Любовь начинается с безопасности

Большинство людей пренебрегают основными средствами защиты, думая, что с их сайтом ничего не случится. Это большая ошибка.

В 2019 году 60% сайтов были поражены разного рода вирусами. Это на 4% больше, чем в 2018 году.

Если вы примете базовые меры безопасности, клиенты ничего не подхватят на вашем ресурсе, а хакеры не смогут помешать вашим отношениям.

Поощряйте безопасный выбор

👮‍♂️👮

Вашим посетителям могут не нравиться сложные пароли: многие говорят, что с ними неудобно. Но требуя создать такой пароль, вы, прежде всего, заботитесь о данных самих пользователей. Убедите их создать надежный пароль минимум из восьми символов, включая заглавные буквы и цифры. Сначала использовать такой пароль будет неудобно, но сознательные пользователи оценят ваше стремление к безопасности.

Убедитесь, что не передаете ничего вредоносного

🤝✅

Получение сертификата SSL позволит вам перейти на безопасный протокол HTTPS. Сочетание SSL-сертификата и HTTPS гарантирует, что между вашим сервером и браузерами пользователей не передается ничего, кроме зашифрованных данных. Замочек безопасного режима рядом с адресом сайта, как замочек влюбленных на мосту, укрепляет отношения с пользователем.

Используйте барьерную защиту

🌧️☂️

Межсетевые экраны (Firewall) помогут избежать самых распространенных вторжений, включая инъекции SQL и межсайтовый скриптинг. Firewall работает как щит, защищающий от хакерских атак, постоянно отслеживая и анализируя трафик, идущий с сервера вашего веб-сайта.

Регулярно проверяйтесь

🕵️‍♀️👌

Даже если вы все делаете правильно, нет 100% гарантии, что с вашим сайтом все в порядке. Вам по-прежнему нужно регулярно проверять его работоспособность вручную и с помощью специальных инструментов. И если вы не знаете, чем межсайтовый скриптинг отличается от межсайтовой подделки запросов, не стыдитесь обратиться за помощью к профессионалу.

Пробуйте новое

🏋️‍♂️🍑

Держите сайт в чистоте и обновляйте ПО. Хакеры часто атакуют популярное программное обеспечение, потому достаточно найти всего одну щель в системе безопасности, чтобы заразить тысячи сайтов за раз. Каждый апдейт ПО решает такую проблему. Убедитесь, что у вас стоит последняя версия — так вашему сайту ничего не угрожает.

Всегда имейте запасной план

🕯️🧯

Регулярно копируйте все данные, как на внутренний сервер, так и в облако. Если, несмотря на все меры предохранения, ваш сайт заразится, последние резервные копии помогут его восстановить.

Помните: чем дольше — тем лучше

👩‍🦰📆

Чтобы отношения не закончились раньше времени, важно помнить главные даты. Из-за просроченного домена вы можете потерять любимых клиентов, поэтому лучше настроить напоминания об окончании срока.

Иногда хочется сделать все побыстрее, пренебрегая самыми простыми и часто дешевыми средствами защиты. Но если ваша цель — построить долгие доверительные отношения, вы должны позаботиться о безопасности. Будьте партнером, на которого можно положиться ❤

SE Ranking