Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

Approaching Identity Theft in Education from an Interdisciplinary Perspective

Susan Helser and Denise McKernan, *Davenport University*

***Abstract* - The focus of this paper is to discuss observations and common issues that exist with respect to information assurance in rural and urban environments. Due to an often limited prior exposure to computer technology before starting college, students in rural and urban areas begin their studies with an experience deficit that provides an easy attack vector for *identity thieves* to exploit. In addition to potentially significant personal harm to the individual, losses that result have a negative impact on society. We propose an interdisciplinary approach to address the problem that incorporates the use of case studies to promote discussion and awareness in at risk student populations.**

Index of Terms – Identity theft, privacy issues information assurance in education, rural and urban student populations

I. OVERVIEW

Davenport University (DU) is a multi-ethnic, private institution with an enrollment of approximately 12,000. DU focuses on preparing students for careers in three main areas that include business, health and technology. Students attend multiple campuses located in the state of Michigan and online. Davenport University's School of Technology offers a number of degree options at the undergraduate and graduate levels in computer related technologies. Areas of study include security, programming and information systems/information technology management. Currently, the School of Technology is in the process of pursuing the second security certification level rating of Center of Academic Excellence (CAE) awarded by the National Security Agency (NSA). [1] Within the computer security area students have choices of study that include concentrations in biometric security, information assurance (IA), and network security. Programs are designed to provide students with firsthand experience in the classroom working with tools used in the field as well as opportunities for experiential learning in the form of internships or service learning. Members of the School of Technology faculty who teach IA content are involved in community based outreach programs to assist in educating the general public. [2]

The authors' work at DU includes teaching mathematics and technology courses, guest speaking at area schools on IA and in assisting students in the library with learning how to access and use print and non-print resources. Because the use of technology is integrated into the curriculum across DU, students are exposed to computers on a daily basis. Students who come to DU from rural and urban areas may be unfamiliar with computers and related technologies and are, consequently, unaware of the potential risks that they face when using them. [3] Students can fall victim to *identity theft* which is a fast growing crime that also affects individuals, businesses and economies across the globe. [4] Technical solutions address some aspects of the problem, but the human factor is multi-faceted and, thus, requires a suitable and robust approach to mitigate the crime. In our experience in education we have observed common issues that relate to a lack of exposure, information and understanding of the use of computer technology in low income rural and urban student populations. This deficit effectively supports an open door for abuse by *identity thieves.* The lack of knowledge in student populations contributes to misconceptions that flourish. [5] [6] [7] *Identity thieves* are quick to capitalize on these vulnerabilities and then exploit students in rural and urban areas. In our professional work with students we regularly address and integrate the secure use of computer technology. Whether in the library when accessing online resources and doing research or in the classroom teaching students about hardware or software it is imperative that appropriate measures that relate to sound information assurance practices be stressed. We have found that addressing issues as they arise coupled with the use of explanatory examples has benefited students' understanding. [8] [9] [10]

II. INTRODUCTION

America has gone digital – from TV watching to exercise, education to government, it is nearly impossible to find an aspect of our lives that is not influenced by or dependent upon electronic technology.

For those who would choose to avoid this shift from paper-based to digital – be if from lack of experience and resources or personal preference – they are forced to participate by academic, professional, social and governmental institutions. In the age of online classes and registration, professional and social networking, information databases, job search banks and, ultimately, online tax filing, it is increasingly difficult to excuse oneself (and in some states for tax purposes, illegal) from utilizing internet services.

The push for electronic information has been strong….The rate at which we progress toward an exclusively digital society is also the rate at which we put

ourselves at risk for violations of privacy, *identity theft* and other serious crimes. Without a proper education regarding the risks of Internet use, Americans are vulnerable. [11]

Academia has accepted the Digital Age, in many cases with arms wide open. We offer online courses, registration, even student and library services. We ask students to trust that we will protect their privacy and financial information, and that we will adhere to every law regarding these issues. Many students, of all ages, backgrounds and gender, accept this without question – just as they accept the same of their social networking sites, departments of local, state and federal government, commercial websites and non-profit institutions. There is a trust that exists, be it in individual people, departments, and institutions – or in the legal aspects of protection. There is an innocence and ignorance in the way many students approach the Internet and the information they either voluntarily share, or involuntarily agree to sharing – and in turn, a vulnerability that students need to be made aware about.

This paper is organized in the following manner and includes an Overview, Introduction, Case Studies, Future Work, Conclusion and References. The Introduction addresses our concerns and common observations as well as how we incorporate Case Studies into our work with students. The Case Studies consider a variety of examples of problems that are the result of a lack of student understanding and represent a composite of the issues that we have observed. We use similar examples in our work with students to generate thoughtful discussion that supports learning about the risk of *identity theft*. The section on Future Work examines several other forums in which we plan to expand awareness of the issues outlined in this paper. The Conclusion discusses our combined observations working with students in rural and urban environments. References follow.

