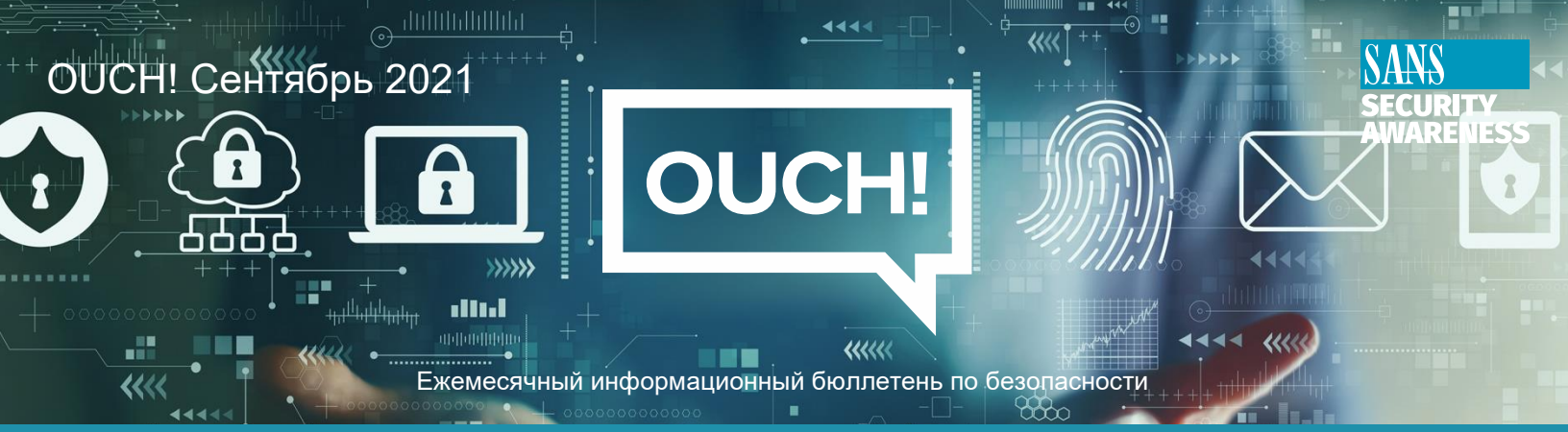
OUCH! Сентябрь 2021



Один простой шаг к защите ваших учетных записей

Кажется, что у киберпреступников есть волшебная палочка для проникновения в вашу электронную почту или банковские счета, и вы ничего не можете сделать, чтобы их остановить? Разве не было бы замечательно, если бы вы могли сделать один-единственный шаг, который помог бы защитить вас от киберпреступников и позволил вам безопасно использовать технологии? Хотя ни один шаг не остановит всех киберпреступников, одним из наиболее важных шагов, которые вы можете предпринять, является включение так называемой двухфакторной аутентификации (иногда называемой 2FA, двухэтапной проверкой или многофакторной аутентификацией) для ваших самых важных учетных записей.

Проблема с паролями

Когда дело доходит до защиты ваших учетных записей, вы, скорее всего, уже используете какой-либо тип пароля. Есть несколько способов аутентифицироваться в учетной записи: что-то что у вас есть, что-то вы знаете, кем вы являетесь, где вы находитесь. Когда вы используете более одного метода аутентификации, вы добавляете дополнительный уровень защиты от киберпреступников - даже если они взломают один метод, им все равно придется обходить дополнительные факторы для доступа к вашей учетной записи. Пароли подтверждают вашу личность на основании того, что вам известно. Опасность паролей в том, что они представляют собой единую точку отказа. Если киберпреступник сможет угадать или скомпрометировать ваш пароль, он сможет получить доступ к наиболее важным учетным записям. Кроме того, киберпреступники разрабатывают все более быстрые и эффективные методы угадывания, взлома или обхода паролей. К счастью, вы можете дать отпор с помощью двухфакторной аутентификации.

