



## Stolen ID

*More and more people fall victim to identity theft each year; now, universities must find ways to keep student, faculty and staff info secure over the Internet.*

*By Krista Glen*

Imagine the excitement of your first career job, marriage and the move out of your cramped bachelor pad. Think of the surge of joy you will feel entering the bank, ready to sign the mortgage on your dream home.

Now, picture the banker as he reviews your application, smirks and, with one swift movement, pounds a stamp down on your carefully filled-in form. How will you feel when you finally make out the mark he left behind in red ink: **DENIED**.

What if this occurs even though you know your credit is impeccable? You pay your bills on time and you eliminated your student loan years ago. How could this happen?

Suddenly, a light goes on in your head; you remember hanging up on a collection agent who demanded you pay up on a credit card account you never opened. Somewhere, someone is using your ID, and laughing all the way to the bank.

Like a choose-your-own-adventure book, you have a number of options. You can think of yourself as a Good Samaritan or philanthropist – after all, the criminal might *need* the thousands of dollars of frivolous merchandise he or she accumulated under your name, right? You can bury your head in a pillow and cry for a week. Or, you can join the millions of North Americans who fall victim to identity theft each year, and begin to reclaim your good credit.

You decide to go with the last solution. You research the scenario only to find it is worse than you thought. After receiving notification in the mail, you learn your personal information was accidentally leaked to hackers

by your alma mater. That's right; the same post-secondary institution that helped you attain a higher education (which led to a good job and, in turn, the ability to purchase a first home), has now fouled you up.

Nowadays, unfortunately, this story isn't fictitious. More and more people fall victim to identity theft each year, and universities are facing increasing challenges to keep student, faculty and staff information secure over the Internet.

In September 2003, six machines at Wayne State University in Detroit, MI, launched a denial-of-service attack (DoS), preventing communication to and from the university and affecting the entire campus network. For over a week, the network was out of commission while technicians repaired the damage. The FBI was enlisted to determine who was responsible for the attack. Their identities remain unknown.

In January 2004, the Washington Square News, New York University's campus newspaper, reported mailing lists with the names, birth dates, addresses, phone numbers, e-mail addresses and social security numbers of over 2,100 students, alumni and professors were accidentally posted on a campus Web site.

In February, the California State University at Monterey Bay warned 2,800 applicants an employee had inadvertently posted their names, addresses and social security numbers on the Internet by

moving the information to a folder that was not secure. Users worldwide were able to access the information before the problem was solved.

In March, the University of California informed over 2,000 applicants an overloaded server may have leaked social security numbers, test scores and other confidential information onto the Internet.



At the beginning of April, officials at the University of Kansas called in the FBI when hackers accessed electronic pharmacy records – social security numbers, names, addresses, birth dates and prescription records filed from July 1994 to January 2004 at the on-campus pharmacy – through the Student Health Services network. The amount of student, faculty and staff

information copied, destroyed or modified has not yet been determined, and the issue is still under investigation,

In May, University of Michigan officials reported an intruder tried to hack into the school's computer system. An information technology technician detected traces of suspect software used to find computers vulnerable to hacking. While no

sensitive information was successfully accessed by the hacker(s), this attempt occurred despite the fact the university had upgraded its security in 2003, after a student allegedly accessed student and faculty e-mail and other private accounts.

These episodes clearly show cybersecurity is a global problem. Consequently, leaders from universities and other organizations across the U.S. have partnered to help reduce the number of incidences, lowering the probability of identity theft by malicious computer hackers.

Vital to this movement is Educause, a Washington D.C.-based non-profit organization with members from institutions of higher education,

businesses, corporations and other related organizations, whose mission, according to [www.educause.edu/about](http://www.educause.edu/about), is "to advance higher education by promoting the intelligent use of information technology."

Educause Security Task Force members are well versed in cybersecurity. In 2001, the task force – led by co-chairs Gordon Wishon and Jack



Suess (Chief Information Officer at the University of Maryland) – worked with the White House to develop the “National Strategy to Secure Cyberspace.” The document aims “to engage and empower Americans to secure parts of cyberspace they own, control and operate, or parts with which they interact.” ([www.whitehouse.gov/pcipb](http://www.whitehouse.gov/pcipb)) One chapter of the document is devoted to cybersecurity among institutions of higher education. Educause members also work with the U.S. Department of Homeland Security and the FBI’s InfraGuard

program, a co-operative undertaking involving the government, businesses and institutions of higher education.

