



For additional information:

Steve Pace
ChosenSecurity, Inc.
(781) 559-3312
info@chosensecurity.com

Mark Cautela
Schwartz Communications, Inc.
(781) 684-0770
chosensecurity@schwartz-pr.com

ChosenSecurity Advises Companies to Restructure Customer Communications to Combat Phishing

Few companies inform customers about new options for secure mail dialoguing

NEEDHAM, Mass.—December 20, 2006—ChosenSecurity, Inc., a leading specialist in identity verification and security services, today announced three essential steps for protecting customer communications from damaging phishing incidents, in response to the rising number of phishing attacks. The Anti-Phishing Working Group (APWG) logged just under 12,000 phishing websites active online in May and in July that figure jumped to 14,191 – with the upward trend continuing.¹

As the number of phishing incidents rise, both the phishing websites and fraudulent e-mails that originate from them are becoming more professional, and appear deceptively authentic. As a result certain industries, including the banking and financial sectors, can not effectively employ e-mail as a communication tool without recipients doubting its authenticity.

ChosenSecurity currently offers Gateway and Team Certificates to help businesses send secure e-mail that customers can readily identify as having originated from a trusted company. The noted specialist for digital certificates and IT security solutions also states that while many companies already actively protect their employees against phishing, they neglect to inform their customers about the security measures in use. ChosenSecurity advises each and every company to follow these three rules in its customer communications, so that customers are no longer left to decide for themselves whether shared mail traffic is trustworthy:

- **Deploy an e-mail signature as basic protection against phishing attacks:** Companies should digitally sign their e-mails. This inexpensive precautionary measure entails no extra work for senders or recipients and is forge-proof. A signature combined with the attendant certificate lets the customer verify the e-mail sender, whether the e-mail is authentic and if it is sent from their bank, insurance company or Internet service provider.
- **Engender trust with open-ended communication:** Companies should inform their customers immediately that they will be receiving exclusively signed e-mails and can safely assume that any unsigned email could not have originated from

¹ “APWG Phishing Report” July 2006; can be downloaded at <http://www.antiphishing.org>

the purported sender. Customers can adapt their behavior accordingly in terms of reading their e-mail and protecting themselves from falling victim to a phishing attack.

- **Allay customer uncertainty with an information campaign:** It is important that companies explain to their customers clearly and specifically what a signed e-mail is and how they can recognize a signed message. A screenshot of a signed e-mail or signature can make it easier for customers to perform a self-check on received e-mails, also helping them to view the security measure as an added customer service and making them willing to accept any extra effort on their part in exchange for greater security.

“Around 94 percent of all phishing e-mails pretend to be from financial institutions, but the creativity of the online counterfeiter is unending,” said Neal Creighton, ChosenSecurity CEO. “Accordingly, all companies should protect their customers’ interests and take effective, coordinated security measures. That’s the only way businesses can maintain their customers’ trust, as well as protect their customers’ identities from being hijacked for criminal activities.”

ChosenSecurity offers a range of anti-phishing certificate solutions for companies of every size. Information about the individual solutions and about how companies can deploy e-mail signatures is available at <http://www.chosensecurity.com>

About ChosenSecurity

ChosenSecurity, Inc. is a leading specialist in identity verification and security services that ensure safe and secure online communication and transactions. Since 1997, the company, previously a subsidiary of GeoTrust, has offered certificates and security solutions along the entire value chain of identity verification. The ChosenSecurity portfolio includes certificates that enable secure access to and encryption of transactions and data; technology for the reliable authentication of users, applications and computers; PKI and smart card solutions that secure access to corporate networks and applications; managed security services; and comprehensive consulting services. With over 3,000 customers across the globe and headquartered in Needham, Mass., ChosenSecurity is a true leader of certification service providers at the forefront of identity management. For additional information, please visit www.chosensecurity.com.

#

All product names are trademarks or registered trademarks of their respective owners.