AMERICAN BANKER
On Focus and In Depth

Security Watch

American Banker | Wednesday, December 9, 2009

By Daniel Wolfe

Ta-Ta, Tokens

The strong authentication provided by one-time password-generating tokens was apparently not worth the hassle or the expense for customers of **AOL LLC**.

AOL, which is being spun off from **Time Warner Inc.** this week, said it would largely discontinue support of the tokens it began offering in 2004, Wired.com reported in its "Threat Level" blog Dec. 4.

The tokens are keychain devices that generate passcodes that quickly expire, so that only the person in physical possession of the token should be able to access the associated AOL account.

Because of the complexity of the system and the cost of distributing the devices to users, tokens are more commonnly used in business settings. Most financial companies use less intrusive security methods to protect consumer accounts, such as transaction monitoring systems.

AOL framed its decision as an ease-of-use issue. It told its customers in an e-mail that discontinuing its use of tokens, which cost users $9.95 up front and then $1.95 a month thereafter, "should make it faster and easier for you to access your e-mail account and any Web site" that required their use.

EMC Corp.'s **RSA Security**, which makes the tokens AOL used, said there was significant interest from AOL users when the tokens were first introduced, but relatively few AOL users have requested the devices in recent years.

Sam Curry, a president of product management at RSA, of Bedford, Mass., told Wired.com that users likely did not perceive their e-mail accounts to require as much protection as bank accounts. "The trade-off may not make sense for users of AOL," Curry said.

The Wired.com story noted that celebrities and other VIP users of AOL would still have access to the tokens.

Online Perils

An electronics testing firm has sued **Capital One Financial Corp.** over fraud losses it claims the banking company refused to cover.

JM Test Systems of Baton Rouge said it lost about $97,000 in February and March to two unauthorized transfers, and said Capital One has denied responsibility for covering the losses, *The Washington Post*'s **Brian Krebs** reported in his "Security Fix" column Tuesday. JM Test filed its suit last week in a Louisiana district court, accusing Capital One, of McLean, Va., of breach of contract and negligence. Krebs said Capital One declined to comment for his story.

Businesses do not enjoy the same protections that consumers do against liability in such fraud cases.

Whereas banks typically reverse fraudulent charges if consumers alert them to the issue within 60 days, businesses are required to report fraud incidents immediately, and even then they have no guarantee of being reimbursed, Krebs wrote.

JM Test said it alerted Capital One to the fraud incidents on the days they occurred. The first took place Feb. 20, when scammers wired over $45,000 to recipients in Moscow.

The second took place March 2, when scammers made smaller transactions totalling $51,556.44 to various accounts that later moved the money internationally. JM Test said that between those two incidents, it was issued new online banking credentials

by Capital One.

Krebs noted that JM Test is not the first company to sue its bank over similar losses.

—

If that childhood friend trying to reconnect with you on Facebook is a rubber duck, some mischief may be afloat.

The U.K. security firm **Sophos PLC** has found that people are often quite willing to share sensitive personal data, such as phone numbers and birth dates, to complete strangers who request this information on **Facebook Inc.**'s social networking Web site. And yes, that includes people who represent themselves with a photo of a rubber ducky, *Computerworld* reported Monday.

Though only 4% to 6% of people tested with the rubber duck ruse gave out personal information (depending on their age range), many more, 46%, gave out information to a fictitious woman who reached out to them through Facebook, Sophos found in a test of a randomly selected group of 100 users of the social networking site.

Graham Cluley, a senior technical consultant at Sophos, said this means scammers have a very good shot at using Facebook to obtain the sort of personal information they could use to commit fraud.

"Criminals essentially have a one-in-two chance of getting information without even trying," Cluley told *Computerworld*. "Ten years ago, it would have taken con artists weeks, maybe with the help of a private investigator, to come up with this kind of information."

Though the duck did not make many friends in Sophos' 2009 test, a 2007 test with a made-up profile for a toy frog netted personal information from 41% of respondents.

—

Google Inc. said a Salt Lake City company has been using its brand to place unwanted charges on people's credit cards, according to an article *Computerworld* ran Tuesday.

The company, **Pacific WebWorks**, advertises the "Google StartUp Kit" and other work-at-home kits that Google said are of little value, according to a lawsuit Google filed in **U.S. District Court for the District of Utah**.

Though the kits are advertised as free, Google claims that they are "subjected to continuing monthly fees that often exceed $50 and range as high as $79.90," according to its lawsuit. Google said it has received complaints from people who felt the charges were unauthorized and were unable to cancel them.

Pacific WebWorks already faces a class action in Illinois that was filed in November. Google said it is proceeding with its own suit to ensure that its brand is no longer used with Pacific WebWorks' products.

Google claims that Pacific WebWorks employs "an ever-changing coterie of Web sites" to avoid detection. These Web sites all use the same template, made from fake news stories and blog entries as well as "pressure tactics to drive unsuspecting consumers to credit card processing sites like those run by PWW," Google claimed in its lawsuit.

The article said Pacific WebWorks was not available for comment and that its outgoing voice mail message referred callers to a nonfunctioning Web site. Pacific WebWorks also runs the payment processer **Intellipay**, the article said.

Security Watch is a weekly roundup of news and developments in data security and their impact on financial services companies.

Please e-mail us any comments, ideas, and suggestions about this column.