



Finding a replacement for passwords

By Ina Fried

http://news.com.com/Finding+a+replacement+for+passwords/2100-1029_3-5586249.html

Story last modified Wed Feb 23 04:00:00 PST 2005

As online scams get more sophisticated, passwords are becoming hopelessly outmoded--as passe as floppy disks.

Yet many businesses and nearly all consumers still rely on passwords as the primary means of verifying who they say they are.

At last week's [RSA security conference](#), Microsoft Chairman Bill Gates sounded once again his [well-worn call](#) for an end to [passwords](#), while on the show floor, companies touted gadgets to help verify identity.

There's plenty of technology that could augment or replace the password, from smart cards to password-generating tokens to cell phone-based systems. They have yet to catch on. One hurdle is that it can be inconvenient to have to keep a piece of hardware handy. But the real problem, analysts said, is that neither businesses nor consumers appear ready to pay for them.

"Every bank I talk to doesn't want to hand out tokens," Gartner analyst Avivah Litan said. "They're too expensive."

The cost of such a service is not insignificant. For instance, companies that have signed up for RSA Security's corporate hardware tokens pay on average \$35 to \$40 per employee as part of an annual service deal. However, a consumer service could cost a bank or other online service provider far less, if they hand out hundreds of thousands or millions of the gadgets.

Passwords are seen by many experts as a weak link in the security chain. A [well-circulated research paper](#) from 1979 noted that a significant share of passwords could be easily guessed in less than 5 minutes--and that was when punch cards were popular.

Web stores, online banks and other companies doing business on the Internet recommend that customers choose a password that is easy for them to remember but hard for someone else to guess. The reality is that the converse is usually true. Few of us can remember all of our passwords, and yet the bad

guys, armed with sophisticated software, can crack most passwords in a matter of minutes.

RSA's SecurID token, which generates a one-time password (OTP) every few seconds, is only one of the hardware products on the market that aim to bolster security for consumers. Credit card-size smart cards slot into a reader and can be part of two-factor authentication. In this system, two ID elements--the smart card and a personal identification number, for example--are used to monitor access. A USB token works like a smart card, but plugs directly into a PC, instead of into a special reader. Another system sends one-time passwords via text message to a customer's registered cell phone.

The biggest factor pushing companies to pay for something better than passwords are the concerns around identity theft and [phishing](#)--Internet fraud in which people are fooled into giving their personal information, such as online banking passwords, to thieves. If something more than a password was needed to get access to financial records, it would be trickier for crooks to profit from such schemes.

"We want to add significantly more protection for our users and are looking at stronger authentication for passwords," said Adam Joffe, chief technology officer for Sony Online Entertainment, at an RSA Conference 2005 [panel discussion](#).

Last week at the show, RSA Security announced plans for a hosted SecurID service where companies can add a layer of extra security for consumers. E*Trade Financial is among those that is trying out the RSA technology--passing out a small number of the devices to customers for free. The company plans to decide later this quarter whether to expand beyond a few hundred early testers.

RSA said there are about a million consumers using its authentication technology, through a variety of pilot programs. Other companies that are eyeing the technology include financial institution Credit Suisse, Yahoo and Sony Online Entertainment.

Joffe said that Sony is "seriously considering" offering the RSA token to some of its customers. While game characters and points may not have the monetary value of a bank account, such identities are just as important to protect from online fraud.

"I wouldn't say (fraud is) a huge issue, but it's an issue," he said.

RSA's hope is that many number of companies will sign up for the program and that consumers would need only one token to manage a variety of accounts. Some businesses will give out the tokens free, while others may make customers foot part or all of the bill, the security provider believes.

Although the devices have the potential to help cut fraud, RSA Vice President Christopher Young said the company is selling consumers as much on peace of mind as on cost savings. He likens it to the alarm that guards his house.

"I haven't had anyone break into my home before," said Young, who until about two months ago was head of safety and security premium services at America Online. "It makes my wife feel more comfortable when I am traveling, and I travel a lot."

