



Reprints of articles about your community bank • www.JohnMarshallBank.com • 703.584.0840

Local Bank Fights Cybercrime



By Daryl Buchanan / reprinted from *The Sentinel Newspapers*

With the help of the FBI, Washington John Marshall Bank is stepping up its efforts to protect customers from cyber fraud in the Washington, D.C. area.

The Washington Field Office of the FBI's Cyber Division and John Marshall Bank held a public symposium for banking customers to teach them how to protect themselves from cyber theft. Bank officers and 65 of their business clients attended the symposium.

"We see about 60,000 attempted online attacks or 'pings' in a typical month. Bank robbers don't always come through the front door. We take cyber security very very seriously," said John Marshall Bank CEO John R. Maxwell.

John Marshall is listed as one of the fastest growing banks in the United States and has a lot to protect, with more than 3,000 accounts and assets of about \$400 million. According to the 2011 Norton Cybercrime Report, the global cost of cybercrime was estimated to be nearly \$400 billion a year, and there are more than 1 million victims of cybercrime per day.

According to John Marshall Senior Vice President Bruce Gemmill, customers should be wary of spam and phishing emails that appear to come from strange sources.

"It has to be stressed that customers should avoid phishing attempts for log in credentials or other personal information. Emails from suspicious sources with file attachments or links to other sites should be avoided at all costs," said Gemmill.

In addition to email and phishing scams, Automated Clearing House (ACH) transactions originated by clients are John Marshall's biggest risk. ACH transactions are an electronic network for financial transactions like debit and credit card transactions. John Marshall COO Carl Dodson says that each ACH is reviewed daily before it goes through.

"We continually update our online banking module to make security more robust. We are also focusing more on customer education regarding fraud protection with mailings, web site notices, and periodic symposiums. We also monitor suspicious online account log in attempts, geographic location of sign-in attempts, and number of failed sign in attempts," said Gemmill.

John Marshall also helps keep customers secure by keeping software security patches and virus definitions up to date. They also utilize 24/7 network monitoring and intrusion attempts. John Marshall even hires a third party to



attempt to hack into their system so they can identify vulnerable areas that need to be fixed.

John Marshall is not alone in the fight against cybercrime. The FBI has set up cyber squads in each of its 56 field offices with more than 1,000 advanced cyber-trained agents, intelligence analysts, and forensic examiners.

“Managing the consequences of a cyber attack entails minimizing the harm that results when an adversary does break into a system. An example would be encrypting data so the hacker can’t read it or having redundant systems that can readily be reconstituted in the event of an attack,” said Shawn Henry, FBI Executive Assistant Director.

“We stay up to date with the current practices of fraudsters and hackers through participation in trade group networking. We also use a third party vendor who continually monitors and protects our network from outside attacks,” said Gemmill.

The best way to stay safe while conducting business online is quite simple, explained Gemmill: be careful what you open and what information you share while online.

“We continually update our online banking module to make security more robust.”

“Never share any personal information on any web site unless it is trusted and has a secure log in feature. Keep virus definitions and security patches up to date. Never open attachments or click links from unfamiliar sources,” said Gemmill.

The Rockville branch of John Marshall Bank is planning a security symposium with the FBI and Montgomery County businesses to address threats and educate the public. It will be held in the first quarter of 2012. For more information, call Ed Harrington, Maryland/DC Regional President at 301-738-0030. ★ *February 2012*