Since the inception of the Educause Task Force four years ago, one of its main goals has been to promote cybersecurity awareness and policies in institutions of higher education. It’s a mandate Wishon follows closely, as he works with the task force to promote education and awareness of security issues to university students, faculty and staff, especially among senior leadership where, Wishon says, “there is a general lack of awareness.” They also establish standards, policies and procedures, not in terms of technology alone, but for business processes as well, for chief information officers (CIOs), information technology directors, management and the like. For this, documents detailing standards, policies and procedures are made available online to university staff,

accommodating the diversity of universities and colleges across the U.S. while remaining sensitive to the fact that, according to Wishon, they “cannot be one size fits all.”

Promoting a set of tools each individual school can implement effectively is also an important function of Educause, whose recommendations include the implementation of an intrusion detection system – software that identifies an attempted interference by hackers or automated attack tools like viruses and worms. And, in the

attempt to stay ahead of the ever-evolving hacking technology, the task force continuously works with computer vendors to ensure the tools – everything from operating systems to antivirus software to computers themselves – produced for use by post-secondary institutions are up-to-date and secure.

Structural organization and information sharing is encouraged and facilitated through the task force. Research and real-time information sharing of incidences occurring on the Internet are central to the security learning process – incident prevention increases when security officials across institutions are informed of the problems their colleagues face and the actions taken in response to these problems.

Recommendations presented by Educause are only part of a key resource for network security across the higher-education community. According to Joy Hughes, Vice President for Information

**Incident prevention increases when security officials across institutions are informed of the problems their colleagues face and the actions taken in response to these problems.**

Technology and Chief Information Officer at George Mason University (GMU), in Fairfax, Virginia, federal and state governments also play a vital role in the prevention of online identity theft and fraud. Providing public service announcements and sharing basic ideas on how individuals can protect themselves from online identity theft is crucial. “Government can also push more responsibility on software vendors to create secure code and on online businesses to utilize secure transmission technologies,” she says.

Wishon says government plays an involved role in dealing with institutions of higher education for a simple reason: what occurs in universities and colleges in turn affects government. He says the federal government sees higher education as an important resource for research that may be used, for example, to advance and enhance government network security and computer systems that house classified information.

**Because universities own a vast chunk of Internet space and house some of the fastest, most powerful Internet connections, malicious hackers and criminals use university networks “as launch pads for attack.”**

Wishon warns, however, the federal government has overlooked certain realities when enlisting universities for research and advancement. Because universities own a vast chunk of Internet space and house some of the fastest, most powerful Internet connections, malicious hackers and criminals use university networks “as launch pads for attack.”

According to Cathy Hubbs, Information Technology Security Coordinator for the Information Technology Unit at GMU, avoiding such attacks is no easy task. Hackers can gain access through a number of vulnerabilities that may exist in a school’s network system, including the misconfiguration of target hosts, system flaws, poor public education and a deficiency in vendor response. With such an abundance of susceptibilities, hackers seem more enabled than challenged when it comes to breaching computer systems.

Wishon knows first-hand what it is like to encounter a security scare. In addition to his involvement in Educause, he is also Associate Vice President, Associate Provost and Chief Information Officer at the University of Notre Dame (UND) in Indiana. He recalls an incident that happened nearly two years ago: an unprotected server exposed UND members’ personal information on the Internet. University officials never discovered if any of the

data was downloaded or accessed, but measures were immediately taken regardless; each potential victim was contacted by the school by mail and was sent information about identity theft.

Wishon, who works with UND to continuously build defenses against security risks, says it is a constant challenge that takes a lot of time, money and staff. In order to raise awareness among students, staff and faculty, UND has developed a set of initiatives, including a mandatory security session conducted for freshmen (it is voluntary for returning upperclassmen and faculty), in which a video about safe computing is played and streamed in a campus-wide Web cast. UND has also rebuilt its security structure and has implemented firewalls, a virus-scanning engine for both outgoing and incoming e-mails, an intrusion detection system and an active risk-assessment program.

