**Что такое SSL-сертификат и почему вашему сайту нужно с ним «подружиться»?**

Представьте себе ситуацию: вы рассказали другу страшную тайну или интересный секрет, а он взял и поделился им с другими. Неприятно, правда? Каким бы странным не было сравнение, но похожая неприятная ситуация может случиться с вами и во время серфинга в сети. Ведь «растрепать» секретики, а точнее личные данные, способны некоторые незащищенные сайты. Думаем, такой ценной информацией о себе или своих клиентах с плохими «дядями» вы делиться точно не захотите. Но защититься от злоумышленников шанс все же есть. И спасибо за это SSL-сертификатам.

SSL (или Secure Socket Layer) – спасительная технология. Она как тайный агент шифрует данные пользователей при передаче их браузером на веб-сервер. SSL-сертификаты всего-навсего небольшие файлы данных, но как говорится: маленькие, да удаленькие. Такой сертификат представляет собой что-то вроде удостоверения личности вашего сайта, доказывающего его подлинность. В этом серьезном документе, указываются своеобразные «Ф.И.О» и «прописка» ресурса, а также многое другое.

«Общение» браузера с сервером, защищенным с помощью SSL, отчасти напоминает встречу двух агентов. Прежде чем передать ценную информацию браузер и сервер обмениваются идентификаторами, подтверждениями и прочим. В итоге данные пользователя отправляются на сервер лишь тогда, когда их шпионские «пароли», «явки» и «отзывы» совпали.

Все эти хитрые технологии понятны специалистам. Но как же обычному пользователю «вычислить» защищенный сайт? Довольно просто! Видели когда-нибудь значок закрытого замка рядом с URL-сайта или префикс https вместо http? Так вот это и есть нужный маячок!

**Кому стоит «подружиться» с SSL?**

Самое время задуматься, кому же пригодятся все эти околошпионские страсти? На самом деле практически каждому! К примеру, владельцу интернет-бизнеса. Как бы человек не нуждался в ваших услугах, он явно засомневается, если будет подозревать, что его личные данные и сведения о банковских картах могут попасть в руки мошенников. Если же вы дадите гарантию о сохранности информации, то сделаете шажок на встречу к процветанию своего бизнеса.

Ваш сайт к коммерции никакого отношения не имеет? Это не значит, что от «дружбы» SSL вам можно отказаться. Все дело в недавних изменениях работы популярного поисковика Google. Его система теперь внимательно следит за сайтами с префиксами https и в прямом смысле их превозносит. Защищенные ресурсы теперь поднимаются выше среди результатов поиска. Так что если в ваших интересах «обскакать» коллег и конкурентов – использование SSL-сертификата – ваш выбор.

**Такие разные сертификаты**

Ну что, решились обзавестись SSL-сертификатом для своего родного сайта? Тогда давайте определимся, какую из его разновидностей выбрать.

Владельцев небольших проектов может устроить самый бюджетный и быстрый в получении вариант – сертификат с проверкой домена (Domain Validation). Покупая его, вам не придется собирать кучу ~~неопровержимых «доказательств»~~ документов. Нужно лишь подтвердить владение доменом с помощью электронной почты, DNS-записи или через загрузку на сервер специального файла.

Немного больше вопросов к вам появится у центра выдачи сертификатов при покупке сертификата с проверкой компании (Business Validation). Чтобы получить большее доверие от пользователей вам придется предоставить сведения о самой компании и пройти процедуру проверки. Правда есть пара «но» - такой сертификат недоступен для частных лиц и процедура его оформления займет от пары до 10 рабочих дней.

И, наконец, сертификаты с расширенной проверкой (Extended Validation). Они пригодятся особенно серьезным организациям, к примеру, сайтам банков или ресурсам, через которые проходит огромное число посетителей. Процесс получения такого SSL-сертификата более трудоемкий, центр выдачи о-о-очень внимательно будет проверять вашу организацию, но результат того стоит. По итогу в адресной строке URL вашего сайта будет подсвечен зеленым цветом, а рядом будет красоваться название вашей организации. Все это должно стать добрым сигналом для пользователей о серьезной защите вашего сайта.

**Как получить SSL-сертификат**

Все, мы окончательно убедились, что жизнь сайта куда краше с SSL-сертификатом. Осталось разобраться, как же заполучить эту чудо-технологию на свое вооружение.

Если в дальнем уголке вашей души живет маленькая внутренняя жаба, вы, конечно, можете сэкономить на покупке и обзавестись бесплатным самоподписным сертификатом. Вот только пользы от такого будет не много – браузеры будут то и дело нервировать пользователей сообщениями, что ваш сайт не прошел должную проверку. Так что, может, немного раскошелимся? Согласны?

Представим, что с разновидностью сертификата вы определились. Теперь нужно обратиться в центр по их выдаче или к компании-партнеру. В них вам подробно расскажут, какие документы следует собрать для проверки и озвучат стоимость нужного вас сертификата. Уверены, вы успешно со всем этим справитесь и вам останется лишь ждать контрольного звонка от компании (это один из этапов проверки). Если все пройдет гладко, то спустя какое-то время на своей электронной почте вы найдете весточку о готовности SSL-сертификата. Останется лишь скачать его и установить на сервер.

Остались вопросы? Тогда звоните нам: 8(4162)21-23-17. Мы поможем разобраться в премудростях SSL и сделать ваш сайт самым привлекательным и защищенным.