Simple passwords no longer suffice

AP) -- To access her bank account online, Marie Jubran opens a Web browser and types in her Swedish national ID number along with a four-digit password.

For additional security, she then pulls out a card that has 50 scratch-off codes. Jubran uses the codes, one by one, each time she logs on or performs a transaction. Her bank, Nordea PLC, automatically sends a new card when she's about to run out.

As more Web sites demand passwords, scammers are getting more clever about stealing them. Hence the need for such "passwords-plus" systems.

Scandinavian countries are among the leaders as many online businesses abandon static passwords in favor of so-called two-factor authentication.

"A password is a construct of the past that has run out of steam," said Joseph Atick, chief executive of Identix Inc., a Minnesota designer of fingerprint-based authentication. "The human mind-set is not used to dealing with so many different passwords and so many different PINs."

When a static password alone is required, security experts recommend that users combine letters and numbers and avoid easy-to-guess passwords like "1234" or a nickname.

Stevan Hoffacker follows those rules but commits a different faux pas: He uses the same password everywhere, including access to multiple e-mail accounts, Amazon.com, The New York Times' Web site and E-ZPass electronic toll statements.

In such cases, should hackers or scammers compromise one account, they potentially have one's entire online life.

"This is one of these things that if I stop and think about it, it is not good, but I do my best not to stop and think about it," said Hoffacker, an information technology manager in New York.
Password harvesting

But it's difficult to remember dozens of strong passwords -- so many sites now require them. Alternatives include writing them down on a sticky note attached to a monitor or in an electronic spreadsheet -- practices security experts also deem unsafe. Software such as Symantec Corp.'s Norton Password Manager and Apple Computer Inc.'s Keychain help store passwords in secure, encrypted form. But if you compromise the master password, you're out of luck. Your entire collection is gone.

Many sites, meanwhile, will e-mail passwords insecurely -- without encryption -- if you forget. A site called BugMeNot.com even encourages users to share passwords for nonfinancial sites like newspapers.

The tools of password harvesting are many:

Keystroke recorders secretly installed at public Internet terminals can capture passwords, as can "phishing" e-mails designed to trick users into submitting sensitive data to fraudulent sites that look authentic. There are computer viruses programmed to harvest passwords as well as software that guesses passwords by running through words in dictionaries.

Though analysts have no hard figures on password-specific fraud, they blame insecure passwords for unauthorized financial transfers, privacy breaches and even the hacking of corporate networks.

With two-factor authentication, having a password alone is useless.

"We will never play the fear factor here, but still it stays a fact that with our products, phishing is no longer an issue," said Jochem Binst of Vasco Data Security International Inc.

The Belgian company issues devices the size of pocket calculators or keychains. You type your regular password into the device for a second code that is based on the time and the unit's unique characteristics. That's the code you type into the Web site.

Someone who steals your device won't have your password; someone who steals your password won't have your device.

Two-factor authentication

Jubran's bank, Nordea PLC, automatically sends a new card containing 50 scratch-off codes when she's about to run out.

MasterCard International Inc. has been testing similar systems in Britain, Germany and Brazil. Swipe a credit card with a smart chip into a special reader, enter your PIN and obtain a password good only once at Office Max, British Airways and a dozen other merchants.

In Singapore, bank customers wishing to designate new accounts for fund transfers must likewise obtain a second password -- through a phone call, e-mail or mobile text messaging.

Biometric systems are similar, except a fingerprint or iris scan replaces one or both passwords.

In the United States, use of two-factor authentication remains limited. RSA Security Inc. has several products, including RSA SecurID, but they are primarily issued to employees for remote network access and to customers with high-value portfolios.

"There's a delicate balance between maintaining security but also providing customers with ease of use," said Doug Johnson, senior policy analyst at the American Bankers Association.

Gartner analyst Avivah Litan said banks are "all afraid of making the first step. They don't want consumers going to other banks because it's too hard." U.S. banks and e-commerce companies have focused, for now, on making sure passwords are strong. EBay, for instance, now rejects attempts to create passwords such as "ebay" or "password."

Before two-factor authentication becomes commonplace, laptops must come standard with biometric readers, or manufacturers must bring down costs for password-generating devices.

Outfitting 1 million customers with such devices could cost $20 million, while Internet fraud for those customers amounts to "tens of thousands at most," said Tony Chew, director of technology risk supervision at the Monetary Authority of Singapore. Singapore banks thus limit dynamic passwords to fund transfers, he said.
Setting standards

Companies also need to set standards. Though Jubran enjoys her bank's scratch-off passwords, she wouldn't want the Amazon.coms of the world all adopting them as well. "It would be too complicated to have 10 different cards you scrape off," the 24-year-old medical student said.

Jason Lewis, vice president of product management at RSA Security, figures companies will have to create services so a single device can work on multiple sites. Nordea and other Scandinavian banks already have partnered with government agencies and utilities, and an identity-management coalition called the Liberty Alliance Project has begun to explore standards.

People will pay more attention to security as they keep more of their lives online, said Robert Chesnut, eBay's vice president for rules, trust and safety. He offered this analogy: "The more stuff you have in your house, the better the deadbolt lock you have."