Ежемесячный журнал по вопросам компьютерной безопасности

OUCH!

В ЭТОМ ВЫПУСКЕ…

Двухступенчатая Верификация

Кто ты?

Процесс проверки того, кем вы являетесь, (так называемая аутентификация) является основным способом защиты ваших онлайн данных. Необходима уверенность в том, что только у вас есть доступ к вашим личным данным. Соответственно, требуется способ проверки вашей личности, например, для доступа к электронной почте, онлайн покупок или интернет банкинга. Вы можете подтвердить свою личность тремя различными способами: тем, что вы знаете, например, паролем, тем, что у вас есть, например, паспортом, и тем, кем вы являетесь, например, отпечатками пальцев. У каждого из этих методов есть свои преимущества и недостатки. Наиболее распространен способ аутентификации с помощью того, что вы знаете: пароля.

Об авторе

Джеймс Тарала – лектор, автор и старший инструктор Института SANS. Джеймс является ведущим консультантом в компании Enclave Security, участник проектов Critical Security Controls и **AuditScripts.com** С Джеймсом можно пообщаться онлайн в Twitter **@isaudit** или встретиться лично на наших новых курсах.

Пароли

Мы практически каждый день используем пароли. Главная задача пароля – убедиться, что вы тот, за кого себя выдаёте. Это и есть то, что вы знаете. Основной недостаток пароля в том, что кто-то ещё может его узнать или подобрать. Обладая паролем, легко можно выдать себя за вас и получить доступ ко всей информации. Вот почему вы должны тщательно подходить к выбору пароля, например, использовать сильные пароли, которые сложно подобрать. Ещё один недостаток паролей в том, что они быстро истекают. С помощью современных технологий, например, кейлогеров, кибер мошенники легко могут изменить или подобрать пароль. Для большей безопасности необходимо использовать более сильную аутентификацию. К счастью, данная возможность все более доступна – так называемая двухступенчатая верификация. Для лучшей защиты своих данных используйте эту опцию всегда, когда это возможно.

Двухступенчатая Верификация

Двухступенчатая верификация

Двухступенчатая верификация (или, так называемая двухфакторная аутентификация) – один из самых надежных способов защиты идентификации вашей личности. Вместо одного шага аутентификации, например, запроса пароля (того, что вы знаете), требуется два шага. Отличным примером является банкомат. Для того, чтобы снять деньги через банкомат, вы проходите двухступенчатую верификацию. Для того, чтобы подтвердить свою личность и получить доступ к деньгам, вам нужно две вещи: банковская карта (то, что у вас есть) и ПИН код (то, что вы знаете). Даже если вы потеряете карту, то деньги все ещё в безопасности: даже если кто-то найдет вашу карту, то не сможет снять деньги без ПИН кода (только если вы не написали его на обратной стороне карты, что не очень разумно). Тот же принцип и в случае кражи ПИН кода без карты. Злоумышленники должны получить обе составляющих для получения денег в банкомате. Вот почему двухступенчатая верификация более безопасна: она обеспечивает два уровня безопасности.

Двухступенчатая верификация обеспечивает лучшую защиту, чем пароли.

Использование двухступенчатой верификации

Одним из лидеров по использованию двухступенчатой верификации можно назвать Google. В дополнении к множеству бесплатных онлайн сервисов, например, Gmail, Google предлагает более надёжную верификацию для миллионов пользователей. Google внедрил двухступенчатую верификацию в большинстве своих сервисов. Бесплатная двухступенчатая верификация доступна не только пользователям Google: ряд провайдеров использует подобные технологии на своих сервисах, например, Dropbox, Facebook, LinkedIn и Twitter. На примере работы двухступенчатой верификации Google вы легко сможете понять принцип работы двухступенчатой верификации других онлайн сервисов.

Двухступенчатая верификация Google работает следующим образом. Прежде всего, вам потребуется имя пользователя и пароль. Это первая составляющая, то, что вы знаете. Однако Google запрашивает и вторую составляющую – то, что у вас есть - в данном случае, смартфон. Есть два различных способа

Двухступенчатая Верификация

использования смартфона как составляющей процесса аутентификации. Первый способ - регистрация номера на Google. В случае попытки аутентификации с помощью вашего имени пользователя Google отправит смс с уникальным кодом на зарегистрированный номер. Вы сможете войти в аккаунт только с помощью этого кода. Второй способ – установка специальной программы Google, которая будет генерировать для вас уникальные коды. Преимущество второго способа в том, что вам не нужны услуги провайдера, ваш телефон генерирует код сам.

Обычно двухступенчатая верификация не подключается по умолчанию, вам нужно её активировать. Большинство мобильных приложений ещё не поддерживают двухступенчатую верификацию. Для этих мобильных приложений вы можете использовать специфические пароли, которые можете сгенерировать с помощью двухступенчатой верификации. Наконец, вы можете использовать ключи восстановления паролей, если потеряете смартфон. Мы рекомендуем их распечатать и хранить в надёжном месте.

Мы настоятельно рекомендуем использовать двухступенчатую верификацию всегда, когда это возможно, особенно для таких важных сервисов, как электронная почта или хранения файлов. Двухступенчатая верификация обеспечит лучшую защиту, так как злоумышленникам придется приложить намного больше усилий, чтобы взломать ваш аккаунт.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Дополнительная информация

В каких случаях используют двухступенчатую верификацию:
http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two+factor-authentication-right-now

Двухступенчатая верификация Google:
http://www.google.com/landing/2step/

Соварь терминов по информационной безопасности:
http://www.securingthehuman.org/resources/security-terms

Ежедневные советы Института SANS:
https://www.sans.org/tip_of_the_day.php

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова