

Afterthoughts

>> The Online War: 'Us Versus Them'

BY JON FISHER

I recently viewed a Dateline episode on television where correspondent Chris Hansen hunts down identity thieves using bait credit cards and a fake online store. It is just one of the many recent news items that confirm fraudsters are becoming more ingenious in their exploitation of the Internet as a breeding ground for fraud to extract billions of dollars annually from unsuspecting consumers and businesses.

So as we move into the era of Web 2.0 and the brave new world of online commerce, we are all left to wonder who will prevail, them or us?

We all have seen the numbers by now. Experts estimate there is a phony charge made with a stolen credit card number once every four seconds, thousands of times a day, millions of times a year. Identity-theft-related fraud cost Americans

\$53 billion last year. Computer viruses, worms and phishing attacks are so commonplace that announcements of new fraud techniques hardly resonate in the

daily news cycle.

Every year, the means by which attackers can abuse the Internet for fraudulent purposes increases 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 and improved technologies, the malicious attackers rapidly adapt and develop more resilient attacks. So can anything really be done to preserve the future of Internet commerce, or are we doomed to failure?

Some predict that we are destined to surrender the Internet to a state of lawlessness where no consumer will dare to conduct transactions unless we restake our claim.

But how?

In a strategic plan released by the President's Identity Task Force in April, the counsel calls for government agencies, private companies and consumers to work in collaboration to address the battle against Internet fraudsters.

Consumer awareness and increased regulation will help stack the odds in our favor. But as we face increasing threats, including man-in-the-middle attacks, Trojans and other forms of malicious software, businesses must resolve to fix the core security issues that fraudsters exploit versus taking the Band-Aid approach of the past.

Respected security experts concur that no single silver-bullet technology will allow the defenders to outpace the attackers. But through a multilayered, comprehensive approach to Internet security that leverages both defensive and offensive solutions, the good guys can find the foothold they need to level the playing field.

Criminals always will look for ways to extort money from the unsuspecting. But businesses can contain online risks to acceptable levels by applying a holistic approach.

As a first line of defense, businesses should perform a comprehensive security review of their information-technology systems environment. They also should offer targeted programs to teach customers how to recognize basic phishing schemes and avoid attacks that utilize social-engineering tactics.

With the increase in virus attacks, another key step is to ensure servers, workstations and desktop computers have up-to-date protection installed. As the basis of strong authentication, businesses also should utilize reliable methods to verify customers' identities before originating new accounts online. For example, they could track the unique characteristics of a user's personal computer before he logs in. A unique "fingerprint" for each device can be used to authenticate a user in subsequent transactions.

Finally, the industry must turn the tables on fraudsters 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 damage is done. **CP**

Jon Fisher is CEO of Bharosa Inc., a Santa Clara, Calif.-based company that provides fraud-detection and multifactor authentication services. He can be reached at jfisher@bharosa.com.

