

# It's Eleven O'Clock: Do You Know Where Your Identity Is?

Elizabeth A. Evans  
UNC Chapel Hill  
CB # 1135  
Chapel Hill, NC 27599-1135  
1-919-698-8755  
evans@unc.edu

Carolyn M. Kotlas  
UNC Chapel Hill  
CB # 3420  
Chapel Hill, NC 27599-3420  
1-919-962-9287  
kotlas@email.unc.edu

Donna W. Bailey  
UNC Chapel Hill  
CB # 3470  
Chapel Hill, NC 27599-3470  
1-919-966-1289  
dbailey1@email.unc.edu

Abe J. Crystal  
UNC Chapel Hill  
CB # 3360  
Chapel Hill, NC 27599-3360  
1-919-593-6129  
abe@unc.edu

Terri Buckner  
UNC Chapel Hill  
CB # 3500  
Chapel Hill, NC 27599-3500  
1-919-843-6865  
tbuckner@email.unc.edu

## ABSTRACT

Identity theft continues to be a growing problem in our society. This paper describes a poster session that will give attendees the opportunity to consider identity issues related to campus life and how we might better educate our campus communities. We will describe what identity means, ways in which it might be abused in our campus environments, and how to balance risks and benefits. We will also provide tips on how faculty, staff, and students can better protect themselves and others. All attendees will be asked to complete an anonymous checklist to gauge how well we, as computer support professionals, protect our identities. The poster content is based on a symposium held in February 2004 on the UNC Chapel Hill campus.

## Categories and Subject Descriptors

K.4.2 [Computers and Society]: Social Issues – *Abuse and crime involving computers.*

## General Terms

Management, Security

## Keywords

Identity abuse, identity theft

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SIGUCCS '04, October 10-13, 2004, Baltimore, Maryland, USA, Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

## 1. INTRODUCTION

*Better Homes & Gardens. The Chronicle of Higher Education. The Washington Post. Communications of the ACM. PC Magazine.*

What do all of these have in common?

In the past year, all have featured articles about the risk of identity theft [1-5]. These articles (like many others) are focused on the specter of financial disaster. They caution readers to shred credit card offers, to protect Social Security numbers, to refuse information requests from telemarketers and salespersons, and to consider carefully all requests for personal information.

As these articles indicate, identity theft is a pervasive problem. We will broaden the focus to consider the potential of what we call “identity abuse” on campus. We define identity abuse as the act of someone pretending to be someone else. Identity abuse may involve only a single act—perhaps signing an anonymous discussion forum posting with someone else’s name. Or it may be embedded in familiar habits, such as sharing passwords with friends and colleagues. We read about and hear about the need to protect our identities almost daily; this poster will help identify issues and questions and provide some specific suggestions for better education about those issues and questions on campuses.

## 2. WHAT IS IDENTITY?

The first thing to do as we address identity abuse is to define what “identity” is. Although we could debate the philosophical meaning of identity, our purpose is more pragmatic. Therefore, we define identity as one or more pieces of information that may cause others to believe they know who someone is. Examples include a login name and password; an ATM card and PIN; or, for many of us in the campus environment, simply a name.

### 3. THE BALANCING ACT

#### 3.1 Openness or privacy?

Universities are built around the creation and dissemination of knowledge through open inquiry and investigation. Information sharing is at the core of our existence. If we impose too many barriers to access information, our universities fail to fulfill their missions—but if we make information too freely available, we risk rampant abuse. How can we negotiate this tension between the tradition of access and the need for protection?

We believe that whenever information is shared, the risks and benefits of doing so must be weighed.

#### 3.2 People or technology?

How much of our protection depends upon personal responsibility and how much can be provided for us by technology? Again, there are no easy answers. We each carry a responsibility for protecting ourselves as well as our colleagues and our students. Nevertheless, there are technologies that help. Virus protection software, strong password requirements, and data encryption, among other approaches, provide some protection. But if virus definitions are not kept up-to-date, if users write down their passwords, if data are left unencrypted and a laptop is lost or stolen, the technologies fail. Technology is constrained by personal behavior and social context. We will identify practices and examples that will help *people* use *technology* more securely.

### 4. IDENTITY ABUSE ON CAMPUS

#### 4.1 What?

What are the opportunities for identity abuse on campus? We mentioned two examples earlier: signing an anonymous discussion forum posting with someone else's name and sharing passwords with friends and colleagues. Other examples include subscribing to a listserver using another person's email address; entering someone else's address onto a Web site; or providing information (whether true or false) about someone on the Web which then becomes available via search engines (and so is archived, copied, and distributed further). Many of these abuses require knowing nothing more than publicly-available information: name, email address, perhaps a home address and phone number.

Abuse possibilities expand dramatically once a login name and password are known. Email can be sent *as* the person; online quizzes can be submitted; non-anonymous writings can be posted to discussion forums; student grades can be displayed; files can be viewed, copied, or transferred. Despite these (and many other) risks, people persist in sharing their login names and passwords or in writing them down where they can be discovered.

#### 4.2 Why?

Given the risks, why do people continue to engage in behaviors that might enable abuse of their identities? And what can we do to convince them to change their behaviors?

