CA Security COUNCIL
www.casecurity.org

LONDON PROTOCOL

Joint Certification Authority (CA) Voluntary Protocol to Reduce Phishing On Identity Websites

6 June 2018 - Version 1.6

Objective of Protocol: To improve identity assurance and minimize the possibility of phishing activity on websites encrypted by OV (organization validated) and EV (extended validation) certificates (together referred to as "Identity Websites"). The London Protocol reinforces the distinction between Identity Websites making them even more secure for users than websites encrypted by DV (domain validated) certificates. That security feature can then be utilized by others for their own security purposes, including informing users as to the type of website they are visiting and use by antiphishing engines and browser filters in their security algorithms.

How the Protocol Will Be Implemented: The London Protocol will be implemented through voluntary action by public Certification Authorities (CAs) working jointly to take the following steps:

(1) Actively monitor phishing reports for websites encrypted by the CA's own OV and EV certificates;

(2) Notify the affected website owner that phishing content was found and provide remediation instructions as well as prevention methods;

(3) Each CA will contribute to a common database to help reduce future phishing content. This data will be available to other participating CAs so that each CA can conduct additional due diligence before issuing new OV or EV certificates to the website.

Sources of Phishing Data for Encrypted Websites: The CAs who are voluntary members of the London Protocol will collaborate to find the most reliable sources of anti-phishing data useful in implementing the protocol.

Public Reports: Data and results will be shared among participating CAs. Those who find the information useful will be encouraged to utilize it in their own security processes. Additionally, those who use this data will be encouraged to provide feedback on how this data can be improved to better serve the ecosystem.

From time to time the participating CAs will compile statistics and other information collected during implementation and publish the results to the CA/Browser Forum and to the media.

Protocol Phases: This London Protocol will be implemented in four phases:

Phase 1 (June - August 2018): Official announcement of Protocol and participating CAs. Participating CAs further develop Protocol details and research feasibility of implementation and may begin to implement some basic procedures.

Phase 2 (September - November 2018): Participating CAs apply Protocol concepts to their own customers' Identity Websites according to their own policies and procedures, share feedback with other participating CAs, refine Protocol as warranted by experience.

Phase 3 (December 2018 - February 2019) Participating CAs update Protocol policies and procedures and approve plan for uniform policies and procedures to be applied by all participating CAs on a voluntary basis.

Phase 4: (March 2019) Participating CAs forward report and recommendations to CA/Browser Forum for possible changes to Baseline Requirements.

Antitrust Laws; Withdrawal by CAs: The participating CAs will comply with all applicable antitrust laws, including the limitations specified by the Antitrust Notification read aloud prior to CA/Browser Forum meetings. Participating CAs may withdraw from this Protocol at any time upon notice to the other participating CAs.

The following Certification Authorities have agreed to follow this London Protocol as of June 6, 2018 (listed alphabetically):

Founding Participants in the London Protocols:

1. *Comodo CA*
2. *Entrust Datacard*
3. *GlobalSign*
4. *GoDaddy*
5. *Trustwave*

Other Participants in the London Protocol:

[Additional CA names to be added]