SANS SECURITY AWARENESS

OUCH! | Декабрь 2017

Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Фальшивые интернет магазины
- Безопасность компьютера/мобильного устройства
- Безопасность кредитных карт

Надёжная защита вашего аккаунта

Обзор

Об авторе
Тиффани Шоник – директор отдела инициативных разработок Национального Альянса Кибер Безопасности (@staysafeonline). В 2016 госпожа Шоник сотрудничала с Белым Домом, правительством и промышленным сектором над созданием и продвижением кампании «Надёжная защита вашего аккаунта» (Lock Down Your Login) в рамках проекта «Остановись. Подумай. Подключись» (STOP. THINK. CONNECT.тм) направленной на продвижение двухфакторной аутентификации.

Процесс аутентификации, или подтверждения вашей личности - это основной способ защиты вашей информации, такой как электронная почта, аккаунтов социальных сетей или банковского счета. Знаете ли вы, что существуют три основных способа подтвердить вашу личность: то, что вы знаете – пароль; то, что у вас есть – например, водительское удостоверение; и то, что является частью вас – например, отпечатки пальцев. Каждый из этих способов имеет свои достоинства и недостатки. Самый популярный метод – использование пароля; то, что вы знаете. Но использование для защиты только пароля становится всё менее и менее надёжным способом защиты. В этом выпуске мы поговорим о том, как защитить себя и свой логин чем-то более надёжным, чем просто пароль. Это называется «двухфакторная аутентификация».

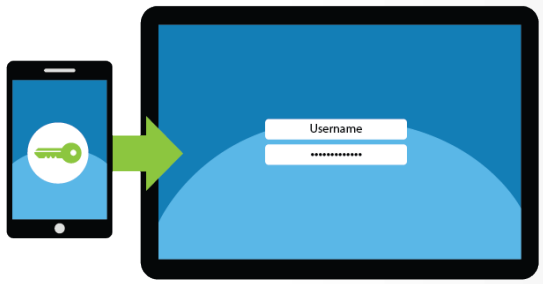
Пароль – ненадёжная защита

Защита паролем подразумевает знание вами чего-то. Но если кто-то сможет угадать или взломать ваш пароль, то они смогут выдавать себя за вас и легко получит доступ ко всем вашим данным. Взлом паролей - самый распространённый способ получения доступа к аккаунтам. Вот почему следует использовать сложные парольные фразы, которые сложно взломать, разные пароли для каждого аккаунта, и никогда не сообщать свой пароль другим. Но даже при соблюдении всех этих рекомендаций, пароль все равно не может обеспечить надёжной защиты. Но есть выход: применение двухфакторной аутентификации.

Надёжная защита вашего аккаунта

Что такое двухфакторная аутентификация

Двухфакторная аутентификация (её также называют двухступенчатая верификация, многофакторная аутентификация или 2FA) защищает намного лучше, чем просто пароль. Этот метод заключается в использовании двух различных способов подтверждения личности. Хорошим примером служат банковские карты. Когда вы снимаете наличные деньги в банкомате, вы используете не что иное, как двухступенчатую верификацию. Для получения доступа к деньгам вам нужны две вещи: банковская карта (то, что у вас есть) и пароль доступа к ней PIN (то, что вы знаете). Если вы потеряете карту или её украдут, то все равно нельзя будет совершить операцию с деньгами без пароля. Ворам нужна не только карта, но и пароль для снятия денег. Двухфакторная аутентификация работает по такой же схеме.



Используйте двухступенчатую верификацию при любой возможности – это ключевой фактор вашей безопасности в интернете.

Как это работает

Двухфакторная аутентификация широко распространена на большинстве сайтов: банковских, почтовых, социальных сетей и многих других. Эти же сайты предлагают простую пошаговую инструкцию по подключению данной услуги (больше информации об этом в секции Ресурсы, в конце этой статьи). После подключения она будет работать следующим образом. Первое, вам нужно войти в аккаунт под своим логином и паролем, как обычно. Это первый фактор из двух – то, что вы знаете. Затем вы получите на смартфон уникальный код доступа. Этот код доступа нужно ввести в окошко логина. Это второй фактор из двух – вам нужен смартфон для получения уникального кода. Теперь ваш аккаунт надёжно защищён. Даже если злоумышленники взломают пароль, они всё равно не получат доступ к вашему аккаунту без вашего телефона.

Надёжная защита вашего аккаунта

Вы можете получать уникальный код с помощью смс или установить на телефон специальное приложение. Это приложение будет генерировать уникальный код каждый раз при входе в аккаунт. Преимущество приложения заключается в его безопасности, код генерируется прямо на телефоне, а не отправляется смс. Ещё одно преимущество приложения в том, что вам не нужно подключаться к телефонному сервису для получения кода. Приложение постоянно генерирует новые коды для входа в аккаунт.

Несмотря на то, что двухступенчатая аутентификация требует больше усилий, обязательно стоит её использовать для защиты личных данных. Не стоит ждать, пока ваш аккаунт взломают, защитите ваш логин, используя двухступенчатую аутентификацию для входа в банковские аккаунты, социальную сеть и наслаждайтесь чувством безопасности.

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 securingthehuman.sans.org/ouch/archives.

Ресурсы

Парольные фразы:	https://securingthehuman.sans.org/ouch/2017#april2017
Сайты, поддерживающие двухступенчатую верификацию:	https://twofactorauth.org
Остановись/Подумай/Подключись:	https://www.lockdownyourlogin.org
Двухступенчатая аутентификация Google:	https://www.google.com/intl/ru/landing/2step/
Двухфакторная аутентификация Яндекс:	https://yandex.ru/support/passport/authorization/twofa.html
Сведения о двухшаговой проверке:	

https://support.microsoft.com/ru-ru/help/12408/microsoft-account-about-two-step-verification

Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли
Русский перевод: Александр Котков, Ирина Коткова