### A 12-step guide to safer computing habits

**Step 1 •** When not using your computer, disconnect it from the Internet. Connected, your computer is open to intrusions by hackers who can access your files, bank account information and personal details, or may use your machine as a “zombie” to launch Denial of Service (DOS) attacks against Internet Service Providers or Web sites, shutting them down.

**Step 2 •** Use updated anti-virus and personal firewall software. Firewalls ensure no outside users can access confidential or private data. They also filter inbound and outbound traffic and alert you to attempted intrusions.

**Step 3 •** Make sure your operating system and application software are current. Download software patches for your Windows or Macintosh systems at <http://v4.windowupdate.microsoft.com/en/default.asp> and [www.uark.edu/compserv/softsys/macintosh/index.html](http://www.uark.edu/compserv/softsys/macintosh/index.html), respectively.

**Step 4 •** Use strong passwords more than eight characters long that include both alpha and numeric elements. Passwords should be completely random. Do not use words from the dictionary or numbers similar to your address, phone number or birth date.

While these security tactics are working well for UND, the IT Department at Indiana University (IU) recognizes having a secure password is an important technology that also keeps sensitive information protected. Taking its cues from banks, corporations and other organizations, IU has a “two-factor” authentication login system that includes “smart cards” and PIN tokens. First introduced in Europe in the 1970s, the system has since been accepted by the international computing community, says [www.itsecurity.com/papers/rainbow2.htm](http://www.itsecurity.com/papers/rainbow2.htm), with more than one billion cards shipped annually. IU, however, joins only a handful of universities who have adopted the technology. Mark Bruhn, Office of the Vice President for Information Technology and CIO at IU, explains the lack of enthusiasm for smart cards in the higher-education community: “These things do cost a bit of money. [Other universities] may have decided the costs outweigh the risks.”



Nevertheless, Bruhn defends the system. He says IU has been using password generator tokens since the early 90s and the two-factor login system has successfully ensured the safety of private accounts even if a user exposes his or her

password on a Web site, posts it on a monitor or if it gets stolen.

The two-factor system guarantees in order for anyone to access information at IU (particularly through applications permitting updates or inquiries to sensitive data), one password is not enough. Users with the authority to access sensitive data are issued smart cards, which require a username, password and personal identification number (PIN) token (an electronic piece of data unknown to the user and activated with a custom PIN); the physical card itself must also be presented. After entering their username and password, users must pass a four-character challenge. After they have activated their smart card with its PIN, the card gives them a four-character response, which they in turn can key into the application. All elements must be valid for access.

Members of IU’s IT department know that the intricate smart-card system does not come without some adversity. Initial challenges to its implementation included installing the software and obtaining interfaces designed to match IU’s own authentication dialogues. “And, of course,” says Bruhn, “We had to train users on how to use the cards.” In the end, the smart card prevailed, and IU now has over 10,000 cards working effectively on all eight of its campuses.

Other groups who have implemented smart cards into their computing systems have encountered similar difficulties to IU. A recent study of smart cards, conducted by the U.S. Military, showed installing and configuring the smart card reader (a device that literally “reads” the cards) onto an existing Windows system takes, on average, more

If you must use a familiar word or number to remember your password, rearrange it, invert it or combine it with another word or number. If your cat’s name is Fluffy and you live on Pine Street, spell the words backward and combine them: Fluffy becomes “yffulf” and Pine, “enip,” making your new password, “yffulfenip.” For added security, throw your favourite number in: “1yffulfenip3,” “yffulf13enip” or “yffulfenip13.” Use as many characters as the program for which the password is needed permits.

**Step 5 •** Never write your password down or post it on your monitor – someone may find it! If you must write it down, never leave it unattended.

**Step 6 •** Change your password regularly.

**Step 7 •** Files for sharing need password protection. Also, you must always understand what you are downloading. Many files found on peer-to-peer sharing programs contain Trojans (malicious programs contained inside seemingly harmless data) or Spyware (a program that can go undetected on your system and gather personal information to transmit over the Internet).

**Step 8 •** If you discard or trade in your computer, make sure you erase your hard drive first, ridding it of all sensitive information.

than 30 minutes. This makes it easier to understand why more universities haven't adopted the system: installing these devices would be a huge undertaking for IT departments, most of whom are already strapped for time and cash.