III. CASE STUDIES

We have found that direct and open dialogue about the risks associated with online resources to be effective with relatively small groups of students. We incorporate the use of relevant and timely examples to promote discussion and better understanding. Scenarios are presented in the form of case studies and reflect events and incidents that relate to students. Fairly often at least one member of a discussion group will indicate that she/he either has been subjected to *identity theft* or knows of someone else who has been. In some cases, students do not believe that they could become a victim of *identity theft*. [9] In fact, students often believe that, because of their modest means, that they have nothing of value that anyone would want to steal. This misconception is far from the truth and we believe helps to fuel the growing problem of *identity theft*. Students are often surprised to learn that their *identities* become more valuable over time. In addition, we believe that inherent cultural differences impact students' behavior and decisions. For example, in many rural communities it is a common practice is to leave doors to homes and automobiles unlocked. Because of the level of trust that exists in these communities, we believe that students who come to school with this understanding of the world are at significant risk of becoming victims of *identity theft* when they log on to online resources. The exchange between students in a small group setting can be an eye opener for some class members. Because the interaction is peer-based, we believe that it tends to be more plausible to students. Clearly, the students who benefit most are those who have little or no prior experience dealing with issues that involve *identity theft.* We believe that the less formal method of engaging students in conversation through the use of case studies lends itself to the dissemination of information.

In a typical student information session we open by defining *identity theft* and then discuss some possible outcomes. If the group is of sufficient size, we divide it into smaller subgroups prior to the distribution of case studies. We believe that smaller groups promote and facilitate good communication and participation among members. Each group receives copies of a single case study and is instructed to read the scenario and then to discuss it with fellow group members. If multiple groups with the same case study exist, they are instructed to come together as a larger group to share their thoughts and ideas about the scenario. Following this level of discussion a representative is selected for each case study. This individual then summarizes the incident as well as the subsequent associated dialogue and presents it to the larger group. After all of the case studies have been discussed the facilitator encourages the group to address issues that have been presented. Underlying threads emerge that suggest common and related issues. Once the key points have been addressed the facilitator draws the information together and then wraps up the discussion. Generally, students are awestruck to learn how easily they can be exploited

We have included several example case studies here for the benefit of the reader. All scenarios are fictitious and are the result of blending multiple experiences into a single example.

CASE 1: JANE'S STORY

At the start of period the instructor polled the class about a variety of current technology terms. This week popular vocabulary was the focus of the session. The mid-class discussions had become an integral part of the course. The instructor had worked in the IT/IS industry and realized the importance of students learning key terms and phrases. Different topics were discussed. The focus this time was on *identity theft.* The instructor asked the class to define the term. Several students responded. The instructor then asked what could happen if a student left the computer that she/he was working on in the lab to go

for a sandwich, pop, or some other activity. Students replied and voiced concerns stating that work might be disturbed, deleted or copied without their knowledge. In the minds of the class, the worst thing that could happen would be that their work would be lost. The instructor took the opportunity to discuss the possibility that *identity theft* could occur. It was certainly true that the student's work might be affected, but it was also the case that a great amount of the student's personal information which was stored on the university's computer system was available and of value to the *identity thief.* In addition, the email utility used in *phishing* attacks could be exploited by an *identity thief.* The instructor explained that bogus or harmful email could be sent out under the name of the student whose computer was accessible and was compromised. The information amazed the students. They were unaware of the many scams that could be perpetrated in their names because they had gotten up to go for a cup of coffee. The possibilities incensed the students. A lively discussion followed. The instructor was pleased and knew it had been a good day. While it was clear that some of the students believed that *identity theft* would never impact them, some had realized the devastating possibilities and had vowed to be more careful. It was a positive start and one that had made a difference.

