

Online security a work in progress

Half of financial institutions in Ohio haven't met new ID requirements

Thursday, March 01, 2007

Denise Trowbridge

THE COLUMBUS DISPATCH

Your bank should be asking you to enter more than a username and password when you bank online. But there's a good chance it isn't.

Many Ohio banks missed the Federal Financial Institutions Examination Council's Dec. 31 deadline to add security features to their online-banking Web sites.

The agency requires banks to use "multifactor authentication," which means online banking customers need to enter more than a username and password to verify their identity.

Customers could pick a photo to appear after they log in, answer a series of personal questions, or enter a code from a small digital device that randomly generates numbers every time they log in.

Unfortunately, not all banks are up to speed, said Jon Fisher, CEO of security software firm Bharosa in Santa Clara, Calif. Bharosa is developing security features for National City and Sky Financial.

About 50 percent of Ohio banks do not have systems in place, he said.

Large regional banks are the most likely to have installed new security features, he said. Smaller community banks are least likely to have met the deadline.

Missing the deadline is not as bad as it sounds, said Mike Van Buskirk, president of the Ohio Banker's League. About "47 percent of the 50 percent (that missed the deadline) are really close."

They didn't miss it for lack of attention, he said. "A lot of smaller community banks are using outside (software) vendors for this, and the vendors just aren't finished yet."

Delaware County Bank hired an outside company to design new security features and is making them available to customers in mid-April. Customers will be asked to choose a phrase or photo, which they'll have to identify every time they log in to their account.

National City has not finished installing its new features, either, but customers should see changes by the end of 2007, spokeswoman Kelly Wagner-Amen said.

Regulatory officials, recognizing that it will take time for banks to design and install new software, aren't cracking down on banks that missed the December deadline, Van Buskirk said.

"They're looking to see how far along banks are, and so far, the industry overall looks pretty good."

Many Ohio banks have added the extra features.

Huntington gave password "keys" to its commercial banking customers in November. The bank also asked its online banking customers to choose several personal security questions. Users are prompted to answer those questions if they log in from a computer they don't normally use.

Park National Bank also rolled out extra Web security in November; the company chose the photo-identification option.

But don't judge your bank by its Web site. Banking customers cannot necessarily gauge their bank's security system by appearance alone, Fisher said. "A lot of the changes, customers might never see."

Some banks are using fraud detection software that only flags out-of-the-ordinary transactions, he said.

In that case, customers would be prompted to answer a personal question or identify a photo only if they are doing something unusual, such as logging in from a different computer.

But all banking customers should get used to periodic changes in their online banking, because the federal guidelines are basically "a moving target," Van Buskirk said.

dtrowbridge@dispatch.com