Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

Пять шагов к безопасности

Обзор

Технологии играют все более важную роль в нашей жизни; они также становятся всё сложнее. Учитывая технологические изменения, соблюдать безопасность становится непросто. Складывается впечатление, что рекомендации о том, что делать и чего делать нельзя, постоянно меняются. Но следует помнить, что, несмотря на постоянно меняющиеся со временем детали, фундаментальные принципы безопасности остаются неизменными. Независимо от того, какую технологию и где вы используете, мы рекомендуем следующие пять ключевых шагов.

Об авторе

Ленни Зельцер обеспечивает информационную безопасность клиентов компании NCR Corp и читает курс по борьбе с вредоносными программами в Институте SANS. Ленни ведет записи в Twitter **@lennyzeltser** и ведет свой блог **blog.zeltser.com**.

Пять ключевых шагов

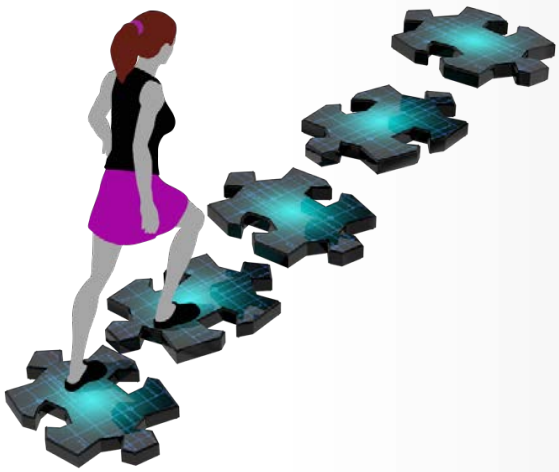
Мы коротко расскажем о каждом из пяти шагов. Дополнительную информацию по каждому из них можно найти в разделе Ресурсы.

1. **Вы сами**: Всегда помните, что технология сама по себе не сможет вас защитить. Злоумышленники знают, что лучший способ обойти любую техническую защиту - атаковать вас напрямую. Если они хотят получить ваш пароль или номер кредитной карты, они попытаются обмануть вас и заставить сообщить эту информацию. Например, кибер преступники, которые хотят получить доступ к вашему компьютеру, могут позвонить от имени Службы Поддержки Microsoft, сообщить, что ваш компьютер заражён, и попытаться получить доступ к нему. Или вам могут прислать по электронной почте письмо с информацией о том, что вашу посылку не могут доставить, так как адрес неверный и попросят перейти по ссылке для его подтверждения. На самом деле, вас пытаются заманить на вредоносный сайт и заразить ваш компьютер. В любом случае, вы сами – наилучшая защита. Будьте бдительны, здравый смысл поможет вам выявить и предупредить большинство атак.

2. **Обновления**: Убедитесь, что ваши компьютеры, мобильные устройства, приложения и все, что подключено к сети, регулярно обновляется. Кибер преступники постоянно ищут уязвимости в используемых

Пять шагов к безопасности

технологиях. Когда они их находят, то запускают специальные программы для взлома вашей сети, компьютеров или мобильных устройств. Компании-производители постоянно работают над обновлениями своих продуктов и технологий. Поэтому, когда уязвимость обнаружена, производитель выпускают обновления для устранения уязвимостей и предоставляют их пользователям. Регулярные обновления снижают риск взлома, и усложняют задачу кибер преступникам. По возможности, настройте автоматическое обновление. Это относится ко всем устройствам, подключенным к сети, в том числе телевизорам с интернет функциями, детским мониторам, домашним роутерам, игровым приставкам и даже, в скором будущем, автомобилям. Если операционная система компьютера или другая технология снята с поддержки и больше не обновляется, то мы рекомендуем установить новую, с поддержкой.



Пять ключевых шагов обеспечат безопасную работу с самыми новейшими технологиями.

3. **Пароли**: Следующим шагом является использование сильных, уникальных паролей для каждого устройства, онлайн аккаунта или приложения. Ключевые слова: сильный и уникальный. Под сильным подразумевается пароль, который сложно угадать или подобрать с помощью специальной программы. Не используйте слово в качестве пароля, лучше использовать парольную фразу, состоящую из нескольких слов и ряда символов и цифр для дополнительной защиты. Используйте различные пароли для каждого девайса или аккаунта. В случае взлома одного из них, остальные аккаунты или девайсы по-прежнему будут в безопасности. Вы не можете запомнить такой пароль? Не волнуйтесь, практически никто не может. В этом случае мы рекомендуем использовать менеджер паролей, который можно установить на компьютер или телефон. Он будет надёжно хранить ваши пароли в зашифрованном виде. И, наконец, если аккаунт поддерживает двухступенчатую верификацию, мы настоятельно рекомендуем ей воспользоваться, это один из самых надёжных способов защиты аккаунта.

4. **Шифрование**: Четвёртым шагом является использование шифрования. Шифрование предоставляет доступ к информации только вам или людям, которым вы доверяете. Данные можно шифровать при передаче или хранении. Шифрование данных при хранении обеспечивает защиту файлов на жестком диске

Пять шагов к безопасности

или USB-носителе. Большинство операционных систем позволяют автоматически шифровать все данные с помощью функции Full Disk Encryption. По возможности, используйте эту функцию. Под шифрованием данных при передаче подразумевается шифрование данных, передаваемых между вашим компьютером и другими системами, как, например, онлайн банкинг. Если в адресной строке посещаемого сайта вы видите «https:» и значок замка, значит обмен данными с этим сайтом защищен шифрованием.

5. **Резервные копии**: Иногда, несмотря на все меры предосторожности, ваше устройство могут взломать. В этом случае, самым безопасным способом избавления от вирусов является полное удаление системы и её переустановка. Злоумышленник даже может закрыть вам доступ к личным файлам, фотографиям и прочей информации на зараженном устройстве. Единственным способом получения этой информации будет восстановление из резервной копии. Убедитесь, что вы регулярно делаете резервные копии всех данных и можете их восстановить. Большинство операционных систем и мобильных устройств поддерживают функцию автоматического резервного копирования.

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

Фишинг: атаки по электронной почте:	http://www.securingthehuman.org/ouch/2013#february2013
Как защитить новый планшет:	http://www.securingthehuman.org/ouch/2013#december2013
Пароли:	http://www.securingthehuman.org/ouch/2013#may2013
Менеджер паролей:	http://www.securingthehuman.org/ouch/2013#october2013
Двухступенчатая верификация:	http://www.securingthehuman.org/ouch/2013#august2013
Шифрование:	http://www.securingthehuman.org/ouch/2014#august2014
Резервное копирование и восстановление:	http://www.securingthehuman.org/ouch/2013#september2013

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