After the break the instructor returned to the issue of *identity theft*. Students were encouraged to participate and to share their ideas, thoughts, opinions and experiences. Jane volunteered that she had received numerous statements from one of the major utility companies that indicated that she was in arrears and that many months of unpaid bills were outstanding. Jane had interpreted the notices as scams and had continued to ignore them. She said that it was true that she had lived in the community in question years earlier as a child, but that her family had moved away from the area when she was very young. Jane said that since that time she had lived in the community where she currently resided and had not returned to the earlier neighborhood. Because she had not returned to her childhood community, she believed that the utility company or some other entity posing as the utility company was trying to hoodwink her. Jane insisted that whoever was responsible was attempting to take advantage of her. She was belligerent and said that she would not fall for the trick. The instructor explained that there was a strong possibility that Jane had become a victim of *identity theft* and that the bills were, in fact, very real. An *identity thief* using Jane's identity had mostly likely racked up bills in her name. Perhaps the thief had started recently or had been using Jane's identity for some time, but had been paying the bills. The instructor continued and said that ignoring the statements the utility company had mailed was not a solution to the problem and would only result in more damage to Jane's credit report. Because it was likely that the utility truly believed Jane had a substantial unpaid balance, she would need to communicate directly with the business to straighten out the issue. In order to mitigate the problem, Jane would need to take a proactive role and to explain her position to the company. The instructor encouraged Jane to follow up with the utility as quickly as possible and to not ignore additional statements. The problem would continue without intervention on Jane's part and would actually worsen. The instructor explained that if nothing was done, that ultimately Jane would find it difficult, if not impossible, to get credit. In addition, if Jane was able to get credit in the future, interest rates would be set based on her problematic credit rating which would continue to follow her. Jane and her classmates were astounded at the instructor's remarks and found it incredible that they could be held accountable, disciplined or penalized because of the actions of an *identity thief.* The instructor told the students how to check their credit bureau reports and urged them to do so routinely. After the students' questions had been answered, the instructor wrapped up the conversation. It had been a good day.

CASE 2: ADAM'S STORY

Adam, a forty-five year old local sales representative for a large metropolitan telephone company, decided to begin a Master of Business Administration to further his career. Although familiar with standard practices and procedures in a business setting, Adam had never enrolled in online courses and was about to begin a two year program exclusively online. A professional who had always valued his independence, Adam made plans to stop by the university campus to become familiar with the online course system the next day.

The next day, his first as an online student, he sought help from anyone he could find in the college computer lab to assist him with the automated course registration. Student lab technicians advised him to seek assistance from his academic advisor, but he was insistent that he could handle the issue by himself. In his frustration and in spite of years of experience in business and protecting people's privacy, Adam freely shared his personal and financial information with well-intentioned classmates who assisted him. At the end of the day, after he had tried to familiarize himself with the online classroom programs and registration, he surrendered with the intention of contacting his academic advisor the next day.

That night, at the university computer lab, someone logged into the system with Adam's username and password and registered him for several courses; changed his contact information; and visited websites that violated student user agreements. The automated university bill pay system withdrew course fees from his bank account and sent a financial statement to a new address in the system. Adam was locked out of the system for visiting pornography sites. The next several weeks he spent trying to sort out the problem, prevent further unauthorized activity and defending himself against academic probation.

CASE 3: ABBY'S STORY

In 2008, Abbey, a young single mother of two, had recently begun classes at a local business college to earn a degree in Nursing. She had relocated to a rural area of in order to distance herself from her former life in another part of the country and was trying to start anew for the sake of her young children, ages four and seven. Although she had been out of school for several years, was working part-time at a local gift shop, and had never used a computer for anything more than communicating with her extended family and designing greeting cards, Abby was determined to succeed.

As she had previously been a stay-at-home mother, reliant upon her husband for support, Abby was unsure how to approach household finances. After seeking the advice of a social services professional, Abbey began to organize and evaluate her personal finances and credit. In the process, she used an Internet company with popular and catchy advertisements that promised free credit reporting. The company website prompted her to provide credit card, bank account and other personal and financial information in order to offer official and up-to-the-minute credit reports from three major credit-reporting agencies. When no report resulted and the page timed out, she assumed there had been a glitch, and forgot all about it. Two months later, a sizeable charge appeared on her credit card for the reporting company, as well as further unapproved charges, which generally appeared unrelated.

Stressed and upset, Abbey consulted the librarian at her university about these issues. The student was shocked to learn that most credible businesses never require a client to provide such extensive, sensitive and private information – particularly on an unsecured website - and that any company that practices this needs to be reported to authorities immediately. Abby was also advised to contact her bank, and credit card companies to stop all cards and recent charges. Over the course of two years, Abby faced financial issues that devastated her 'fresh start' and forced her to put her academic pursuits on hold.

IV. FUTURE WORK

Because of the clear need to address the issue of the lack of non-traditional student knowledge and the negative and often significant impact that it has on them, we are currently in the process of putting together formal presentations that can be readily distributed to students and to members of the faculty. Related documentation will accompany an audio enhanced PowerPoint geared to the respective audiences. We have chosen PowerPoint as a delivery medium since its small file size requires little computer resources such as bandwidth. Our goal is to get information to people quickly and efficiently.

For example, rural students' ability to access the Internet at locations outside of the University is an issue in and of itself. Service is limited and often quite costly. Currently, in many rural settings only dial-up is available and/or affordable. While dial-up service can be purchased for approximately $10/month, if high speed wireless service is available, it may cost several times as much as dial-up and is not an option for the our student population. For this reason, a file that can be sent as an email attachment or downloaded easily has great value.

