Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

Помощь близким – залог вашей безопасности

Обзор

Многие из нас хорошо разбираются в современных технологиях и даже знают и соблюдают правила безопасности. Но не все члены семьи или друзья владеют технологиями на таком же уровне. Технологии могут их смущать и даже пугать. Это и делает их лёгкой добычей для киберпреступников. Компьютерная безопасность не должна быть чем-то страшным; если понять её основы, то всё не так уж сложно. Вам просто нужно объяснить азы компьютерной безопасности своим друзьям и родственникам.

Об авторе

Рэнди Марчани (Twitter: **@randymarchany**) – CISO университета Virginia Tech и сертифицированный инструктор Института SANS.

Пять простых шагов

Вот пять простых шагов, которые помогут вашим близким преодолеть страх и использовать современные технологии безопасно. Для получения более подробной информации по каждому из этих шагов, почитайте материалы, указанные в разделе Ресурсы, в конце статьи:

1. **Социальная инженерия**: Техника социальной инженерии наиболее часто используется злоумышленниками для получения обманным путём паролей, конфиденциальной информации или заражения компьютера вирусами. В этом нет ничего нового, аферисты и мошенники существуют тысячелетиями. Но есть одно существенное отличие: плохие парни применяют те же трюки в интернете. Объясните близким основные приёмы атак социальной инженерии, такие, как создание ситуации срочности, предложение неправдоподобно хороших вещей и условий, или когда мошенники притворяются кем-то из ваших друзей и пишут от их имени странные сообщения. Поделитесь примерами таких атак, например, фишинговые атаки или известная афера «Звонок из службы поддержки Microsoft». Проще говоря, члены вашей семьи должны уяснить, что не при каких обстоятельствах они не должны давать никому свои пароли и разрешать доступ к своему компьютеру.
2. **Пароли**: Использование сложного пароли – основной способ защиты устройства и онлайн аккаунта. Расскажите близким о способах создания сложных и надёжных паролей. Мы рекомендуем использовать

© SANS Institute 2017

Помощь близким – залог вашей безопасности

парольные фразы – это пароль, состоящий из нескольких слов; его легко печатать и запомнить. Можно помочь выбрать и установить менеджер паролей. Важно защитить каждый аккаунт и устройство отдельным паролем. Если использование менеджера паролей покажется слишком сложным, то можно просто записать пароли на листочке и спрятать в безопасное место. Для важных аккаунтов следует использовать двухступенчатую верификацию (также её называют двухступенчатой аутентификацией). Двухступенчатая верификация – один из самых надёжных способов защиты аккаунта.

Помогите другим безопасно пользоваться технологиями с помощью пяти простых шагов, описанных в этой статье.

3. **Обновления**: Использование самых последних версий систем и программ и своевременное их обновление – один из ключевых шагов безопасности. Это относится не только к компьютеру или мобильному устройству, но и актуально для любых устройств, соединённых с интернетом, например, игровых приставок, термометров или даже ламп и музыкальных колонок. Самый простой способ – настроить автоматическое обновление, если это возможно.
4. **Антивирус**: Иногда люди по ошибке открывают или загружают файлы, которые могут заразить систему. Антивирус создан для того, чтобы защитить от таких ошибок. Антивирус не защищает от абсолютно всех вирусов, но большинство атак может остановить. Поэтому следует установить антивирусы на всех домашних компьютерах и мобильных устройствах и регулярно их обновлять. Большинство современных антивирусов включают в себя дополнительные технологии безопасности, например, защиту браузера и файрвол.
5. **Резервное копирование**: Если всё вышеперечисленное не поможет, то резервная копия – единственная возможность восстановить данные в случае ошибочного удаления файлов или кибер атак, например, программ-вымогателей (ransomware). Помогите друзьям и членам семьи настроить автоматическое создание резервной копии. Часто простейший способ резервного копирования – использование облачного сервиса, который ежечасно или по мере изменения файла сохраняет его копию. Такое решение поможет не только хранить данные, но и восстановить их в случае необходимости.

Безопасность детей в гостях

Скорее всего, вы разбираетесь в технологиях и можете защитить не только себя, но и своих детей. Но что делать,

© SANS Institute 2017

Помощь близким – залог вашей безопасности

когда дети посещают родственников, которые не сильны в современных технологиях, например, дедушек и бабушек? Следующие шаги помогут защитить детей, когда они в гостях у родственников.

- **Правила**. Прежде всего убедитесь, что правила безопасности знают не только дети, но и окружающие. Например, как долго дети могут находится в сети, с кем общаться, во что играть, а во что нет. Поверьте, не стоит ожидать, что дети сами расскажут об этих правилах другим членам семьи. Хорошая идея - напечатать эти правила и ознакомить с ними всех, кого навещает ребёнок.
- **Контроль**. Если ребёнок разбирается в технологиях намного лучше, чем те, кто за ним присматривает, то скорее всего, ребёнок этим воспользуется. Например, ребёнок может получить права администратора на компьютере дедушки и установить игру, в которую вы ему не разрешаете играть. Убедитесь, что родственники понимают, что не следует разрешать детям доступ больше дозволенного.

Подпишите своих друзей и родственников на такие ресурсы, как OUCH!, чтобы они могли сами изучать правила безопасности. Эти статьи бесплатные и публикуются более чем на 20 языках. Заходите на наш сайт https://securingthehuman.sans.org/ouch.

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

Центр безопасного Интернета в России:	http://www.saferunet.ru
Социальная инженерия:	https://securingthehuman.sans.org/ouch/2017#january2017
Парольные фразы:	https://securingthehuman.sans.org/ouch/2017#april2017
Менеджер паролей:	https://securingthehuman.sans.org/ouch/2017#september2017
Двухступенчатая верификация:	https://securingthehuman.sans.org/ouch/2015#september2015
Резервное копирование и восстановление:	https://securingthehuman.sans.org/ouch/2017#august2017
Безопасность детей в сети:	https://securingthehuman.sans.org/ouch/2017#may2017

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