THE WALL STREET JOURNAL.

© 2004 Dow Jones & Company. All Rights Reserved

DOWJONES THURSDAY, DECEMBER 9, 2004 - VOL. CCXLIV NO. 113 - ★★★★ $1.00 ★★★★ WSJ.com

Trying to Remember New Passwords Isn't As Easy as ABC123

* * *

Codes in Flux Have Employees Jotting, Not Memorizing; Long Lists on a Post-It

By Scott Thurm
And Mylene Mangalindan

Before she begins work each morning, Kate Prior must enter eight computer passwords. Each must contain at least eight characters, and most require letters and numbers. Every three months, she must change them all.

How does the 28-year-old monitor of drug trials remember her passwords? Easy: They're written on a blue Post-It note affixed to her computer.

Kate Prior

Ms. Prior knows that her display threatens to undermine the very security that passwords are supposed to promote. "The IT people yell at me," she says, referring to her company's information-technology staff. But she prefers the occasional scolding to the alternative: forgetting a password, guessing incorrectly three times, and then having to call for help.

Security experts have long recommended that computer users choose hard-to-break passwords and change them frequently in order to frustrate hackers. Now, those recommendations are being newly forced on millions of U.S. workers in the name of preventing financial fraud under the Sarbanes-Oxley corporate-reform act.

The law, enacted in 2002 in the wake of accounting scandals at Enron Corp. and elsewhere, created an oversight body for audit firms, stiffened penalties for fraud, and required auditors to certify that firms have adopted adequate "internal controls" to prevent fraud.

No matter that Sarbanes-Oxley doesn't actually require changing passwords: In the name of those "internal controls," auditors and consultants are prodding companies to require that employees pick tougher passwords, and change them more frequently.

But the zeal for impenetrable computer systems rubs up against the limits of human systems. To cope with repeated changes to multiple passwords, many users adopt strategies that actually thwart security.

Roughly three-fourths of computer users memorize their passwords, according to a study done for the computer-security concern Symantec Corp. But memorizing

Please Turn to Page A9, Column 1

Tracking Passwords Gets Harder

Continued From First Page

several wholly new passwords is mind-numbing, so some employees make only trivial changes to old passwords—adding the numeral "1" to the original string, for example. That tactic, security experts say, doesn't make a new password any more difficult to crack than the old one was.

Some break another security taboo, by writing down passwords. The Symantec study, done earlier this year before password-change requirements had been imposed at many companies, found that 16% of users write passwords in a notebook, hand-held computer or on sticky notes.

Petri Darby, a 31-year-old marketing manager for a Houston law firm, used sticky notes for a while. When his stack of eight notes became unwieldy, Mr. Darby transferred the 25 or 30 passwords he needs for work tasks and to access various Web sites to a small piece of paper he kept in his wallet. But the password list kept growing and the paper became unreadable.

"It's driving me absolutely batty," Mr. Darby says. "I'm thinking that tattoos are the way to go."

As a result, some computer-security experts say the frequent password changes will just lead to different, potentially bigger, security threats. "It is not sensible to force people to change to a unique password every six months. You're inviting disaster," says Allen Gwinn, senior director of technology at the Cox School of Business at Southern Methodist University, who has spoken about security issues at trade shows.

"Better to have a password that's two years old that someone can remember than a password that's just been changed that's been written down that somebody can find," Mr. Gwinn says. He stores his passwords in a cellphone-organizer, protected by an encryption program he wrote himself.

Among companies that don't require periodic password changes are some that make computer security their business. At Fortinet Inc., a Sunnyvale, Calif., start-up that makes devices to block viruses and spam from corporate networks, employees must use tough-to-crack passwords, with at least six characters, including at least one that is neither a number nor a letter. The internal security team tests the choices using "password cracking" software and urges employees whose passwords flunk to choose new ones. "But we don't do required changes," says Philip Kwan, director of product management.

Before joining Fortinet, Mr. Kwan spent 15 years as an internal techie for three Silicon Valley companies. There, he repeatedly saw human nature defeat well-intentioned computer-security rules. When he was called to work on a computer and the regular user wasn't there, Mr. Kwan would pick up the keyboard. It was a good bet that he would find a password scribbled underneath. "We found a lot of bizarre passwords being taped all over the place," he says.

The Sarbanes-Oxley law doesn't mandate periodic password changes. Nor do the Securities and Exchange Commission rules implementing the law. Nor does the "guidance" issued by the Public Company Accounting Oversight Board, the nonprofit corporation that Sarbanes-Oxley created to regulate audit firms. Nonetheless, password changes have become a standard feature of management strategies to demonstrate compliance with the law.

One impetus appears to be the IT Governance Institute, a Rolling Meadows, Ill., nonprofit that brings together tech executives from big companies with representatives of major audit firms. The institute's "control objectives" for Sarbanes-Oxley list regular password changes as an "illustrative control" to prevent tampering with corporate financial systems.

Major audit firms then took up the cause. Deloitte & Touche USA LLP, for example, recommends that companies require employees to change passwords at least once every three months, and more often if the process can be automated. Ted DeZabala, national leader of Deloitte's security-services group, says the company has long urged periodic password changes, and used the Sarbanes-Oxley law to drive home the point.

By now, with the first Sarbanes-Oxley reports due to be filed in March, the practice is approaching ubiquity. "In all the companies I've seen, that is something they have adopted," says Marios Damianides, the international president of the IT Governance Institute and a partner with Ernst & Young LLP in New York.

Some experts say frequent password changes will just lead to different threats.

Some security experts think the recommendations aren't tough enough. "All passwords can be broken within 45 to 60 days," says Carl Herberger, senior director of information security services for SunGard Availability Services. He recommends that companies force employers to change their passwords every month.

The thought drives some computer users up the wall. "Who has a brain to remember all these?" asks Alex Ramsey, chief executive of LodeStar Universal, a 10-person management-consulting firm in Dallas. Ms. Ramsey stashes her roughly 75 passwords in a computer file, named "Password." As a back-up, she printed out a copy that she hides under her keyboard.

Candace Jenny, a Silicon Valley engineer, adopts similar tactics. The 47-year-old recently left a job at which she needed 10 passwords, several of which required non-number, non-letter characters—such as #, ^ or * — and which had to be changed as often as once a month.

"I ended up making a list, which is exactly what they don't want you to do," says Ms. Jenny, who now works at a start-up. She stored the list in her computer, and in a notebook she kept in an unlocked file cabinet. But she understood the risk. Once you write a password down, she says, "the chances are you're more careless with it."