A Quarter of Europe’s Largest Banks Do Not Use Best-Practice Security Measures to Protect Against Phishing

Submitted by: Sectigo
Thursday, 27 June 2019

Sectigo Analysis Reveals Gaps for Security-Conscious Customers Using Online Banking Services

ROSELAND, N.J. – June 27, 2019 – Sectigo (formerly Comodo CA), the world’s largest commercial Certificate Authority (CA) and a provider of purpose-built and automated PKI management solutions, today released findings from its latest Secure Impressions: Online Banking Study, revealing how well the world's largest banks (https://www.spglobal.com/marketintelligence/en/news-insights/research/the-world-s-100-largest-banks) in North America and Europe ensure and demonstrate security of customer information on their online banking websites. The study found that a notable percentage of banks left customers vulnerable to phishing scams.

Sectigo rated websites based on the presence of SSL certificates (https://searchsecurity.techtarget.com/definition/digital-certificate) - verifications provided by a Certificate Authority (CA), which confirm that a website is authentic and legitimate. In North America, 40% of banks studied did not receive the highest rating, exemplified by the use of Extended Validation (EV) certificates to demonstrate the website’s true, authenticated identity. In Europe, 25% of banks did not receive the highest rating.

Sectigo rated each bank’s website according to the type of certificate used to secure the home and login pages for the bank’s online banking service. Full marks (green status) were awarded for the presence of Extended Validation (EV) SSL certificates and the maximum level of identity verification on the home and login pages.

Websites without an EV certificate on the home and/or login pages, received a lesser rating (yellow status). No banks in the study displayed “Not Secure” warnings, which would warrant a red status.

Given the extent and value of personal and financial data managed by the world’s leading financial services companies, and the fact that 76% of data breaches are financially motivated (https://searchsecurity.techtarget.com/definition/digital-certificate), it is critical for banking customers to feel assured of the authenticity of their bank’s websites. In fact, 90% of consumers (https://sectigo.com/uploads/resources/EVCertificates_DevOpsGlobalResearch.pdf) report worrying about having their online financial accounts hacked.

Sectigo has conducted similar Secure Impressions studies for the world’s top travel (https://sectigo.com/blog/how-to-make-sure-the-travel-sites-you-visit-are-safe) sites, as well as the UK’s most popular retail e-commerce sites.

“Online criminals routinely use counterfeit websites to trick consumers into unknowingly providing valuable information such as account logins, credit card numbers, and personally identifiable information that can be used for identity theft,” said Tim Callan, Senior Fellow, Sectigo. “To give customers peace of mind, financial institutions can deploy Extended Validation

(https://en.wikipedia.org/wiki/Extended_Validation_Certificate) SSL certificates to communicate the bank's verified identity to site visitors right in the browser's interface. The findings of our study serve as a reminder for banks to pay attention to their online presence, not only to protect customers from phishing, but also to convey that necessary protections are in place.

Added Protection from Phishing

Phishing and pretexting represent 93% of breaches (https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-2018.pdf). Phishing is a cyberattack that is designed to fool a victim into believing the phisher is a specific, trusted party for the purpose of stealing credentials, accessing sensitive data, or propagating malware. EV, indicated by a company-branded address bar, helps to increase site transactions and protects users against phishing. EV shows customers that the website employs the best-of-breed security measures to protect transactions and ensure compliance with standards and regulations.

Eight out of 10 (https://sectigo.com/uploads/resources/EVCertificates_DevOpsGlobalResearch.pdf) people report that the presence of EV influences their perception of a brand or company and half indicate it has a significant influence. EV SSL validates that the identity of the certificate owner is reliably authenticated using the best practices available. Before issuing an EV certificate, the issuing CA must perform a specific, audited authentication process using techniques that are proven effective based on a decade of industry-wide use.

Tips for Online Banking Customers

When completing any online transaction or engaging with email, Sectigo recommends that customers:
- Look for the full company name at the left of the address bar to ensure the site is really part of the intended online business.
- Never input credit card numbers, personal information, logins, or other sensitive data on any web page that is not secured with a certificate.
- When using email, avoid clicking on links in unsolicited, inbound emails to avoid phishing scams.

About Sectigo
Sectigo (https://sectigo.com/) (formerly Comodo CA) provides award-winning (https://sectigo.com/awards) purpose-built and automated PKI management solutions to secure websites, connected devices, applications, and digital identities. As the largest commercial Certificate Authority, trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. For more information, visit www.sectigo.com (https://sectigo.com/).

# # #

Contact
Inés Mitsou

Positive Marketing
+44 (0)20 3637 0640
imitsou@positivemarketing.com