We believe that many times, people who share identifying information about themselves are naïve. They either believe that the person with whom they are sharing the information can be trusted not to abuse it, or they fail to imagine how the information might be abused. They frequently believe they need to share the

information to accomplish some work-related task. We have no research data to support this, but we repeatedly hear such reasons on our campus. Our efforts to educate people *not* to share such information include opportunities to debate the risks and benefits. For an administrator, the need to have someone check mail while she is out of town may seem imperative. She may not realize there are other, more secure options. She may not consider that giving a login name and password for email access may *also* give access to other resources such as student grades (if the administrator also teaches), retirement accounts, and files.

Our responsibility for educating our campuses is multifaceted. We may never be able to stop people from trying to engage in identity abuse. But we believe we *can* decrease the opportunities by doing a better job of 1) convincing faculty, staff, and students to protect identifying information better and 2) helping them find more secure ways of getting their work done.

### 5. USING TECHNOLOGY MORE SECURELY

At the symposium, we used several methods to convince people of the risks of exposing their identities. We presented scenarios as starting points for discussion. For example, one story described an administrator who was planning to be away from campus for the summer and needed to ensure that her email was handled while she was gone. Each scenario led the attendees to weigh the trade-offs involved. Should the administrator give her login name and password to a trusted administrative assistant to process her mail for the summer? What would happen if the assistant left his job during the summer? Was it likely that the assistant would also have access to student grades with the same login name and password and what issues, if any, did that possibility raise? What other ways of meeting the need are there in our campus environment?

We also presented the results of a survey we distributed at the beginning of the symposium. (The survey is the same one we will ask poster attendees to complete.) The survey revealed some serious inconsistencies in attendees' behaviors. For example, almost nobody who attended the symposium carried their Social Security card with them. However, many people carried a health insurance card (for our state health plan) that uses their Social Security number as the identifier.

Another section of the symposium described what information can be found about people on the Internet for little or no money. Given minimal details (some combination of name, some or all of the address, telephone number, and/or date of birth), information such as county tax records, voter registration, family members, and tax liens can easily be gathered. Many attendees at the symposium were surprised to find some local tax records included photographs of houses in the county along with the basic tax information. The liveliest discussion during this part of the symposium centered on whether it does any *harm* for some of the information to be readily available. The discussion illustrated the symposium's theme of "balance"—weighing the risks and benefits of information availability.

The final section of the symposium offered concrete examples of privacy incidents that had occurred on our campus and on other campuses. Some other campuses have experienced large data thefts including personal information such as Social Security

numbers, credit card numbers, passport numbers, and birthdates. On our campus, we have had reports of virus-infected computers mailing files from the computer to everybody in an address book. One person used his computer to complete his tax return. When his computer was infected with a virus, the tax return was mailed to hundreds of people. The tax return included, of course, his Social Security number. In another case, medical information was mailed because the physician had chosen to keep a shadow copy of health-related information on her personal computer. The director of security and computer policy on campus used these and other examples to emphasize the need for some basic protection: remove confidential data from personal computers when you are finished with it; don't keep shadow copies of confidential data; leave your computer off the network when away for extended periods; use antivirus software and keep it up-to-date; wipe data off of computers when they are being prepared for surplus or disposal; and consider what information you should be keeping on easily stolen computer hardware such as laptops, PDAs, and USB memory sticks.

## 6. THE FUTURE OF OUR EDUCATIONAL EFFORTS

We hope the symposium held in February 2004 will be the beginning of an ongoing campaign to better educate members of our campus community about the risks of identity abuse and the steps they can take to better protect themselves, their colleagues, and their students. The symposium was a full-day event, but most of the topics can be presented independently at departmental meetings or during programs sponsored by campus associations. Materials such as the survey and the example stories can be supplied to other campus groups wanting to host their own discussions.

## 7. ACKNOWLEDGMENTS

We gratefully acknowledge the UNC Chapel Hill Odum Institute for Research in Social Science and other campus organizations

that sponsored the February 2004 symposium on campus identity abuse. We would also like to thank the speakers at the 2004 symposium: Benjamin Brunk, Paul Jones, and Jeanne Smythe, all of UNC Chapel Hill. We appreciate contributions by Barbara Wildemuth, UNC Chapel Hill, to the design of the symposium theme and structure. The symposium was one event in the University's 2003-2004 Honor Initiative to raise awareness of honor, ethics, and integrity.

## 8. RESOURCES

Odum Institute for Research in Social Science,  
<http://www2.irss.unc.edu/irss/home.asp>

UNC Chapel Hill Honor Initiative, <http://honorcarolina.unc.edu/>

Working Group on the Internet and the Social Sciences,  
<http://www.unc.edu/internetimpact> (includes materials from the 2004 symposium on identity abuse)

## 9. REFERENCES

- [1] Foster, Andrea L. "New York U. Reports Another Lapse in Web Security." *The Chronicle of Higher Education* 50, issue 24 (February 20, 2004): A29.
- [2] Neumann, Peter G. "Information System Security Redux." *Communications of the ACM* 46, no. 10 (October 2003): 136.
- [3] Noguchi, Yuki. "Online Search Engines Help Lift Cover of Privacy." *Washington Post* (February 9, 2004): A01.
- [4] Radcliff, Deborah. "Wanted: Your Good Name." *Better Homes & Gardens* (March 2004): 168, 170-2.
- [5] Rubenking, Janet. "Identity Theft: What, Me Worry?" *PC Magazine*, March 2, 2004.