



Low Assurance SSL-based Phishing Attacks Against Banks and Credit Unions on the Rise

Comodo Inc, February 17, 2006

URL: <http://www.pr9.net/comp/development/3499february.html>

Latest cases expose vulnerability of low assurance, Non business verified SSL certificates

PR9.NET February 17, 2006 - Jersey City, NJ - Comodo Inc., a global leader in Identity and Trust Assurance (ITA) Management solutions, announced today a new initiative to help consumers re-establish trust in online interactions which has been eroded through the issuance of low assurance SSL certificates. Comodo's new technology called SVT (See. Verify. Trust.) is being incorporated into its VerificationEngine (VE), a free downloaded reader that gives consumers the ability to verify Web content with a simple mouse roll over. Consumers can use VE today to authenticate the site logos of many financial and company sites.

Today, phishing, pharming and online fraud are growing as fast as online sales, which topped \$136 billion in 2004 according to Forrester. Particularly hard hit are smaller financial institutions like banks and credit unions as they are the new "soft target" or favorite of fraudsters as recently reported by The Washington Post, http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html

This type of threat is part of a growing vulnerability directly related to the flood of low assurance SSL certificates that recently entered the market. These low assurance certificates do not validate the legitimacy of the business entity, but rather these low assurance providers rely on automated validation processes which only check to be sure the applicant has control over the domain but does nothing to establish the legitimacy of the business. As a result, fraudsters have a new, easy channel to procure the important gold padlock trust symbol to provide a veneer of legitimacy to their site. These low assurance SSL certificates are damaging to the Internet Trust Model because consumers have no effective means to distinguish between a legitimate and fraudulent business.

"Comodo SVT is a revolutionary approach to authenticating Web content. With SVT technology deployed, the credit union discussed in the Washington Post article could have helped their customers mitigate the threat of this phishing attack," said Melih Abdulhayoglu, President and CEO of Comodo. "Consumers can now avoid most phishing and pharming attacks with a new level of free downloadable security. By making this accessible to all consumers, we believe that Web content verification will become a trusted and standard part of a consumer's online process. This will go a long way to reestablishing trust so consumers can feel more confident when doing business online."

High Assurance SSL certificates, like those issued by Comodo, validate the business legitimacy of the Website through established PKI (Public Key Infrastructure) security processes. These types of certificates are issued by Certification Authorities who adhere to strict standards to authenticate the validity of the business behind the Website. With this type of business legitimacy vetting process, any phisher attempting to obtain an SSL certificate (and the trusted padlock icon) would be stopped.

Comodo's SVT technology provides consumers with an effective, "spoof-proof" means to establish trust, authenticate identities and ensure a trusted transaction. The downloadable Verification Engine (www.vengine.com) distinguishes between "good" high assurances and "bad" low assurance padlocks. This level of authentication occurs automatically when a consumer goes to a secured or "https" session from an unsecured Web page by displaying indicators,

Secondly, during the browsing and transaction processes, consumers can verify specific Web content to verify site identity and authenticity. To authenticate content, consumers simply roll their mouse over the content they want to authenticate and they will see a highly visible "green is good to go" border on verified content - virtually eliminating phishing and pharming trust threats. Importantly, since the verification process takes place outside the browser, it protects consumers from mimic sites and attacks.

###

About Comodo Inc

Comodo, through its group of Internet security companies, is a leading Certification Authority and global provider of Identity and Trust Assurance services on the Internet. Comodo secures and authenticates online transactions and communications for over 1,000,000 business and millions of consumers. With a global presence in the US, UK, Ukraine, and India, Comodo offers businesses and consumers third-generation solutions for intelligent security and authentication technologies that create trust online. Comodo's technological expertise includes PKI digital certification, integrated authentication infrastructure services, regulatory compliance solutions and digital e-commerce services. The Comodo companies develop technologies that address critical authentication and security needs with proven and reliable solutions such as SSL certificates, Mutual Authentication solutions, PCI compliancy services, Desktop Security, Code signing certificates, identity and vulnerability management solutions.

Phone: 1 888 266 6361
FAX: 1 201 963 9003
Website: <http://www.comodogroup.com>
E-Mail: media-relations@comodo.com

Address: 525, Washington Blvd,
Jersey City
NJ 07310
USA

[PR9.NET - Your Free Press Release Service](#)