Despite the development of the smart card and other technologies that guard against the faceless attacks of computer hackers, university officials are constantly exchanging and exploring ideas, an important part of maintaining adequate defenses. "Mason has embraced the challenge of working toward a secure university," says Hubbs. At GMU, two appointed groups, with assistance and input from a university-wide body of system administrators, concentrate on privacy and security issues and disaster recovery plans and procedures. The CIO gives updates to and gets advice on strategies from members of the President's Council, which includes academic deans and vice presidents. The internal auditor provides guidance in identifying areas of risk and remediating these.

True, this kind of manpower aids greatly in preparing for and fixing problems, but it is technology that helps prevent problems at the source. At the technical level, says Hubbs, GMU network engineers can block known exploited ports if necessary, but remote access and portable devices are still potential avenues of infiltration. Rather, a university's plight to protect confidential information must be relentless. "The bottom line is, security is an ongoing challenge that needs to be fought with tenacity, perseverance and diligence," says Hubbs.

Regardless of the efforts universities make to ensure hackers do not acquire sensitive personal



information, they cannot stop every security breach, nor can they be on top of every new technology – resources and manpower are simply not of equal abundance in every school.

This story initially described a potential, yet fictional, incident of identity theft. In reality, 9.9 million Americans were the victims of identity theft last year, resulting in a total personal loss of \$5 billion (according to [www.usps.com](http://www.usps.com), the official Web site for the United States Postal Service). The Aberdeen Group ([www.aberdeen.com](http://www.aberdeen.com)) predicts by the end of 2005, identity theft will result in a total personal loss of \$2 trillion.

The Better Business Bureau of Canada ([www.cata.ca](http://www.cata.ca)) estimates an annual loss of \$2.5 billion as a result of identity theft to Canadian consumers, and a total annual cost to the Canadian economy of \$5 billion.

Steps to reclaiming one's identity can be a long and frustrating process, as there are several requirements for applying for a new SIN card or social security number. If you become a victim of identity theft, your investigation officer will need proof of fraudulent activity under your name,

**Step 9 •** When ordering products online and using your credit card, use only secure Web sites of reputable online merchants. A padlock on your status bar means the site is secure.

**Step 10 •** Do not e-mail your social security or social insurance number to anybody.

**Step 11 •** E-mails announcing you have won a prize or credit card e-applications are suspicious. If you are truly intrigued, ask to be mailed a hard copy of the e-mail or form.

**Step 12 •** Back up critical files and programs. That way, extra copies will be available to you in case of a disaster.

Resources:

[www.vtliving.com/computer/identitytheft.shtml](http://www.vtliving.com/computer/identitytheft.shtml)

<http://pc-pals.com/safecomputing.htm>

[http://itim.tamu.edu/good\\_passwords.shtml](http://itim.tamu.edu/good_passwords.shtml)

<http://infosec.tamu.edu/safecomputing.html>

[www.udel.edu/security/secinternet.html](http://www.udel.edu/security/secinternet.html)

a letter from a credit agency (Trans-Union or Equifax), a recent photograph, a police report (if available), an employment abstract listing all places of employment since the theft and a list of all places of residence over the past five years.

Several services exist to provide information and detail the steps you should take after falling victim to identity theft. Wishon recommends the Federal Trade Commission Web site, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) – a concise online resource on identity theft.

In Canada, [www.safecanada.ca/identitytheft\\_e.asp](http://www.safecanada.ca/identitytheft_e.asp) gives information on identity theft, and [www.hrsdc.gc.ca/asp/gateway.asp?hr=en/cs/sin/130.shtml&hs=sxn](http://www.hrsdc.gc.ca/asp/gateway.asp?hr=en/cs/sin/130.shtml&hs=sxn) explains how you may obtain a new social insurance number. ■



**Treat Each Frog  
Like a Prince**  
—Alicia Silverstone

Every year, millions of frogs, cats, pigs, and other animals are cruelly killed for useless dissection exercises. There are better, more exciting ways to learn (like computer models) that don't require slicing into animals.

For more information on how you can refuse to cut up animals in class, contact

**PETA** People for the Ethical Treatment of Animals  
501 Front St., Norfolk, VA 23510 • 757-622-PETA • PETA.org