

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

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

Jersey City, NJ (February 16, 2006) - 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, "spooof-proof" means to establish trust, authenticate identities and ensure a trusted transaction. The downloadable Verification Engine (www.venigne.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 following indicators,



Low assurance indicator when Entering a site whose business Legitimacy has not verified



High assurance indicator when Entering a site that has been Verified as legitimate.

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

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet, with over 200,000 customers worldwide. Headquartered in Jersey City, NJ with global offices in the UK, Ukraine, Norway and India, the company offers businesses and consumers the intelligent security, authentication and assurance services necessary to ensure trust in online transactions.

As a leading Certification Authority, and in combination with the Digital Trust Lab (DTL), Comodo helps enterprises address digital ecommerce and infrastructure needs with reliable, third generation solutions that improve customer relationships, enhance customer trust and create efficiencies across digital ecommerce operations. Comodo's solutions include integrated Web hosting management solutions, infrastructure services, digital e-commerce services, digital certification, identity assurance, customer privacy and vulnerability management solutions. For additional information on Comodo - Creating Trust Online™ - please visit: www.comodogroup.com.