Двухфакторная аутентификация

Добавление двухфакторной аутентификации - гораздо более безопасное решение, чем полагаться только на пароли. Она работает, требуя не одного, а двух разных методов аутентификации. Таким образом, если ваш пароль будет скомпрометирован, ваша учетная запись будет по-прежнему защищена. Одним из примеров является ваша банковская карта; когда вы снимаете деньги, вы фактически используете форму двухфакторной аутентификации. Чтобы получить доступ к своим деньгам, вам понадобятся две вещи: ваша банковская карта (что-то, что у вас есть) и ваш PIN-код (что-то, что вы знаете). Если вы потеряете свою банковскую карту, любой, кто найдет вашу карту, не сможет снять ваши деньги, так как они не знают вашего PIN-кода. То же самое верно, если у них есть только ваш PIN-код, а не карта. Злоумышленник должен иметь и то, и другое, чтобы взломать вашу учетную запись. Концепция аналогична двухфакторной аутентификации; у вас есть два уровня безопасности.

`` © SANS Institute 2021

Использование двухфакторной аутентификации онлайн

Двухфакторная аутентификация - это то, что вы настраиваете индивидуально для каждой из ваших учетных записей.

На самом деле это довольно просто: обычно вам не нужно ничего делать, кроме как синхронизировать мобильный телефон с вашей учетной записью. Таким образом, когда вам нужно войти в свою учетную запись, вы не только войдете в нее с именем пользователя и паролем учетной записи, но также будете использовать уникальный одноразовый код, который получите со своего телефона. Идея состоит в том, что для входа в систему требуется комбинация вашего пароля и уникального кода. Обычно этот уникальный код отправляется в текстовом сообщении на ваше мобильное устройство или по электронной почте. На вашем телефоне также может быть мобильное приложение (например, Google или Microsoft Authenticator), которое сгенерирует для вас уникальный код. Когда это возможно, мобильные приложения считаются наиболее безопасным способом получения вашего уникального кода.

Что делает это таким простым, так это то, что вам обычно нужно сделать это только один раз с любого компьютера или устройства, которое вы используете для входа в систему. Как только веб-сайт или ваша учетная запись распознает ваше устройство, в дальнейшем вам часто нужен только пароль для входа в систему. Каждый раз, когда вы пытаетесь (или кто-то пытается) войти в систему с вашей учетной записью, но с другого компьютера или устройства, им снова придется использовать двухфакторную аутентификацию. Это означает, что если киберпреступник получит ваш пароль, он все равно не сможет получить доступ к вашей учетной записи, так как не сможет получить доступ к уникальному коду.

Помните, что двухфакторная аутентификация обычно не включена по умолчанию, поэтому вам придется включить ее самостоятельно для каждой из ваших наиболее важных учетных записей, таких как банковская, инвестиционная, пенсионная или личная электронная почта. Хотя сначала может показаться, что это требует больше работы, после настройки им очень легко пользоваться.

Приглашенный редактор

Лисандра Капелла имеет более чем 15-летний опыт работы в сфере информационной безопасности и технологий. Она является инструктором Института SANS по обучению для SANS AUD507, специализируясь на измерении и управлении рисками. В свободное от преподавания время Лисандра поддерживает группы высшего руководства в разработке стратегии, обеспечении безопасности и управлении ИТ. https://www.linkedin.com/in/lysandracapella/.

Ресурсы

Создание простых паролей: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Менеджеры паролей: https://www.sans.org/newsletters/ouch/password-managers/

OUCH! публикуется SANS Security Awareness и распространяется под лицензией Creative Commons BY-NC-ND 4.0. Вы можете свободно делиться или распространять этот информационный бюллетень, если вы не продаете или не изменяете его. Редакционная коллегия: Уолтер Скривенс, Фил Хоффман, Алан Ваггонер, Лесли Ридаут, Принцесса Янг.