Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Пароли
- Двухступенчатая верификация

Двухступенчатая верификация

Обзор

Процесс подтверждения вашей личности (так называемая аутентификация) – ключ, защищающий вашу информацию. Сильная аутентификация позволяет получить доступ к данным только вам, например, вход в электронную почту, доступ к фотографиям или к банковскому счету. Существует три различных способа подтверждения личности: что вы знаете – например, пароль, что у вас есть – например, водительское удостоверение, и кто вы есть – например, отпечатки пальцев. У каждого из этих методов есть свои преимущества и недостатки. Самый распространённый метод – пароль; то, что вы знаете. В этом выпуске мы поговорим о двухступенчатой верификации, более надежном способе защиты, чем пароль и довольно простом в применении. Чтобы было понятней, о чем пойдёт речь, сначала поговорим о паролях.

Об авторе

Кит Палмгрен работает в сфере Информационной Безопасности более 30 лет. Он является сертифицированным инструктором Института SANS и автором 5-дневного курса основ Информационной Безопасности SEC301. В свободное от преподавания время Кит проводит консультации или занимается проектами. Ведет блог **@kpalmgren**.

Пароли

Пароль – это способ подтверждения личности, основанный на знании чего-то. Опасность паролей состоит в том что они являются «слабым звеном». Если кто-то угадает или получит ваш пароль, то получит полный доступ к вашим данным, которые были защищены паролем. Вот почему следует использовать сложный пароль, который трудно угадать. Для разных аккаунтов следует использовать разные пароли, и никогда никому их не сообщать. Все эти правила остаются в силе, только пароли сами по себе не являются эффективными в наши дни. С помощью современных технологий кибер мошенники легко могут подобрать пароль. Вот почему нам нужен простой способ усиления защиты. И такой способ существует, это двухступенчатая верификация.

Двухступенчатая верификация

Двухступенчатая верификация (некоторые называют её двухфакторная аутентификация или 2FA) – это более надежный способ защиты, чем пароль. Она подразумевает 2 метода подтверждения личности. Самый простой пример – банкомат. Для получения денег вам нужно 2 вещи: ваша банковская карта (то, что у вас есть) и PIN-

Двухступенчатая верификация

код (то, что вы знаете). Даже если вы потеряете карту, ваши деньги будут в безопасности. Тот, кто найдёт вашу карту, не сможет снять с неё деньги (если только вы не написали на ней PIN-код, это очень неудачный способ его хранения). PIN-код тоже бесполезен без карты. Злоумышленник должен получить эти две вещи, чтобы добраться до счета. Это и делает двухфакторную верификацию более сильным способом защиты.

использование двухступенчатой верификации обеспечивает более надёжную защиту ваших данных.

Использование двухфакторной верификации

Двухступенчатая верификация настраивается для каждого аккаунта. К счастью, большинство онлайн сервисов предоставляют такую услугу. Компания Google одна из первых предоставила такую возможность. Аккаунты Google бесплатны и миллионы людей ими пользуются, что делает их привлекательными для злоумышленников. Компания Google одной из первых стала использовать для защиты двухступенчатую верификацию для своих онлайн сервисов. Если вы понимаете, как работает двухфакторная верификация аккаунтов Google, то поймете и принцип её работы на других сайтах, например, Twitter, Facebook, Apple, Instagram.

Во-первых, вам нужно подключить услугу двухфакторной верификации для аккаунта Google и ввести номер мобильного телефона. Когда вы это сделаете, двухфакторная верификация будет работать следующим образом. Вы будете входить в аккаунт как и прежде, с помощью логина и пароля. Это первая ступень защиты, то, что вы знаете. Google отправит вам смс сообщение с уникальным кодом из 6 цифр. Эти цифры - дополнительный пароль, их тоже следует ввести на сайте. Это и есть вторая ступень защиты. Для входа в аккаунт вам требуются две вещи: пароль и мобильный телефон для получения уникального кода. Даже если хакеры взломают ваш пароль, они не смогут войти в Google аккаунт без телефона. Для обеспечения надёжной защиты Google каждый раз высылает новый код при входе в аккаунт.

Google и другие сайты предлагают следующий вариант двухступенчатой верификации. Вместо получения смс, вы можете загрузить специальное приложение для смартфона, которое будет генерировать уникальный код для каждого входа в аккаунт. Данный способ получения уникального кода не требует постоянного нахождения в зоне

Двухступенчатая верификация

покрытия мобильной сети, ваш телефон будет их генерировать. Это тоже обеспечивает дополнительную защиту, раз смс сообщение не отправляется, его нельзя перехватить.

Помните, двухфакторная верификация не устанавливается по умолчанию, её нужно настроить. С одной стороны двухфакторная верификация требует больше времени и усилий, но с другой, обеспечивает более надёжную защиту и мы настоятельно рекомендуем ей пользоваться, особенно для защиты таких важных сервисов, как электронная почта, банковские аккаунты и сервисы хранения данных. Двухфакторная верификация обеспечивает более надёжную защиту, чем пароль.

Общественные ресурсы

Не пользуйтесь общественными компьютерами, например, в лобби отелей, библиотеках или интернет-кафе. Вы же не знаете, кто пользовался этим компьютером до вас, компьютеры могут быть заражены вирусами случайно или специально. По возможности, используйте только свое устройство для соединения с Интернетом.
Если возникнет необходимость воспользоваться публичным компьютером, то постарайтесь не пользоваться сервисами, требующими вводить логин и пароль.

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.

Ресурсы

Паролевые фразы:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_ru.pdf
Сайты, поддерживающие двухфакторную верификацию:	https://twofactorauth.org
Stop|Think|Connect:	http://stopthinkconnect.org/2stepsahead
2-факторная верификация Google:	http://www.google.com/landing/2step/
Ежедневные советы Института SANS по информационной безопасности:	http://www.sans.org/tip_of_the_day.php

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