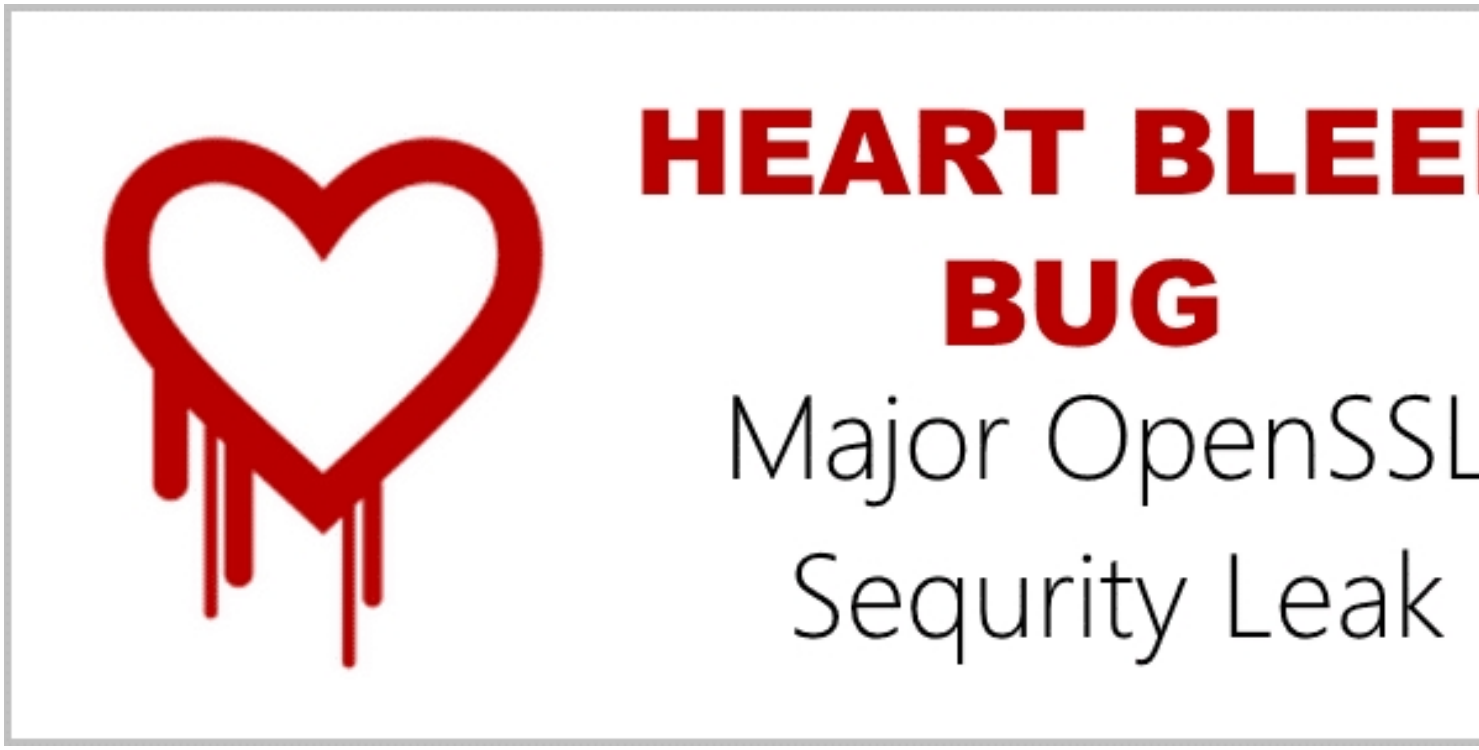
Рассмотрим один из наиболее эффективных способов обеспечения безопасности онлайн.



Ошибка Heartbleed (c) egonsarvreviews.com

В 2014 году ошибка в программном обеспечении OpenSSL под названием Heartbleed сделала уязвимыми сведения о логинах сотен тысяч пользователей благодаря всего-навсего крошечному отрывку кода. В дальнейшем угрозы информационной безопасности стали лишь еще более серьезными. Так, за первую половину 2017 года произошло больше утечек данных, чем за весь 2016 год. В 2018 году ситуация лучше не стала.

Так может ли рядовой пользователь сделать хоть что-то, чтобы уберечь свою информацию? Разумеется, нужно регулярно менять пароли. Однако сам по себе пароль – далеко не самое надежное средство для обеспечения безопасности.

То, что действительно способно помочь вам в данной ситуации – так называемая двухуровневая авторизация, также известная под аббревиатурой 2FA и иными названиями (некоторые из которых приведены ниже). Что же она собой представляет?

Специалисты говорят, что существует три уровня аутентификации. Первый из них основывается на том, что вы знаете (например, пароль). Второй – на том, что у вас имеется (например, аппаратный ключ или ваш мобильный телефон). Третий же – это вы сами (имеется в виду, к примеру, отпечаток пальца). Двухуровневая защита подразумевает, соответственно, использование каких-либо двух из названных опций.

