Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Что такое шифрование?**
- **Шифрование данных при хранении**
- **Шифрование данных при передаче**

Шифрование

Что такое шифрование?

Вы часто можете слышать термин «шифрование» и советы по использованию шифрования для защиты вас и ваших данных. Однако, концепция шифрования может казаться сложной для понимания. Кроме того, шифрование не может защитить вас от всего; у него есть свои ограничения. В этом выпуске мы доходчиво объясним, что такое шифрование, почему вы должны его использовать и как правильно его применять.

Об авторе

Кристофер Краули (**@CCrowMontance**; **+ChrisCrowley**) – консультант из Вашингтона (округ Колумбия). Он является ведущим инструктором курса Mobile Device Security and Ethical Hacking (SEC575) и автором курса Incident Response Team Management (MGT535) в Институте SANS.

Ваши компьютеры и гаджеты содержат огромное количество конфиденциальной информации, такой как финансовые документы, фотографии, сообщения электронной почты или медицинские данные. В случае потери или кражи одного из ваших компьютеров или гаджетов, вся ваша конфиденциальная информация может быть доступна новому «владельцу» вашего устройства. Кроме того, вы можете совершать конфиденциальные операции через интернет, например, банковские транзакции или покупки через интернет. Если кибер-преступники наблюдают за вашими действиями в интернете, они могут украсть всю вашу информацию, такую как ваши банковские счета или номера кредитных карт. Шифрование защищает вас в этих ситуациях, предотвращая доступ или изменение вашей информации злоумышленниками.

Когда информация не зашифрована, она называется «открытый текст». Это означает, что каждый может легко получить к ней доступ или прочитать её. Шифрование превращает эту информацию в нечитаемый формат, который называется «зашифрованный текст». Для превращения вашей информации в зашифрованный текст, шифрование использует сложные математические операции и уникальный ключ. Ключ – это то, что закрывает и открывает вашу информацию, подобно тому, как ключ закрывает и открывает дверь. Один из типичных примеров ключа – пароль. Только люди, которые знают ваш пароль, могут расшифровать и использовать вашу информацию. Чтобы защищать вашу зашифрованную информацию, вы должны защищать ваш ключ. Существует два основных вида шифрования: вы можете шифровать данные в состоянии покоя (например, информацию на вашем компьютере) и передаваемые данные (например, при передаче данных через интернет).

Шифрование

Шифрование данных при хранении

Шифрование – мощный способ защиты вашей информации, но он силен настолько, насколько силен ваш ключ

Основная цель шифрования данных в состоянии покоя – защита информации в случае кражи или утери вашего компьютера или мобильного устройства. 15 лет назад это было не актуально, так как большинство компьютеров были большими, громоздкими стационарными устройствами, которые было тяжело перемещать. Современные ноутбуки весят всего пару килограмм, а мобильные устройства почти невесомы. Эти устройства обладают значительной мощностью и содержат огромное количество информации, но их легко потерять. Кроме того, конфиденциальная информация может содержаться на мобильных носителях, таких как USB флэшки или CD диски. Популярный подход к шифрованию данных на этих устройствах – использование Полного Шифрования Диска (Full Disk Encryption, FDE). Это означает, что всё на диске шифруется автоматически; вам не нужно решать что шифровать, а что нет. Большинство современных операционных систем имеют встроенный функционал Полного Шифрования Диска, вы просто должны включить его. Например, Mac OS X имеет функционал FileVault; современные версии Windows предоставляют функционал BitLocker. Если ваш компьютер поддерживает функцию Полного Шифрования Диска, мы рекомендуем включить её. Многие мобильные телефоны поддерживают функцию Полного Шифрования Диска для своего внутреннего устройства хранения информации. Например, iOS – операционная система используемая в устройствах iPhone и iPad, автоматически включает Полное Шифрование Диска при установке пароля устройства. Если вам нужно узнать, поддерживает ли Полное Шифрование Диска ваш компьютер или мобильное устройство на работе, обратитесь в Службу Поддержки или своему руководителю. Чтобы найти эту информацию для ваших личных компьютеров, свяжитесь с производителем или изучите онлайн документацию устройства.

Шифрование данных при передаче

Когда информация передается, она уязвима. Если данные не зашифрованы, они могут быть подсмотрены и перехвачены через интернет. Вот почему вы должны быть уверены, что передача любой конфиденциальной информации (онлайн банкинг, пересылка электронной почты и доступ к социальным сетям) зашифрована. Наиболее распространенный вид шифрования данных, передаваемых через интернет – HTTPS. Его применение означает, что вся информация, передаваемая между вашим браузером и интернет сайтом, зашифрована. Поищите префикс https:// в адресе (URL) интернет сайта, значок «замок» на вашем браузере или зеленую полоску URL адреса в браузере. Это признаки того, что коммуникация зашифрована. В зависимости от вашего браузера и интернет сайта, вы можете увидеть все три признака одновременно.

Шифрование

Когда вы подключаетесь к общедоступной сети Wi-Fi, используйте шифрование, если оно доступно.
При отправлении или получении сообщений электронной почты, конфигурируйте ваш почтовый клиент так, чтобы он использовал зашифрованный канал передачи. Большинство почтовых клиентов поддерживают шифрование. Ваш интернет провайдер может помочь вам сконфигурировать шифрование на вашем почтовом клиенте.

Правильное использование шифрования

Независимо от типа шифрования и способа его использования, существует несколько общих правил использования шифрования:

- Ваше шифрование настолько надёжно, насколько надёжен ваш ключ. Если кто-то украдёт или угадает ваш ключ, они получат доступ к вашей информации. Вы должны защищать свой ключ.
- Если вы используете пароль или ПИН в качестве вашего ключа, сделайте его длинным и сложным; не теряйте и не забывайте его. Если вы забудете его, вы потеряете доступ к своим данным.
- Ваше шифрование настолько надёжно, насколько хорошо защищен ваш компьютер. Если ваш компьютер был заражен или атакован, злоумышленники могут обойти ваше шифрование. Чтобы предотвратить это, обеспечьте безопасность вашего компьютера или мобильного устройства.
- Если вам доступны разные варианты шифрования, всегда выбирайте самый сильный метод.

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

Mac OS X Filevault: http://support.apple.com/kb/ht4790

iOS encryption: http://support.apple.com/kb/ht4175

Android encryption: http://www.androidauthority.com/how-to-encrypt-android-device-326700/

Защита файлов с помощью шифрования дисков BitLocker:
http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7

Семь простых шагов для защиты компьютера: http://www.securingthehuman.org/ouch/2012#december2012

Менеджер паролей: http://www.securingthehuman.org/ouch/2013#october2013

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

