efficiency. **Journal of Financial Economics,** 84: 529-560.

Koellinger, P., Minniti, M., & Schade, C. 2007. I think I can, I think I can: Overconfidence and entrepreneurial behavior. **Journal of Economic Psychology,** 28: 502-527.

Kucera, K., Plaisent, M., Bernard, P., & Maguiraga, L. 2005. An empirical investigation of the prevalence of spyware in internet shareware and freeware distributions. **Journal of Enterprise Information Management,** 18: 697- 708.

Lohr, S. 2000. Survey shows few trust promises on online privacy. **The New York Times,** April 17: C4.

Maiwald, E. 2003. **Network Security: A Beginner's Guide.** New York: McGraw-Hill.

Shipley, G. 2001. **Maximum security.** Indianapolis, IN: Sams

https://scholars.fhsu.edu/jbl/vol3/iss1/26
DOI: 10.58809/DPCR2816

Publishing.

Messineo, M., & DeOllos, I. 2005. Are we assuming too much? **College Teaching,** 53: 50-55.

Sheehan, K. 2002. Toward a typology of internet users and online privacy concerns. **The Information Society,** 18: 21-32.

Warkentin, M., Luo, X., & Templeton, G. 2005. A framework for spyware assessment. **Communications of the ACM,** 48: 79-84.

Weston, T., & Barker, L. 2002. A profile of student computer use, training, and proficiency. **Journal of Computing in Higher Education,** 14: 87-112.

George Schmidt is an associate professor of accounting at the University of Arkansas - Fort Smith. He received his Ph.D. from the University of North Texas. His research interest focuses on financial and information systems areas.

Margaret Tanner is an associate professor of accounting at the University of Arkansas - Fort Smith. She received her Ph.D. in Accounting from the University of North Texas. Her research interests include pedagogical issues, financial reporting, and curriculum development and assessment.

Thomas Hayes is an assistant professor of accounting at the University of Arkansas - Fort Smith. He received his Ph.D. from the University of North Texas. His research interests include auditing and information systems areas.