Двухфакторная аутентификация для домашних пользователей

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

Сегодня практически все пользователи используют как минимум 3-5 паролей. Если учесть, что пароль должен быть не менее 8 символов, содержать в себе большие и маленькие буквы, цифры, специальные символы, то есть быть типа Gf+2876#hTG то понятно, что большинство пользователей выбирает себе либо один и тот же пароль для всех служб, либо пароль типа 123456 или Password, что, естественно, негативно сказывается на общем уровне безопасности.

В связи с этим некоторые компании, такие как Google, Facebook, Twitter, Apple, Microsoft вводят системы двухфакторной аутентификации. Что это такое? Двухфакторная аутентификация обычно отвечает на два вопроса:

1. Что я знаю (в нашем случае это пара логин/пароль)
2. Что я имею (в данном случае это некий набор цифр (символов) который вы получаете с помощью SMS на указанный номер телефона.

Как воруют ваши пароли

Если верно хотя бы одно из следующих утверждений, то вы находитесь в группе риска:

- Вы используете один и тот же пароль на разных сайтах
- Вы загружаете программы из Интернет
- Вы нажимаете на ссылки в сообщениях электронной почты

Вместе с тем вам рано беспокоиться. В таких случаях вас защитит двухфакторная аутентификация.

Чем грозит кража пароля

Если злоумышленник получил ваш пароль, то:

- Прочесть ваши сообщения электронной почты, посмотреть ваши личные фотографии или даже удалить их.
- Рассылать спам (вирусы) от вашего имени
- Изменить пароли от других аккаунтов, которые вы используете

Двухфакторная аутентификация в Google

В самом Google данная технология носит название двухэтапной:

1. **Ввод пароля.** Данное действие пользователь делает каждый раз, когда вы входите в аккаунт Google
2. **Ввод кода подтверждения**, который вы сможете получить по SMS, с помощью голосового вызова или приложения, установленного на вашем смартфоне

Вместе с тем **при входе в аккаунт вы можете отметить компьютер как надежный, тогда при входе в аккаунт на данном ПК вводить код подтверждения больше не требуется**. Однако учтите, что **если мошенник (или вы сами) захотите войти в ваш аккаунт с другого ПК, система потребует ввести код.**

Как быть получить код подтверждения

Получайте коды по SMS

Код подтверждения можно получить по SMS/

Добавьте резервные номера

Если у вас разрядился телефон или вы его потеряли, то на резервный номер вы сможете получить код подтверждения.

Используйте голосовой вызов

Вы можете заказать звонок на ваш мобильный или городской номер, чтобы голосом получить необходимый код.

Распечатайте резервные коды

Вы можете распечатать или сохранить резервные коды для входа в аккаунт (однако позаботьтесь при этом о сохранности распечатки).

Генерируйте коды на смартфоне

Установив приложение Google Authenticator на свой смартфон (Android, iPhone или BlackBerry). Вы сможете генерировать коды подтверждения, даже если будете не в сети.

Назначьте надежные компьютеры

Чтобы не вводить код на своем личном компьютере, отметьте его как надежный. Код будет требоваться только при входе в аккаунт с других компьютеров.

Как сделать?

На самом деле настройка двухэтапной аутентификации в Google не вызовет сложностей, поскольку проводится пошагово с помощью мастера.

