Содержание

Введение

Этот документ описывает использование homoglyph символов в усовершенствованных фишинговых атаках и как знать о них при использовании сообщения и фильтров контента на Cisco Email Security Appliance (ESA).

Homoglyph усовершенствованные фишинговые атаки

В усовершенствованных фишинговых атаках сегодня, электронные почты фишинга могут содержать homogyph символы. homoglyph является текстовым символом с формами, которые почти идентичны или подобны друг другу. Могут быть

Пример сценария может быть следующие: Клиент хочет заблокировать электронную почту, которая имела, содержит URL

Клиент получил пример почтового, содержащего: www. p ? ypal.com

Фильтр контента согласно конфигурации содержит: www.paypal.com

Если вы будете смотреть на фактический URL через DNS, то вы заметите, что они решают по-другому:

Первый URL использует homoglyph буквы? o? из формата unicode.

Если вы смотрите близко, вы видите что первое? o? в PayPal является фактически другим, чем второе? o?.

Знайте при работе с сообщением и фильтрами контента для блокирования URL. ESA не может сказать различие между homoglyphs и стандартными символами алфавита. Один способ должным образом обнаружить и предотвратить использование homoglyphic фишинговых атак состоит в том, чтобы настроить и включить OF и Фильтрацию URL-адресов.

Irongeek предоставляет метод для тестирования homoglyphs и создания теста злонамеренный URL: Генератор Атаки Homoglyph

Подробное введение в homoglyph фишинговые атаки, также от Irongeek: Из Символа: Использование Punycode и Homoglyph Attacks для Запутывания URL для Фишинга