



9 Ways to Prevent Identity Theft

Keep staff and student data safe and sound.

By Sheila Riley

URL: <http://www.schoolcio.com/showArticle.php?articleID=192501201>

Protection against identity theft—impersonating someone, usually for financial gain—is a concern for every school district.

How can administrators keep data safe?

Larry Wong, information technology security officer for the 140,000-student Montgomery County Public Schools in Rockville, Md., and Matthew Kinzie, director of information technology for the Stanislaus County Office of Education in Modesto, Calif., which supports 24 districts with a total of 70,000 students, offer their suggestions.

Know what ID theft is and how it takes place.

“Unless you know understand what ID theft is and how it happens, you really won’t know how to handle it,” says Wong.

Some techniques that pose big risks are phishing—directing users to realistic-looking but phony Web sites, Wong says. Laptops, disks, and PDAs getting carried out of offices; and spyware, which collects information about computer users, are other trouble spots.

But most ID theft is low tech. It is most often directed at employees and not students, who generally don’t have credit records thieves are after, according to Kinzie. He recommends educating staff about “social engineering” techniques used to manipulate people into giving out confidential information. An ID thief might call a district office with only an employee’s name, for example, and then ask for another piece of information, such as work site. On its own, one piece of information might not be risky, but it can be a step in the ID theft process, Kinzie says.

Assign someone to the role of chief information security officer.

The chief information security officer probably shouldn’t be the CIO, Kinzie says. Security should be separate from day-to-day IT management.

The person in charge of security should be responsible for reviewing all sensitive information, such as how it's handled and where it's stored, plus the security officer should conduct employee awareness programs.

Pay attention to passwords.

Deactivate accounts after multiple failed attempts to use a password, and train employees to create good passwords—a minimum of six characters, including at least one letter and one number—and not to share them, says Kinzie.

But don't go too far in the other direction: too many restrictions on passwords allow hackers carrying out "brute force" attacks (generating and attempting to use all possible passwords to break into a system) to use fewer combinations of letters and numbers to do their dirty work.

Conduct ongoing training.

Montgomery County Public Schools gets security information to staff and student users in a variety of ways including printed literature, e-mails, and televised programs, on cable television stations and online.

The Maryland district also assigns user support specialists to each school. Wong meets with them three to four times a year, and they take information into schools for face-to-face training.

Give employees specific suggestions.

Tell users, particularly those working in sensitive areas such as human resources, to log off or turn off computers when they're leaving their desks.

Montgomery County also advises employees not to respond to anything asking for personal information, such as their computer user ID, password, or social security number, even if it looks as if it came from the district administration.

"We would not request that kind of information through the Web," Wong says. "We make it known that we don't do that."

Keep on top of standard tech precautions.

Make sure operating system patches, firewalls, anti-virus software, and filters are in place and up-to-date. These are obvious but important measures, says Kinzie.

Consider all sources of sensitive information.

When examining potential trouble spots, don't just consider desktop computers, Kinzie says. Look at everything: paper reports, laptops, and PDAs.

Think about addressing social networking sites.

Opinions differ about how to handle the relatively new phenomenon of social networking sites such as

MySpace.

Wong advises training teachers about the dangers of social networking sites, such as the potential for sexual predators to contact users, and how to educate students about them.

Kinzie stops short of making a similar recommendation. But many districts choose to block student access to the sites on school computers, he points out. “Whether schools should address [social networking] is a still a question,” he said.

Shred, shred, shred.

Hire a shredding service and train employees to use it. Alternatively, hire a service to make on-site visits to do the job.

Both Montgomery Public Schools and the Stanislaus County Office of Education shred paperwork with sensitive information, such as reports containing student data and employment applications.

Sheila Riley is a San Francisco-based freelancer who also writes for EE Times and Investor's Business Daily.

© School CIO