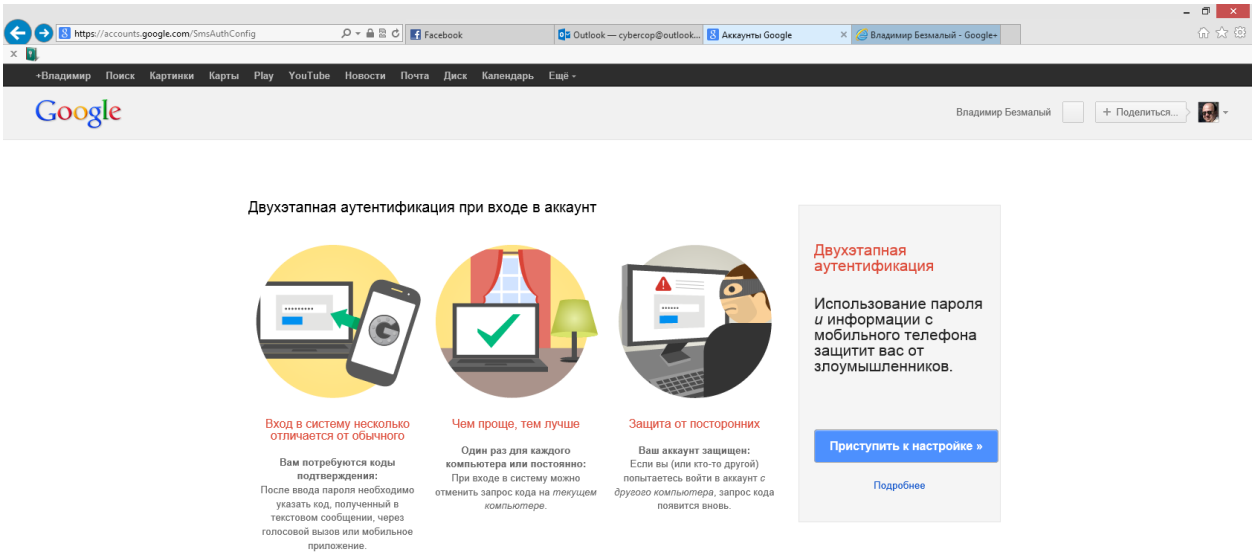

Рисунок 1 Настройка двухэтапной аутентификации при входе в аккаунт

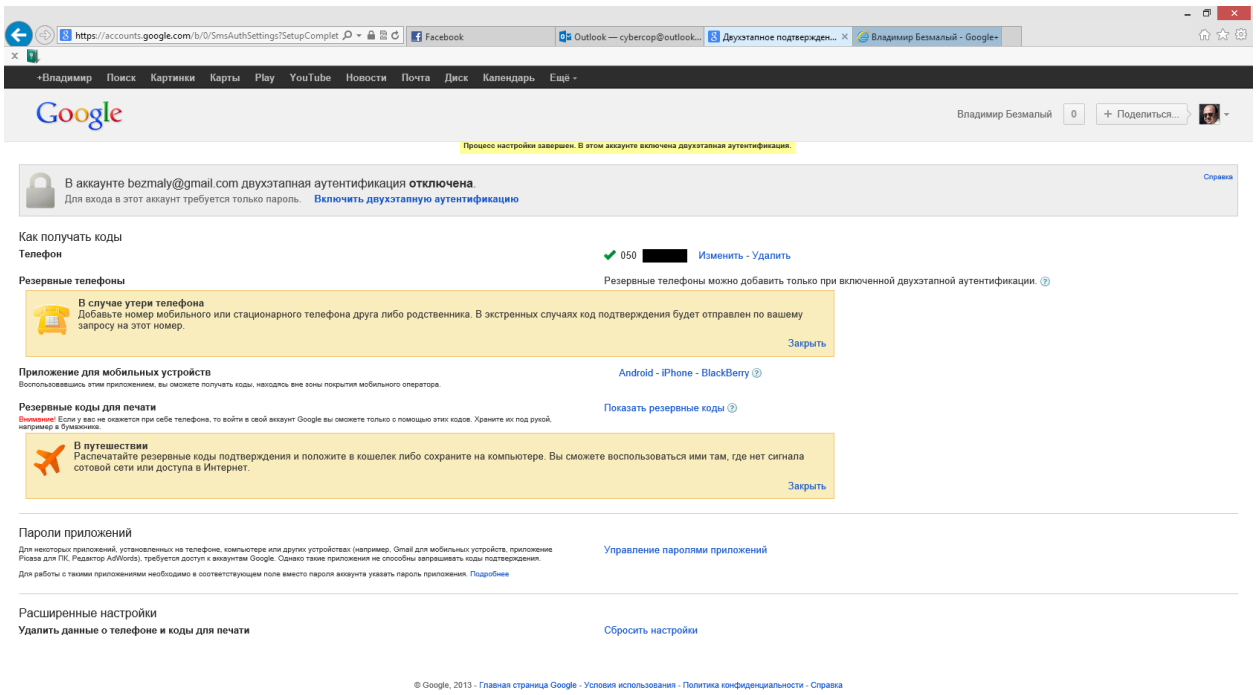

Рисунок 2 Включение двухэтапной аутентификации после настройки

Двухфакторная аутентификация в сервисах Microsoft

Весной 2013 года компания Microsoft объявила о запуске дополнительных мер по аутентификации пользователей для своих онлайн-сервисов.

Необязательная двухфакторная аутентификация для всех доступных профилей Microsoft сделана в традиционной манере, т.е. кроме обычного пароля для входа в учетную запись, пользователю придется ввести дополнительно короткий цифровой код подтверждения.

Для получения одноразовых кодов авторизации компания Microsoft уже выпустила фирменное мобильное приложение Authenticator для платформы Windows Phone. В то же время, компания заявила, что есть и другие средства авторизации для Android и iOS (генераторы кодов), которые уже совместимы с новой схемой двухфакторной проверки личности пользователя от Microsoft. Включить двухфакторную авторизацию нужно лишь один раз – в этом поможет специальный мастер, доступный из личного профиля. В дальнейшем коды подтверждения можно будет получать через SMS или по эл. почте.

