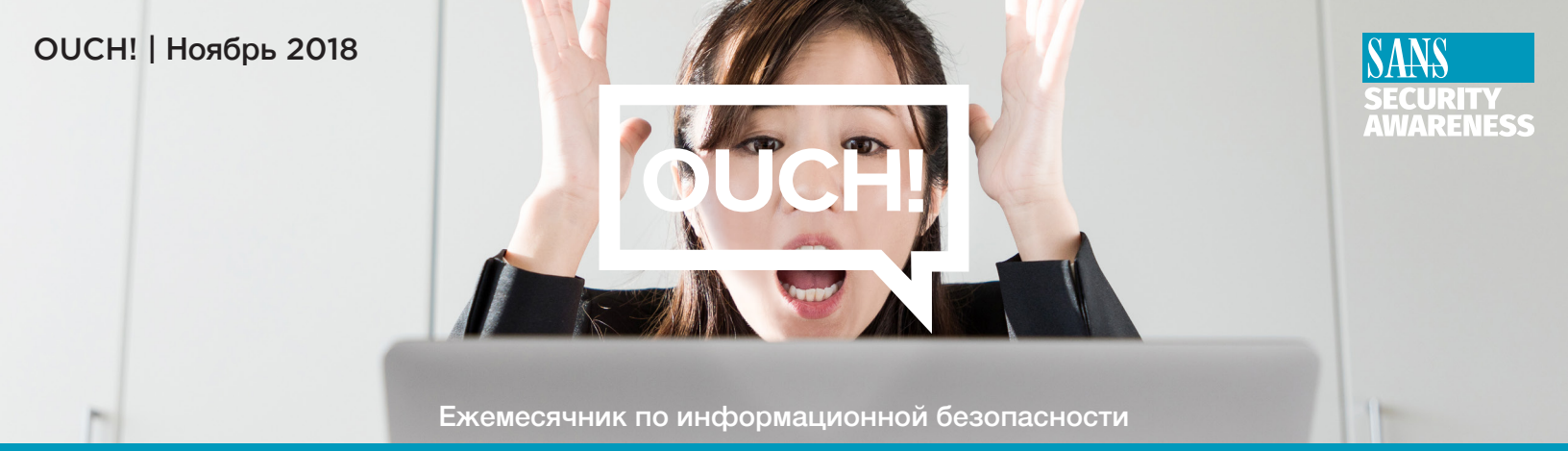

Ежемесячник по информационной безопасности

Мой компьютер взломали?

Обзор

Независимо от того, насколько вы соблюдаете правила безопасности - как и в случае вождения автомобиля - рано или поздно может произойти инцидент. В этой статье мы поговорим о признаках взлома компьютера и что делать, если взлом произошел. Чем раньше вы обнаружите взлом системы, тем проще устранить последствия.

Признаки того, что ваш компьютер взломали

Ваша программа-антивирус выдает сообщение о том, что ваш компьютер заражен. Убедитесь, что сообщение действительно от вашего антивируса, а не всплывающее окно от сайта, который пытается вынудить вас позвонить куда-то или загрузить неизвестную вам программу. Не уверены? Тогда откройте ваш антивирус и посмотрите.

Всплывающее окно говорит о том, что ваши данные зашифрованы и вам следует заплатить за их восстановление.

Ваш браузер открывает сайты, на которые вы не собирались заходить.

Ваш компьютер или приложения постоянно зависают, появляются иконки неизвестных приложений или странные всплывающие окна.

Ваши пароли больше не работают, даже если вы уверены в их правильности.

Друзья спрашивают, почему вы им присылаете спам по электронной почте, хотя вы ничего им не отправляли.

С вашей кредитной карты или банковского счёта списаны средства, а вы не совершали покупок и не снимали деньги.

Что делать

Если у вас есть подозрения, что ваш компьютер взломали, то действовать следует как можно быстрей. Если взломали ваш рабочий компьютер, не пытайтесь ничего предпринимать самостоятельно, а срочно свяжитесь со Службой Поддержки. Если взломали домашний компьютер или личный аккаунт, то следует предпринять следующее:

Смените все пароли. Необходимо сменить не только пароли на компьютере или мобильном устройстве, но и пароли ко всем вашим интернет-аккаунтам. Но не используйте для этого компьютер, который взломали - используйте другую систему, в безопасности которой вы уверены. Если у вас очень много аккаунтов, то начните менять пароли на самых важных. Если не можете запомнить все пароли, воспользуйтесь менеджером паролей.

Финансы. Если возникли проблемы с вашими кредитными картами или банковскими счетами, немедленно свяжитесь со службой поддержки банка. Звонить следует по телефону, который указан на обратной стороне банковской карты или на сайте банка, который вы открыли с проверенного компьютера. Банковскую карту следует немедленно заблокировать.

Антивирус. Если ваш антивирус выдает сообщение о инфицированных файлах, то следуйте его инструкциям. Большинство антивирусов выдают ссылки, по которым вы можете получить дополнительную информацию о вирусе.

Переустановка системы. Если вы не можете исправить повреждения или хотите быть уверенны в безопасности системы, то следует переустановить операционную систему. Не следует это делать из резервной копии – используйте её только для восстановления личных данных. Если вы не знаете, как это правильно сделать, воспользуйтесь услугами профессионалов. А если ваш компьютер старый, то наиболее простым решением будет покупка нового устройства. После того, как вы переустановили или заменили систему, настройте автоматическое обновление.

Резервные копия. Основной способ защитить себя от будущих проблем – создание регулярных резервных копий. Большинство систем позволяют делать резервные копии ежедневно или даже каждый час. Вне зависимости от того, какое решение вы выберете, обязательно проверьте возможность восстановления данных с резервной копии. Ведь иногда резервная копия может стать единственной возможностью восстановления данных в случае взлома компьютера.

Нарушение закона. Если вы чувствуете, что вам угрожают, немедленно обратитесь в местный органы правопорядка. Если вы стали жертвой кражи личности в США, то заполните заявление об этом на сайте https://www.identitytheft.gov.

Об авторе

Доктор Йоханнес Ульрих *(@johullrich) – Декан факультета Исследований Института SANS, Директор Центра Мониторинга Интернета (Internet Storm Center) Института SANS. Он создал распределенную сеть сенсоров DShield и ведёт ежедневные подкасты Internet Storm Center по безопасности сетей.*

Ресурсы

Резервное копирование и восстановление: https://www.sans.org/u/JGP
Парольные фразы: https://www.sans.org/u/JGU
Менеджер паролей: https://www.sans.org/u/JGZ
Что такое вредоносные программы: https://www.sans.org/u/JH4
Credit Freeze: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Как заблокировать кредитную карту: http://creditsecrets.ru/articles-card/56-kak-zablokirovat-kreditnuyu-kartu.html

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:* www.sans.org/security-awareness/ouch-newsletter. *Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова*