

Knock, Knock, Who's There?

An epidemic of identity (ID) theft threatens both users and suppliers of online information services. In one traditional form, a victim's personal information—such as name, address, birth date, and social security number—is used by a criminal to apply for a new credit card (often granted instantly at major retail outlets), which is then used to run up a string of illicit charges. Although victims eventually discover the crime and may recover most of the lost funds, they often suffer extensive damages in a tangle of debt collectors, bad credit ratings, lost time, and stress.

This type of ID theft is particularly dangerous in the world of information systems, which may provide access to the records of thousands of individuals in a single lapse of security. For this reason, several states now require information service providers who suffer such a breach to notify all potential victims. At academic institutions, such lapses often involve insecure systems in departments or auxiliary units that have little professional support for security (remember the missing files and laptops at prominent government labs and agencies?). Many campuses still store social security numbers, the gold standard for ID theft, as a legacy identifier, even while the numbers are being phased out for safer “campus IDs.” Such campuses are accepting real risks, with potential liabilities. At best, the cost of notifying potential victims can exceed \$100,000 per incident, but to this dollar cost must be added the loss of community confidence and reputation.

Although the situation would be improved for all if the financial industry dealt with the “instant credit” problem,

higher education must undertake every reasonable precaution to protect the privacy of personal information. This is not rocket science, but it *is* hard work. It involves taking a completely new look at information security on campus—starting with a risk assessment followed by an ongoing program that addresses the people, process, and policy underpinnings of security. Ultimately, this requires a change in institutional governance to make campus executives, deans, directors, and other leaders responsible for the security of their own units, with appropriate evaluation and reporting. A wealth of relevant information and practical advice is available through the EDUCAUSE/Internet2 Task Force on Computer and Network Security at <http://www.educause.edu/security>.

As we increasingly depend on campus networks and the Internet for our core business processes, a second type of ID theft is rising to prominence. Known throughout history, the use of stolen passwords is much more dangerous on electronic networks, where an imposter may access the private information of thousands, fraudulently modify information, or even launch attacks on other systems. Passwords have always been susceptible to eavesdropping and guessing. More recently, they have been stolen by worms that log keystrokes, phishing attacks that masquerade as online banks, and “evil twin” wireless access points that eavesdrop on conversations.

Standard solutions rely on technologies such as PKI and encryption, which can block many types of attacks. One problem is that many such techniques are implemented by storing secret codes on

the computer hard disk. Such codes are hard to move from computer to computer and may be stolen by someone with access to the computer. The current solution of choice is hardware tokens, which are devices the size of a credit card or a USB memory stick. They contain and process secret codes and travel with an individual everywhere. Tokens fit nicely into our culture of carrying and protecting driver's licenses and car keys. Card-style tokens can also be used to open locked doors, combining important functions of physical security. A few academic institutions, including Dartmouth and the University of Texas Health Science Center at Houston, have adopted hardware tokens for wide use. Others are investigating the use of these tokens. Perhaps more important, all agencies of the U.S. government will soon issue such ID cards to every employee and to many contractors, a move sure to stimulate further adoption.

How will all this fit together? Member groups in EDUCAUSE and Internet2 have been experimenting with these issues for a number of years and are now involved in charting a course for our community through projects such as the HEBCA, Shibboleth, the NSF Middleware Initiative, and the InCommon Federation. We are working with industry and the federal government in groups such as the E-Authentication Partnership to ensure that the resulting systems interoperate. The goal is a global system that can solve the “Who are you?” problem without exposing the secrets of our identities.

Mark A. Luker, Vice President of EDUCAUSE, heads the Policy Office in Washington, D.C.