Биометрические устройства для сканирования отпечатков пальцев, сетчатки глаза или лица довольно успешно развиваются благодаря таким инновационным сервисам, как Face ID в iPhone X и Windows Hello. Однако они все же пока являются крайне малораспространенными. В большинстве случаев, двухуровневая авторизация представляет собой всего лишь числовой код, отправляемый на ваш телефон в качестве сообщения, который может использоваться всего один раз.

Face ID в iPhone X (c) extremetech.com

Многие сервисы поддерживают специальные приложения на телефоне под названием «аутентификатор», которые выполняют ту же функцию. Такое приложение, предварительно настроенное на работу с сервисом, имеет постоянно меняющийся набор кодов, которые могут быть использованы в любое время даже без подключения к интернету. Пожалуй, одним из лидеров в данной области является Google Authenticator (доступный бесплатно для Android и iOS). Также на мобильных и некоторых стационарных платформах популярны Twilio Authy, Duo Mobile и LastPass Authenticator. Также двухуровневой авторизацией обладает большая часть популярных диспетчеров паролей.

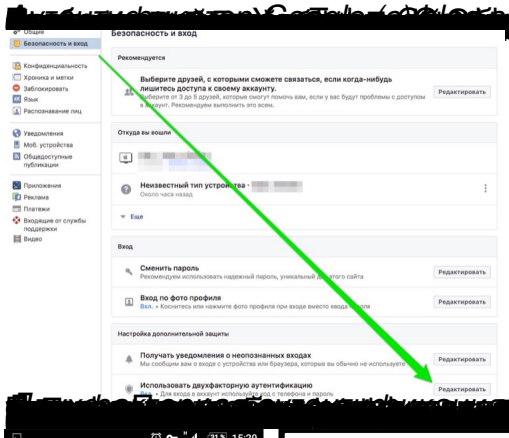
При этом коды из вышеуказанных приложений синхронизируются со всеми вашими учетными записями, поэтому вы можете просто просканировать двумерный штрих-код на телефоне, чтобы получить в браузере шестизначный цифровой код для осуществления доступа (если у вас поддерживается такая функция).

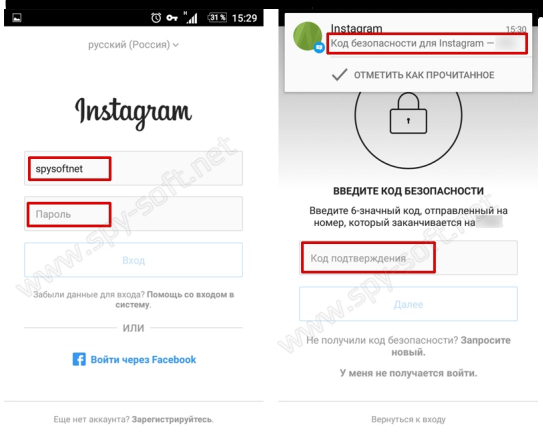
Необходимо помнить, что установка 2FA может нарушить доступ к некоторым другим сервисам. Например, если вы пользуетесь двухуровневой авторизацией от Microsoft, все идет замечательно до тех пор, пока вы не захотите воспользоваться Xbox Live. Дело в том, что данный сервис не поддерживает второй пароль. В таком случае следует положиться на пароли приложений, которые вы генерируете на том или ином сайте для использования в определенном приложении (таком, как Xbox Live). Аналогичные пароли могут понадобиться и в случае с Facebook, Twitter, Microsoft, Yahoo, Evernote и Tumblr.

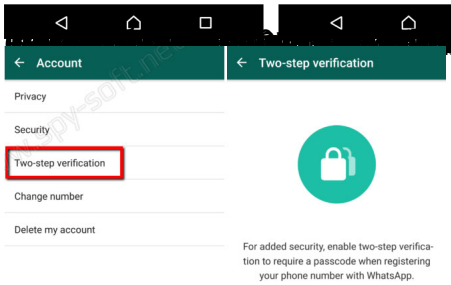
Как бы сложно все это ни звучало, не следует забывать, что обеспечение безопасности никогда не бывает простым. Даже если из-за прохождения двухуровневой авторизации вы потеряете чуть больше времени, надежная защита ваших данных стоит этого.

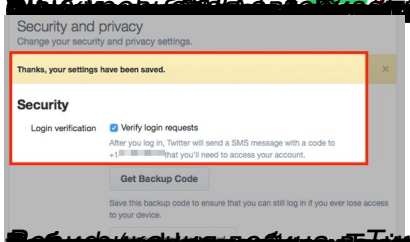
Двухшаговая авторизация в Google

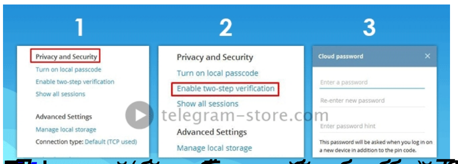
GOOGLE AUTHENTICATOR











Источник

году, так, ли, может, за, лучше, стала, безопасности, ошибка, 2018,