Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

Основы безопасности для старшего поколения

Обзор

Большинство из нас легко освоили технологии, включая их безопасное использование. Но не всем членам семьи это дается легко, особенно, если они не росли с компьютерами и Интернетом. Поговорим о некоторых шагах, которые помогут преодолеть разрыв между поколениями. Дома вы обеспечили детям безопасность использования компьютера, но не всегда эти меры предприняты в домах родственников. Поэтому поговорим и о том, как обеспечить онлайн безопасность в гостях.

Об авторе

Брайан Хонан (Twitter **@brianhonan**) – независимый консультант по компьютерной безопасности из Дублина (Ирландия), основатель и глава первой в Ирландии группы реагирования на компьютерные инциденты (CERT), Специальный Советник Центра Киберпреступлений Европола (EC3) и преподаватель информационной безопасности в Университетском колледже Дублина. Брайан написал несколько книг; он регулярно пишет статьи для профессиональных изданий.

Основы

Вот несколько простых шагов, которые обеспечат безопасность для каждого в электронной жизни. Эти правила касаются всех членов семьи. Но если вы видите, что кому-то не понятны эти правила, то следует их подробно объяснить или реализовать их самим.

- **Социальная инженерия**: объясните это понятие простыми терминами, доступными каждому. Обман и мошенники существуют тысячи лет и это не новость. Единственное отличие в том, что теперь мошенники используют свои схемы в Интернете. Приведите примеры самых распространённых атак, например, фишинговых писем или пресловутых звонков из Службы Поддержки Microsoft. В любом случае члены семьи должны понимать, что нельзя никому давать свои пароли или разрешать удалённый доступ к компьютеру. Наконец, дайте понять, что не следует стесняться вопросов о странных письмах электронной почты или звонках; при малейших сомнениях стоит обратиться к вам за помощью.
- **Домашняя Wi-Fi сеть**: уделите время проверке безопасности домашней сети Wi-Fi. Как минимум, следует установить сильный и надежный пароль администратора, вместо установленного по умолчанию, и убедится, что используется современное шифрование. Также вы можете сконфигурировать настройки Wi-Fi так, чтобы использовать безопасный сервис DNS, такой как www.opendns.org. Этот

Основы безопасности для старшего поколения

сервис поможет предотвратить посещение не только зараженных сайтов, но и сайтов, которые не стоит посещать детям.

- **Обновления**: помните, что регулярные обновления и использование последних версий – это основа безопасности. Убедитесь, что все домашние устройства, включая мобильные, регулярно обновляются. Самый простой способ это сделать – настроить автоматическое обновление, по возможности.
- **Антивирус**: часто люди совершают ошибки, переходя по ненужным ссылкам или устанавливая программы, которые не нужны. Антивирус не может защитить от всех вирусов, но спасает от большинства атак. Поэтому убедитесь в наличии последней версии антивируса на всех домашних компьютерах и в том, что антивирус включён.

старшее поколение следует научить безопасно использовать современные технологии, и сделать их дом безопасным для детей.

- **Пароли**: с помощью надежного пароля можно защитить не только устройство, но и онлайн аккаунт. Объясните членам семьи, как правильно создавать сильные и надёжные пароли. Паролевые фразы – лучший вариант, их легко придумать и легко запомнить. Как вариант, можно установить менеджер паролей, и научить им пользоваться. Если перечисленные варианты не подходят, то пароль можно записать на бумаге и хранить в надёжном месте. Для очень важных аккаунтов следует применять двухступенчатую аутентификацию.
- **Резервное копирование**: в случае неудач резервное копирование сохранит вам много времени. Убедитесь, что у членов семьи установлена надежная система резервного копирования файлов.

Вы можете ежемесячно или ежеквартально проверять работу системы. В особых случаях стоит настроить удалённый доступ к устройству, только не забудьте защитить его надёжным паролем и шифрованием.

Визиты детей

Часто правила, которые вы установили дома, не соблюдаются в гостях у родственников, бабушек и дедушек. Это касается и правил безопасности в Сети. Стоит предпринять следующие шаги для защиты детей:

Основы безопасности для старшего поколения

- **Правила**. Убедитесь, что родственники знают о правилах, которые вы установили дома. Например, как долго дети могут играть в сети или когда им можно пользоваться мобильными устройствами. Поверьте, не стоит ожидать, что дети сами расскажут о них другим членам семьи. Один из вариантов напечатать «Свод правил» и раздать его родственникам, у которых дети бывают.
- **Контроль**. Если дети разбираются в технологиях лучше, чем родственники, они могут этим воспользоваться. Например, дети могут попросить или получить права администратора к компьютеру ваших родителей и делать все, что им вздумается, включая установку игр, которые вы запретили. Убедитесь, что родственники понимают, что не должны этого допускать.

Общественные ресурсы

Не пользуйтесь общественными компьютерами, например, в лобби отелей, библиотеках или интернет-кафе. Вы же не знаете, кто пользовался этим компьютером до вас, компьютеры могут быть заражены вирусами случайно или специально. По возможности, используйте только свое устройство для соединения с Интернетом. Если возникнет необходимость воспользоваться публичным компьютером, то постарайтесь не пользоваться сервисами, требующими вводить логин и пароль.

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

Социальная инженерия:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_ru.pdf
Защита домашней сети:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201401_ru.pdf
Паролевые фразы:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_ru.pdf
Что такое антивирус?:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201412_ru.pdf
Защита детей от онлайн опасностей:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201304_ru.pdf
Мошенничество «Телефонная Служба Поддержки»:	http://www.onguardonline.gov/articles/0346-tech-support-scams
Постер «Создание кибер безопасного дома»:	http://www.securingthehuman.org/resources/posters

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
Русский перевод: Александр Котков, Ирина Коткова

