Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Что такое шифрование**
- **Что следует шифровать**
- **Как правильно использовать шифрование**

Шифрование

Что такое шифрование?

Вы могли слышать термин «шифрование» и советы по его использованию для защиты информации. Однако шифрование не так просто понять и у него есть свои ограничения. В этом выпуске мы объясним суть шифрования, как оно может быть использовано для вашей защиты и как правильно его использовать.

Об авторе

Франческа Боско (**@francibosco**) – исследователь и руководитель проектов по расследованию киберпреступлений, кибербезопасности и злоупотреблениям в этой сфере. Она работает в Межрегиональном институте изучения преступности при Организации Объединенных Наций. Франческа - соучредитель Центра Технологии и Правопорядка.

На наших электронных устройствах содержится огромное количество личной информации: документы, фотографии или электронные письма. Если потеряете устройство или его украдут, вся информация будет доступна его новому обладателю. Помимо этого, вы можете управлять конфиденциальными данными онлайн, например, при совершении онлайн покупок или банковских операций. Если кто-то отследил эти операции, то может украсть все данные, включая счет в банке и номера кредитных карт. Шифрование может защитить в подобных ситуациях: оно предотвратит возможность чтения и изменения ваших данных посторонними.

Шифрование применяется уже тысячи лет. В наши дни способы шифрования более современные, но суть остается прежней – доставить секретное сообщение из одного места в другое, обеспечивая доступ к нему только авторизованным людям. Если информация не зашифрована, это называется простым текстом. То есть любой человек может прочитать сообщение или получить данные. Шифрование преобразует текст в нечитаемый формат, так называемый зашифрованный текст. Современное шифрование состоит из комплекса математических операций и уникального ключа, которые преобразовывают данные в зашифрованный текст. Ключ позволяет заблокировать и разблокировать информацию. В большинстве случаев ключ – это просто пароль или код доступа.

Что следует шифровать

Информацию, которую можно шифровать, делят на два вида: данные в состоянии покоя (например, информация в мобильном устройстве) и данные в движении (электронная переписка или сообщения от друзей).

© SANS Institute 2016

Шифрование

Шифрование данных в состоянии покоя поможет их защитить в случае утери или кражи устройства. Современные мобильные устройства очень мощные и содержат огромное количество данных, но их очень легко потерять. Другие типы устройств тоже могут содержать конфиденциальную информацию, например USB-флешки или съёмные жёсткие диски. Полное шифрование диска (FDA – Full Disk Encryption) – самый популярный метод шифрования всех данных носителя. Он позволяет автоматически шифровать абсолютно всю информацию. Большинство современных компьютеров имеют функцию FDE, но её нужно включить или активировать вручную. На компьютерах Mac полное шифрование называется FileVault. На компьютерах Windows, в зависимости от версии операционной системы, вы можете использовать Bitlocker или Device Encryption. Большинство мобильных устройств тоже имеют функцию полного шифрования (FDE). Система iOS на устройствах iPhone и iPad автоматически включает FDE при установке пароля доступа. На устройствах с Android такое возможно начиная с версии 6.0 (Marshmallow): Google требует использования FDE по умолчанию, при условии соответствия спецификаций аппаратуры минимальным требованиям.

шифрование помогает защитить ваши данные, но эффективность шифрования зависит от надёжности ключа доступа к нему.

Информация подвержена опасности и во время передачи. Если данные не зашифрованы, то их можно отследить, изменить или перехватить онлайн. Вот почему нужно шифровать конфиденциальные данные и переписку. Самый распространённый вид онлайн шифрования HTTPS. Он позволяет шифровать весь поток информации от вашего браузера к сайтам. Чтобы определить, использует ли сайт шифрование, поищите символы https:// поле адреса, иконку с замочком в окне браузера; полоска ввода адреса браузера становится зелёной. Другим примером может служить отправка или получение электронной почты. Большинство провайдеров электронной почты позволяют подключить опцию шифрования. Третьим примером зашифрованной передачи данных является обмен сообщениями между двумя пользователями с помощью iMessage, Wickr, Signal, WhatsApp или Telegram. Эти приложения используют шифрование на всех стадиях передачи данных от одного устройства к другому. Это значит, что переписка доступна только вам и человеку, с которым вы переписываетесь.

© SANS Institute 2016

Шифрование

Как правильно использовать шифрование

Вот признаки того, что вы правильно используете шифрование и надёжно защищены:

- Шифрование дает надёжную защиту только при использовании надёжного ключа. Если кто-то подберёт ключ или получит доступ к нему, он получит доступ и к вашей информации. Убедитесь, что используете сильный код доступа или уникальный пароль. Чем сложней и длинней пароль, тем трудней злоумышленникам его подобрать или взломать. И не забудьте этот пароль, иначе тоже не сможете расшифровать свои данные. Для этого мы рекомендуем использовать менеджер паролей.
- Шифрование защищает до тех пор, пока ваше устройство в безопасности. Если ваше устройство взломали или заразили вирусами, то злоумышленники обойдут и шифрование. Вот почему необходимо соблюдать меры безопасности, включая использование антивирусных программ, сильных паролей и регулярных обновлений.
- Большинство мобильных и компьютерных приложений предоставляют опцию шифрования данных и общения. Если приложение не предоставляет эту опцию, следует поискать другое.

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

Encryption Explained:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Паролевые фразы:	https://securingthehuman.sans.org/ouch/2015#april2015
Менеджеры паролей:	https://securingthehuman.sans.org/ouch/2015#october2015
Что такое вредоносные программы:	https://securingthehuman.sans.org/ouch/2016#march2016
Безопасность планшета:	https://securingthehuman.sans.org/ouch/2016#january2016

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

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

© SANS Institute 2016