Двухфакторная авторизация уже действует для таких сервисов Microsoft, как эл. почта (Outlook.com), Skype, SkyDrive (облачное хранилище файлов), Xbox (игры), подписки Office и онлайн-дополнения к Windows 8.

Так же как и для онлайн-приложений Google, решение от Microsoft позволяет назначить некоторые устройства доверенными, т.е. при авторизации на них от вас не будет требоваться двухфакторной аутентификации. Однако если вы не использовали «доверенное» устройство более 60 дней или постоянно меняете браузеры для доступа к сервисам, вам все же придется ввести контрольный код. При потере смартфона его статус «доверенного» можно отключить через личный профиль в браузере.

Двухфакторная аутентификация в Facebook

Двухфакторная аутентификация в Facebook основана на тех же принципах.

Для настройки необходимо войти в Настройки-Безопасность-Подтверждения входа и далее с помощью мастера настроить подтверждение.

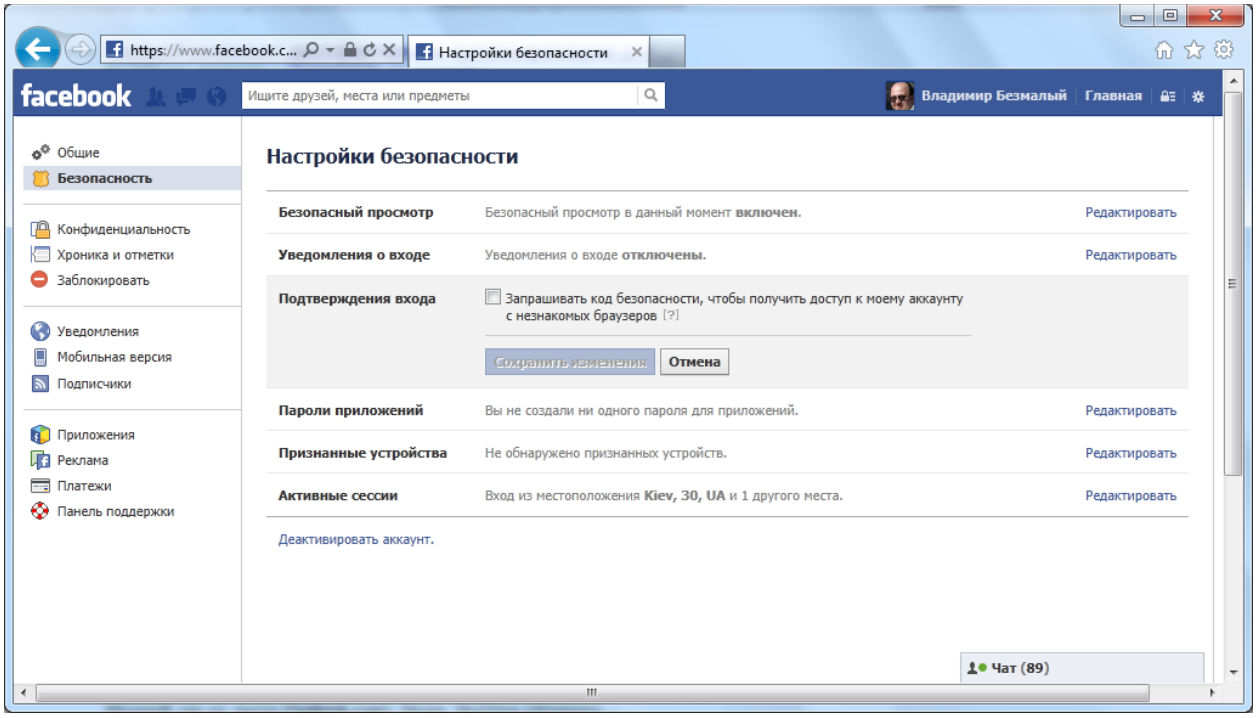

Рисунок 3 Настройка двухфакторной аутентификации в Facebook

Далее процесс настройки осуществляется с помощью мастера и не требует никаких усилий.

Аналогично предыдущим решениям можно указать доверенные ПК.

Заключение

Двухфакторная аутентификация в приведенных сервисах – это, безусловно, шаг вперед в решении проблемы аутентификации. Однако не обойдется, как обычно, без ложки дегтя.

Во всех сервисах заявлена возможность распечатать коды подтверждения «на будущее». На мой взгляд, это плохо. Почему? Да потому что человек теряет такие листы. Хотя, с другой стороны, нужно еще и пароль знать. Все же в любом случае это надежнее чем росто пароль.