Tony Gentile, a San Jose, Calif.-based Web marketing consultant who runs a site called Buzzhit.com, said he would like to see a second method of authentication for many online activities, including banking, stock trading, Web-based health care and electronic voting.

But, he warns, any system is fraught with challenges. And he's not sure he or other consumers are ready to pay for it.

"The devil's in the details here," Gentile said. Tokens have a place, he said, but that place is not the same in each business. "What's appropriate for one type of business and usage pattern may be very different from another."

There is also the issue of convenience. While RSA's tokens are small enough to fit on a keychain, they are also easily lost. People might be amenable to carrying one token. Less appealing to people is the prospect of needing one device to verify themselves to a bank, then another for their stockbroker, and ending up with a bunch of tokens.

A solution would be for online service providers to agree on a single product or standard. For now, it's unclear whether companies will come to an agreement on this. RSA, for its part, said it will try and work not only with its devices, but also with similar devices from others.

End of the line?

Some analysts do see the password fading as the primary means of authentication, particularly for online banking.

In a December report, Gartner estimated that by the end of 2007, 60 percent to 75 percent of U.S. banks will use something stronger than a password, but stop short of giving out hardware tokens. Roughly 7 percent more will go as far as to hand out something like the RSA token, the research firm predicted.

Overseas, the overwhelming majority of banks will require something more than a simple password, with anywhere between one-third and one-half of banks requiring a hardware token, Gartner analysts said.

The bad news in Gartner study is that by the time many of these new systems become common, the thieves will have also moved on. By the end of 2007, half of today's stronger methods of authentication will no longer be strong enough to foil phishing or online attacks, the report's authors said.

While technology providers have focused on hardware devices as a secondary means of identity authentication, research has come up with less costly replacements for the password.

One alternative is a picture-based password. Instead of remembering a word or digits, a user would click on a specific part of a large digital photo. Another idea is that a series of random numbers or letters appear and you enter the letters for your password based on a shape that you remember. While perhaps more difficult for random thieves to guess, some have warned that such graphical passwords might be more easy for a co-worker or other passersby to spot.

Another suggestion has been to use unique personal traits, such as fingerprints, as a means of authentication. Although there are a handful of notebook, handheld and desktop computers that come with fingerprint readers, such biometric technology is not widespread enough to make it a standard method of verifying identity. Voice prints are another option, but until speech recognition improves in reliability, customer frustration could be high.

Still life in passwords

Despite all the criticism of passwords, not everyone thinks they are past their prime.

Richard Parry, who is responsible for assessing threats for consumer banking giant JP Morgan Chase, argued that too much attention is being given to Internet security fears in general and passwords in particular.

"It would be untrue to say (the password) is not still working for us in many applications," Parry said. "Whether it is sustainable is another question."

Parry pointed out in a panel discussion at the RSA show that in any 24-hour period, more money will be lost from burglary than from Internet fraud. "The sky isn't falling," he said.

That said, he noted that two-factor authentication is already in relatively high use in financial institutions for very wealthy and corporate customers, as well as for certain large transactions. JP Morgan Chase's own workers use RSA's tokens, for example. He did note that such measures probably don't make sense for the masses, where two-thirds of bank accounts contain less than \$1,000.

In the background of the debate over passwords is the suggestion that if online banks don't tighten security, U.S. regulators may force them to do so. In places

like Singapore and Sweden, laws already require stronger means of authentication. And a December FDIC [report](#) says that the industry's reliance on passwords "offers an insufficient level of security" and suggests hardware tokens may be the way to go.

Parry is particularly concerned that well-intentioned regulation could have economic drawbacks for service providers.

"Some regulation is good, and regulators have every right and even an obligation to be concerned," he said. But "regulation as a blunt instrument could dramatically increase costs."

[Copyright](#) ©1995-2005 CNET Networks, Inc. All rights reserved.