

Chameleon Network

From: Karl B. Jessen
VP Hardware Development and Market Research
Chameleon Network Inc.

For more information contact:
Helen Sullivan
Inhouse Communications, LLC.
(703) 847-9702
Email: hs@inhouse-com.com

BACKGROUND FOR FINANCIAL AND TECHNOLOGY EDITORS:

THE “PHISHING” THREAT—AND A SOLUTION

January 28, 2004

Phishing – The Latest Form of Financial Fraud on the Internet

One of the newest forms of financial fraud being perpetrated on the Internet involves phishing, a scam designed to fool people into submitting personal, financial or password data. Victims often supply the data—which is used to steal identities and commit other crimes—after being directed by an official-looking email to a replica of a financial institution’s Web page. The term “phishing” reflects the method of the fraud: *fishing* for data online to create *phony* identities for use in criminal activity.

Avoid Becoming a Phishing Victim

At present, banks and brokerage firms are limited in what they can do to prevent a customer from becoming a phishing victim. Their principal defense is dissemination of information about the nature of the fraud. Many institutions (Citibank, Bank of America and Fidelity Investments, among others) are warning customers about the risk and

providing detailed advice to help them discriminate between legitimate emails with bona fide bank or brokerage Website links, and fraudulent ones. However, many consumers fail to take the time to follow such steps or misread the indicators. Others simply ignore legitimate marketing email as part of a less discriminatory, but easier to implement, response to the phishing threat. The result? Fewer responses to legitimate emails, more time required for customers to validate emails and more fraud due to phishing.

Banks and other firms are also taking steps to reduce the amount of phishing fraud. Tumbleweed Communications recently launched the Website Anti-Phishing.Org with the participation of several banks. (The majority of phishing e-mails *appear* to come from financial institutions.) Bank of America and Wells Fargo were among the first banks to team up with Anti-Phishing.Org, but its list of partners today includes many technology companies, which are working together to accept complaints and help to track down fraudulent sites.

Chameleon Network's Solution

The Pocket Vault System, an electronic portable wallet that docks to a PC, effortlessly prevents phishing fraud, while maintaining customer trust and improving customer email response rates. The Pocket Vault System provides transparent authentication of the email source/website and consumer to one another for all Website partners, without imposing any new time-consuming task on the consumer. As a result, the Pocket Vault System will prevent the fraud before it occurs, provide a simple way to measure email effectiveness and restore confidence in financial institutions' email marketing campaigns.

The Pocket Vault System can also be used offline in any retail store or financial institution (including ATM's), allowing consumers to use their existing debit and credit accounts more securely in any environment. Our own company, Chameleon Network Inc. in Concord, MA, is developing the Pocket Vault System, which is expected to be available later this year.

The Pocket Vault System is an electronic PDA-sized device with a color touch screen and a fingerprint sensor. It holds a single credit-card-sized card – the Chameleon Card – that can change identity at the direction of the consumer, taking on the characteristics of nearly any of his or her own legitimate cards, thereby replacing nearly all of the paper and plastic cards cluttering the owner's wallet. The Chameleon Card can be used at any ATM and in any retail store that accepted the original issued paper or plastic card. So in addition to its online anti-phishing benefits, it can improve a consumer's sense of security and convenience with everyday wallet-based activities.

The Pocket Vault System Can Prevent Phishing

After initial set-up, the Pocket Vault is configured to securely validate any ostensible Chameleon Network partners' Website to a bona fide Pocket Vault holder/financial institution customer and to also validate the Pocket Vault holder to any Chameleon Network partner's Website. For example, if a Pocket Vault holder received what appeared to be a valid email with a link to Citibank.com and clicked on the link, the consumer would then be confronted with a non-obvious fraudulent request for secure information to "log on." Since the consumer would be accustomed to logging on to the financial institution's Website with the Pocket Vault, and since the fraudulent Website

could not successfully respond to the Pocket Vault authentication sequence, it would be clear to the consumer that the Pocket Vault was unable to set up the normal secure session. The Pocket Vault, unable to set up the parallel secure session, would throw up a warning to the Pocket Vault holder, prior to any exchange of confidential information.

Economic Benefits of the Pocket Vault Solution

The Pocket Vault System will not eliminate credit card fraud, but it could empower consumers, enabling an effective response to phishing, presentment fraud, skimming and identity theft. Chameleon Network expects that its partners will attain these savings, in addition to a net savings in operating costs from reduced card issuance and marketing costs. The payback to partners for integrating Pocket Vault authentication services should be under two weeks for the typical partner, just based on reduced pin number administration costs.