

JANUARY 26, 2007

FOCUS ON: FINANCE
dayton.bizjournals.com

New security guidelines in place for online banking

BY ANNA GUIDO
DBJ STAFF REPORTER

Username, password and even mom's maiden name may no longer be enough to protect consumers from online banking fraud.

Guidelines issued in 2005 by a branch of the Federal Reserve Bank (the Federal Financial Institutions Examination Council, FFIEC), concluded that more protection is needed to secure Internet banking transactions.

The guidelines, called "Authentication in an Internet Banking Environment," took effect in January and require banks to fortify their Web sites to protect consumers from a growing army of cyber thieves.

"The guidelines simply are calling for another factor of security beyond username and password," said Jon Fisher, chief executive officer of Bharosa Inc., an international security software company based in Santa Clara, Calif.

Since 2001, the increased incidence of online banking fraud is part of what has contributed to the growth of improved transaction security technologies for online banking.

Nick Selby, a senior analyst and director for the enterprise security practice of The 451 Group in Boston, said banks are implementing three factors of consumer authentication.

- Something you know, such as a password, or an image you recognize.

- Something you have, such as your computer, or a one-time password (as proof you possess the device that generates it).

- Something you are, such as your fingerprint or a retinal scan (which would be proved through biometric readers, but these typically are only used in very high security environments).

The FFIEC guidance is non-prescriptive. Upon regular audits, however, banks will be fined if their sites do not authentication mechanisms (besides the standard username/password) in place.

Cincinnati-based Fifth Third Bank was a step ahead of the game, having investigated the matter a few months before the FFIEC guidance was issued, said Debbie Wheeler, Fifth Third's chief information security officer.

Fifth Third has had customers impacted by online fraud, Wheeler said. "But this effort is driven more by our desires to strengthen the security of our online banking operations," she said.

Fifth Third is partnering with Bedford, Mass.-based RSA (the security division of EMC) to implement a suite of products to enhance authentication and assist with fraud

prevention and detection, Wheeler said.

One, an RSA "anti-phishing" product, has been in place since July.

The term "phishing" alludes to the use of increasingly sophisticated lures to "fish" for users' financial information and passwords. Phishing attacks unsuspecting users and lure them to sites that appear to belong to a trusted partner—often a bank or retailer—where users are duped into entering their personal information like a password and username. Criminals then use the credentials.

Wheeler said its anti-phishing product trolls the Internet looking for instances of brand infringement then "shuts down sites that are illegally referencing the Fifth Third brand."

She said typical phishing e-mail might read like this: "We're about to shut your account access off unless you click on the following link and complete the requested information."

When users click on the link, they are redirected to another Web site, known as a "collecting point."

The software quickly shuts down the collection points, so even if a customer would inadvertently click the link, they would be protected, Wheeler said. "It's a constant cat and mouse chase," she said.

Even though Fifth Third communicates to its online customers that it would never ask for this information, some still click the link no matter what, Wheeler said.

The California firm Bharosa is among a growing number of vendors worldwide developing transaction security products to combat online banking fraud.

One of Bharosa's products used by National City and Sky banks is "Tracker," which works behind the scenes to learn the online tendencies of users. It looks at everything from the types of transactions conducted to the machines used to confirm a user's identity.

"If your username or password are stolen through whatever means, then the attacker cannot access your account because the anomalies are immediately screened and the account is protected," said Bharosa's Fisher.

The FFIEC guidelines are another example of how the federal government and private industry are cracking down on online banking fraud.

Just last week, a California man was found guilty under the federal CAN-SPAM Act for using fraudulent junk e-mails to trick America Online users into giving up bank account numbers and other personal information.

It was the first jury conviction under the act, which was signed into law by President Bush in 2003.

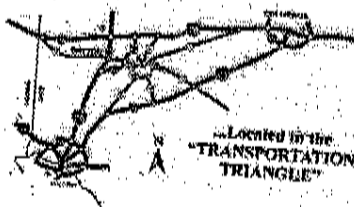
■ E-mail aguido@bizjournals.com. Call 222-8900, Ext. 120.

Xenia Economic Growth Corporation

XENIA is in the middle of the "Transportation Triangle", formed by I-70, I-71 and I-75, providing one-day access to nearly two-thirds of the US market.

XENIA has more than 340 acres of available industrial land, including more than 140 acres in the Xenia Industrial Park. Most priced at \$35,000 an acre or less.

XENIA has a diverse, dedicated and skilled workforce. And with more than 25 area colleges, universities and career centers, we can meet all your training needs.



...Located in the
"TRANSPORTATION
TRIANGLE"

XENIA
Ohio USA
CITY OF HOSPITALITY

Xenia Economic Growth Corp.
181 W. Main St. • Xenia, OH 45385-2935

(937) 372-6389 • (800) GO XENIA • Fax: (937) 372-3509 • www.xegc.org • xegc@xegc.org

AWA
WINN
DESE
EXPER
TECHN
EXPER
INTEG

One Te
937.849.



- SMALL B
- COMMER
- CASH MA
- BUSINESS

937.224.4
15 Area L
www.libert

SWITCH
ALWAY