Similarly, in a significant number of urban settings, students do not own a computer or have personal Internet access. They must go to a relative's or friend's home to access online resources. Often these students, on entering a college computer lab for the first time, will ask the instructor for advice about the type of computer to purchase. Clearly, it is important that the students get useful and sound information prior to making such a purchase and that their initial experience is not tainted by a first-hand experience of *identity theft.* Again, because resources are generally limited in this student population a small file is a benefit.

In the case of resources for instructors, the material will be very portable and easy to distribute for the same reason. We believe that the development of an instructional tool for faculty members to use in their classrooms to assist with the dissemination of information about the topic of *identity theft* will benefit students in the at risk population that we have identified. It is

V. CONCLUSION

In conclusion, we have discussed our observations as they relate to the issue of the lack of knowledge and related vulnerabilities associated with *identity theft* among college students, and in particular rural and urban populations. A significant number of low income students begin college without prior knowledge or understanding of the risks that are inherent with online tools, resources and communication. In the time that we have worked with students in these environments, we have observed that their prior experience before entering the University in dealing with computer technology is often limited at best. Because of this lack of background, we believe that students from these areas are vulnerable to exploitation by *identity thieves.* We have seen that in a significant number of cases, one seemly helpful and friendly individual can quickly gain ready access to unique account information at the University that makes it possible to adopt the student victim's identity. At that point it is possible to establish bogus relationships based on the initial fraud. Clearly, this problem is not unique to low income rural and urban populations as it has become a major issue of concert in the wider society as a whole. Along with the personal tragedy suffered by the individual, *identity theft* undermines the general economy due to the sheer amount of losses that are accrued because of fraud. We believe, based on our experience with low income student populations from rural and urban areas, that they are particularly susceptible to

exploitation since they often enter the classroom with little prior knowledge of computers and a host of misconceptions that provides fertile ground for *identity thieves.*

For the reasons that we have outlined in this paper in addition to IA coursework and community outreach programs sponsored by DU to educate the public, we have made a conscientious choice to address the issues stated here about *identity theft* to students whenever the opportunity presents itself whether it is in a classroom setting or in the library. In either case, students have direct access to online resources as well as pitfalls that are afforded via the Internet. We consider these challenges as opportunities to inform our students of the risks that are present. We have developed an instructional methodology that incorporates the use of Case Studies to promote learning and to generate discussion in an effort to expedite student understanding.

In addition, we have set forth to *take our program on the road* via the Internet highway in the form of easy to distribute informational tools created in PowerPoint to provide material to students and faculty members about the very real risks inherent with *identity theft.* We plan to demonstrate our tool in PowerPoint in a DU informational meeting for faculty in the near future. Faculty will, in turn, be able to reach a greater number of students and inform them of the potential problems that are possible from only a few keystrokes. Our work will continue in this direction, because it is our belief that education is a key component in combating the increasing and devastating crime of *identity theft.*

VI. REFERENCES

[1] National Centers of Academic Excellence [website]. Retrieved April 13, 2010 from http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

[2] Helen Schneider, Loren Wagner, "Information Assurance Awareness: Partnership between Students and Community", Proceedings of the 13th Colloquium for Information Security Education (CISSE '09), pp. 71-75 (2009).

[3] John Winterdyk, Nikki Thompson, "Student and Non-Student Perceptions and Awareness of Identity Theft", CJCCJ/RCCJP, pp. 153-186 (2008).

[4] Federal Trade Commission – 2006 Identity Theft Survey Report [website]. Retrieved April 13, 2010 from http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

[5] R. Mecuri, "Scoping Identity Theft", *Communications of the ACM*. Volume 49, Issue 5, May 2006.

[6] J. E. Potter, Postmaster General and CEO United States Postal Service. (2008). February letter to postal customers warning of identity theft

[7] Stephan Schmidt, M. McCoy, (2005). *Who Is You? The Coming Epidemic of Identity Theft*. The Consortium

[8] Mohamed Chouchane, "Injecting Information Security in Core CS Courses: Methods, Challenges and Impact", Proceedings of the 13th Colloquium for Information Security Education (CISSE '09), pp. 38-43 (2009).

[9] William Conkling, George Trawick, J.A. Hamilton, "Engaging Students through and Information Assurance Exercise", Proceedings of the 13th Colloquium for Information Security Education (CISSE '09), pp. 51-58 (2009).

[10] W. Wang. Y. Yuan. N. Archer, "A Contextual Framework for Combating Identity Theft". IEEE, 1544-7993/06, 2006

[11] Anthony William. (2004). *Digital Nation: Toward an Inclusive Information Society.* Cambridge, Massachusetts: Massachusetts Institute of Technology Press