

AMERICAN BANKER

On Focus and In Depth

Viewpoint: Web Fraud's Inevitable But Containable

Friday, May 11, 2007

By Jon Fisher

I recently saw a "Dateline" where Chris Hansen used bait credit cards and a fake online store in a feature on identity theft. It was just one of the many recent reports on how fraudsters are becoming more ingenious in exploiting the Internet.

We've all seen the numbers by now. Experts estimate there's a charge made with a stolen credit card number once every 4 seconds, thousands of times a day, millions of times a year. Fraud related to identity theft cost Americans \$53 billion last year.

Every year these scams grow in scope and sophistication. In 2007 we face botnets, spear-phishing, Spit (spam over Internet telephony), cybersquatting, and domain "kiting," to name a few. As quickly as security practitioners thwart burgeoning threats by implementing new technologies, the attackers develop more resilient techniques.

Can anything be done to preserve the future of Internet commerce, or are we doomed to failure?

In a strategic plan released last month by the president's Identity Task Force, the counsel calls for government agencies, private companies, and consumers to band together against Internet scams.

Consumer awareness and stepped-up regulation will help stack the odds in our favor, but as we face increasing threats businesses must fix the core security issues.

Security experts concur that no single silver-bullet technology will allow the defenders to outpace the attackers, but a multilayered approach to Internet security that leverages defensive and offensive solutions can help. Businesses can contain online risks to acceptable levels through a holistic approach, including these basic steps.

Security/risk assessment. As a first line of defense, businesses should perform a thorough review of their IT systems.

Education. Show customers how to recognize basic phishing schemes and avoid attacks that employ social engineering tactics.

Virus protection. With the increase in virus attacks, it is crucial to ensure that servers, workstations, and desktop computers have up-to-date protection installed.

Account origination verification. Businesses should use reliable methods to verify customers' identities before originating accounts online.

User behavior profiling. By tracking the unique characteristics of a user's PC before login, a unique fingerprint for each device can be used to authenticate a user in subsequent transactions.

Risk-scoring engine. To detect fraud, the user's login and online behavior can be profiled. Deviations from expected behaviors could trigger additional authentication requests.

Multifactor authentication (in band and out of band). When suspicious activities are detected, additional authentication — such as an out-of-band communication — can further qualify the legitimacy of a transaction.

Fraud intelligence/modeling. Finally, the industry must turn the tables on scam artists by sharing and analyzing fraud data. With access to up-to-the-moment aggregated information, companies can predict and respond quickly to new attacks, before any damage is done.

There is too much at stake for legitimate businesses and consumers in this fight. By working collectively and individually, we can provide the safeguards and education required to protect consumers and maintain trust in the Internet.

Mr. Fisher is the chief executive officer of Bharosa Inc., a security technology provider in Santa Clara, Calif.