



Archives

Note: Searching is always free. There is a \$2.95 fee to view the full-text of any article.
[Check out our Pricing Options.](#)

San Jose Mercury News (CA)

September 4, 2003

Section: Personal Technology

Edition: Morning Final

Page: 1G

Memo:PASSWORD TIPS

Managing multiple passwords can be tough, but following a few simple steps will help keep user names and passwords away from high-tech bad guys.

DO

(box) Use a combination of letters and numbers.

(box) Write down hints that will remind you but won't reveal the password to anyone else.

For example, write down "My third-grade teacher" instead of "Smith."

(box) Change your password frequently.

DON'T

(box) Don't write down your password.

(box) Don't share your password with others.

(box) Don't use easy-to-crack passwords, such as pet names, words that can be found in a dictionary, places of birth, Social Security numbers, birthdates.

(box) Don't store your user names and passwords on the hard drive of your computer. If you must make a note of passwords, store them someplace other than the computer's hard drive, such as a floppy disk.

PASSWORD OVERLOAD

SOFTWARE, GADGETS ON THE MARKET TO KEEP YOUR SECRETS SAFE

SAM DIAZ, Mercury News

If you're anything like the rest of us, you have user names and passwords floating around cyberspace and, even worse, you're doing a poor job at keeping them a secret.

I'll admit that I have at least a half-dozen names and passwords taped to the outer part of my computer screen. I know that's a bad thing, but I also know that I'm not alone.

A recent survey, conducted by tech security company Rainbow Technologies, found that 55 percent of computer users have written down a password at least once and 40 percent have shared a password with someone else.

And forcing us to use a combination of letters and numbers or prompting us to change our passwords every few months has actually increased our likelihood of writing down passwords.

But what else are we to do? Keeping track of an e-mail user name and password was simple enough. But then came online news subscriptions, online auctions, online banking and bill-pay -- and each of them brought a new user name and password.

"There's an awful lot of pain generated out there when dealing with passwords," said Andrew Finkle, vice president of marketing for Siber Systems, which makes the AI RoboForm, a form-filling software. "Consider that a password and log-on are just form fields from a computer standpoint."

The software -- available for download at www.roboform.com -- kicks in when the user visits a specific Web site -- the sign-on page for your online bank, for example -- and fills in your user name and password and will even click the Submit button for you.

Passwords Plus by DataViz, a similar product, also keeps track of Web-based user names and passwords and stores that data on the hard drive -- but requires a master password to open those files.

Ugh, sounds like just another password to remember.

Microsoft Windows offers a password manager that remembers and fills in your passwords when you visit a site but imagine a colleague sitting at your terminal, visiting E(*)Trade and suddenly viewing your personal financial information.

The latest trick, Finkle said, is to store the data file on a USB keychain drive, leaving the software installed on the PC itself.

"It's like being able to take all of their stuff with them," Finkle said. "There's nothing more solid than that. When you remove the key, the data is gone."

Rainbow Technologies, the company that conducted the survey, is pushing a similar product but is hoping that iKey, its USB token, will replace passwords, not manage them.

"Passwords really offer such minimal security," said Shawn Abbott, president of the company's e-security division. "But we've really never had anything better."

At the business level, employees would be assigned iKeys to authenticate themselves as authorized users on the computer. They also could use the key to prove their identities when they tap into the company network from remote locations.

SecuriKey, a product by Griffin Technologies, is selling a consumer USB token that unlocks and locks files, Internet browsers and even the computer itself by inserting and removing the token from the USB port.

It's a noble idea, but until authentication turns the corner into the next generation -- using biometric services such as eye scans, fingerprint recognition and voice authentication -- we're stuck with passwords.

It's a good thing that there are tools to help manage them.

Illustration: Drawing

DRAWING: TRACY COX -- MERCURY NEWS

Copyright (c) 2003 San Jose Mercury News