



For Immediate Release:

Media Contacts:

Joan Lockhart
GeoTrust, Inc.
781-292-4153
joanl@geotrust.com

Bill Keeler or Liz Serotte
Schwartz Communications, Inc.
781-684-0770
geotrust@schwartz-pr.com

GeoTrust Publishes White Paper to Alert Internet Users to New Phishing Vulnerability that Will Enable Highly Convincing Attacks

Netcraft Survey Shows Second-Generation SSL Certificate Authentication, Which Mitigates Phishing Risk, is Growing Twice as Fast as Manual Processes

NEEDHAM, Mass.—April 12, 2005—GeoTrust, Inc., a leader in identity verification solutions for e-business and the world's second largest issuer of SSL (secure sockets layer) certificates for web security, today released a white paper entitled "*Vulnerability of First-Generation Digital Certificates and Potential for Phishing Attacks and Consumer Fraud*" that describes new risks for fraud associated with first-generation authentication, which is still used by some certificate authorities (CAs). GeoTrust also cited the results of the April 2005 Netcraft study that showed second-generation SSL certificate authentication methods, which GeoTrust pioneered, are growing at a rate twice that of first generation manually-based authentication processes.

The April Netcraft survey marks the first time that the internet research firm has segmented the market for SSL certificates based on the validation methods of the certificate authorities into "domain-validated" and "organization-validated" categories. Over the past six months, second-generation domain-validated certificates have outsold first-generation organization-validated certificates by more than two to one, accounting for more than 70% of the growth in the SSL market.

"I'm pleased to see VeriSign's *thawte* brand and other CAs join GeoTrust in adopting second-generation authentication practices, because it's making online commerce safer for consumers," said Howard A. Schmidt, former White House cyber security advisor and previous CSO of both Microsoft and eBay. "Manual vetting of organizations creates a huge vulnerability that can be used to the benefit of phishers and identity thieves. I hope that certification authorities who are still using first-generation processes will understand why they should migrate to advanced authentication without delay."

GeoTrust's second-generation authentication technology utilizes automated domain control, email and telephone validation, combined with sophisticated fraud-detection algorithms, to virtually remove the potential for web merchant fraud and eliminate significant phishing holes created by more vulnerable organizational vetting processes.

David Jevans, chairman of the Anti-Phishing Working Group, said: "We applaud this effort. The organizational field vulnerability represents an opportunity for phishing that needs to be addressed. We are pleased to see CAs moving to processes that better protect consumers."

Organizational Vetting Opens the Door for Online Scams

Organization-validated certificates are not only prone to human error; they present a huge opportunity for fraud. For example, virtually anyone can obtain a certificate with almost any company name from a certificate authority using manual vetting. This makes it easy for a disreputable person or entity to request a certificate in a well-known company name, and then create a phishing site to defraud consumers. This could become a large risk when viewed in a browser that displays the organization name along with the SSL lock as an indicator of a web site's legitimacy.

The following example illustrates the dangers of relying on organization validation for SSL certificates. A company, Seaside Details, obtained a certificate with the organization name "Charter One." To the consumer viewing this with a browser that displays the organization name, the SSL lock displays next to Charter One, leading the consumer to believe it's a trusted and secure site. However, a disreputable party could easily copy or recreate the well-known bank's site and "phish" for consumers' user names and passwords.

To view this site, go to <http://www.geotrust.com/resources/advisory/sslorg/index.htm> where this, and several other spoofed site examples are available.

White Paper Presents Technical Detail, Case Studies

Further details, as well as several other examples of the vulnerabilities, are detailed in GeoTrust's white paper entitled "*Vulnerability of First-Generation Digital Certificates and Potential for Phishing Attacks and Consumer Fraud.*" GeoTrust is issuing this paper to help certificate authorities understand the importance of migrating to the advanced authentication standards used in second-generation vetting processes. It also warns consumers about the danger of relying on the organizational name in a certificate as an indication of a web site's legitimacy.

The white paper, written by noted expert on secure sockets layer certificate verification Kirk Hall, examines the traditional, paper-based manual vetting process, or organizational assurance vetting, still employed by some certificate authorities. The white paper uses examples showing how easy it was to obtain a valid SSL certificate with a well-known company name that could then be used by a phisher on a fraudulent site. The paper further illustrates that relying on organizational names to determine a site's legitimacy is flawed because valid organizations can share the same company name.

The GeoTrust white paper contrasts the two major vetting processes that are used by CAs to validate organizations before an SSL certificate is issued. It examines the differences between

the paper-based, manual, “organization-validated” approach employed by some certificate authorities and the “domain-validated” advanced authentication, second-generation approach used by GeoTrust and VeriSign’s *thawte* brand.

A copy of the white paper, “*Vulnerability of First-Generation Digital Certificates and Potential for Phishing Attacks and Consumer Fraud*,” can be obtained at the Anti-Phishing Working Group’s website, <http://www.antiphishing.org/resources.html> or at GeoTrust’s website, http://www.geotrust.com/resources/white_papers/pdfs/SSLVulnerabilityWPcads.pdf. Interviews with GeoTrust CEO Neal Creighton, author Kirk Hall, cyber security expert Howard Schmidt and Anti-Phishing Working Group chairman David Jevans can be arranged by contacting Bill Keeler at Schwartz Communications, 781-684-0770.

About GeoTrust, Inc.

GeoTrust is a leader in identity verification and trust services for e-business. Its products include web security services for secure e-commerce transactions, identity verification, managed security services and TrustWatch (www.trustwatch.com), a free toolbar and search site that helps consumers recognize whether a site has been verified and is safe for the exchange of confidential information. With more than 70,000 companies in over 140 countries using its technology for online security, GeoTrust has rapidly become the second largest digital certificate provider in the world. Visit www.geotrust.com.

About Netcraft

Netcraft is an Internet services company based in Bath, England. It has explored the Internet since 1995 and is a respected authority on the market share of web servers, operating systems, hosting providers, ISPs, encrypted transactions, electronic commerce, scripting languages and content technologies on the internet. For additional information, visit www.netcraft.com.

About the Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) is focused on eliminating the problem of phishing and email spoofing attacks, by developing and sharing information about the problem, and promoting the visibility and adoption of industry solutions. Membership in the group is open to qualified financial institutions, corporations, law enforcement agencies, public policy groups and solution vendors. www.antiphishing.org.

###

GeoTrust is a registered trademark of GeoTrust, Inc. All other product names are trademarks or registered trademarks of their respective owners.