Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Ваши аккаунты**
- **Ваши мобильные устройства**
- **Ваша информация**

Ваш компьютер взломали: что делать?

ОБ АВТОРЕ

Автор этого выпуска – Чад Тилбари. У него большой опыт расследования компьютерных преступлений. Чад является соавтором курса FOR408 Windows Forensics и FOR508 Advanced Forensics, преподает в Институте SANS курс по реагированию на инциденты. Чад Тилбари ведёт записи в Twitter как @chadtilbury и публикует блог forensicmethods.com

ОБЗОР

Независимо от того, какие шаги вы предпринимаете, чтобы защитить свою информацию, все равно есть вероятность взлома. Это как вождение автомобиля: независимо от того, насколько вы внимательны за рулем, рано или поздно можете попасть в аварию. Тем не менее, вы можете защитить себя даже после взлома вашего компьютера. Чем раньше вы обнаружите, что вас взломали и чем быстрее отреагируете, тем меньше вреда вам нанесут. Чтобы помочь вам, мы обсудим различные способы диагностики взлома учетных записей, компьютера или данных и варианты защиты. Большинство наших советов относится к личной жизни, поэтому если вы несёте ответственность за служебную информацию, устройства и рабочие учётные записи, то следует немедленно сообщить в Службу Поддержки или сотрудникам Информационной Безопасности вашей организации и следовать их указаниям.

ВАШИ АККАУНТЫ

Скорее всего, у вас есть множество учетных записей: банковских счетов, онлайн покупок, почты и социальных сетей. Отследить и определить, когда аккаунт был взломан, непросто. Вот некоторые шаги, которые помогут выявить взлом аккаунта и отреагировать на него.

Признаки:

- Вы больше не можете войти в аккаунт, хотя уверены, что пароль правильный;
- Ваши друзья или коллеги получают от вас электронные письма, которые вы не отправляли;
- Кто-то от вашего имени опубликовал сообщения в социальной сети (например, Facebook или Twitter);
- Кто-то перевёл деньги онлайн с вашего банковского счета;
- Ваша контактная информация или другие параметры вашей учетной записи изменены без вашего ведома или согласия;
- Вебсайт или организация опубликовали информацию о взломе учётных записей или паролей пользователей.

Действия

- Если вы всё ещё можете войти в аккаунт, немедленно смените пароль; как и всегда, используйте только надежный пароль;

Ваш компьютер взломали: что делать?

- Если вы не можете войти в систему, обратитесь в Службу Поддержки сайта или организации. Большинство организаций предоставляют возможность пользователям сообщить о взломе: онлайн форма, адрес электронной почты или номер телефона для связи в таких случаях;
- После восстановления доступа, проверьте все атрибуты вашей учетной записи; злоумышленники могли их изменить;
- Убедитесь, что вы изменили пароли и на других аккаунтах, если пароль был одинаковый (вообще, никогда не используйте одинаковые пароли).

ВАШИ МОБИЛЬНЫЕ УСТРОЙСТВА

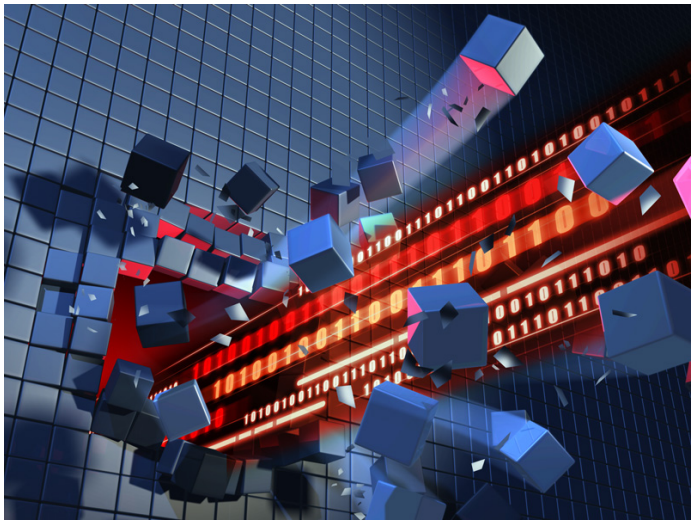
При огромном изобилии мобильных устройств в наше время, возникает необходимость их защищать. Как только злоумышленники получают доступ к устройству, они могут контролировать все действия, которые устройство осуществляет. Вот некоторые шаги, которые помогут правильно определить и реагировать на взлом.

Признаки:

- Ваш компьютер открывает сайты, на которые вы не собирались.
- Ваш компьютер запускает программы, которые вы не устанавливали.
- Ваша антивирусная программа сообщает о наличии вируса.
- Антивирус не может обновляться; системные обновления не устанавливаются.
- Ваше устройство постоянно дает сбои в работе.
- Ваш смартфон без вашего ведома делает дорогие звонки или устанавливает платные приложения без вашего разрешения.

Действия:

- Выполните полное сканирование обновлённой версией антивируса. Если антивирус обнаружит заражённые файлы, следуйте инструкции антивируса. Вы можете провести вторичную проверку с помощью онлайн сканеров;
- Если устройство нельзя проверить специальными программами или вы хотите убедиться в полной безопасности устройства, переустановите операционную систему или осуществите восстановление оригинальной заводской конфигурации, установите последнюю версию антивируса и восстановите данные из резервной копии. (Вы ведь регулярно делаете резервные копии личных



чем раньше вы поймёте, что вашу систему взломали и примете меры, тем больше шансов свести ущерб к минимуму.

Ваш компьютер взломали: что делать?

данных?).

ВАША ИНФОРМАЦИЯ

Защита ваших персональной информации, например, паспортных данных, ИНН, данных медицинской карты и истории покупок - непростая задача, так как в большинстве случаев не вы контролируете эти данные. Такой информацией обладают ваш врач, банк, выдавший кредитную карту, магазины. Вот некоторые шаги, которые помогут определить утечку данных и действия, которые следует предпринять.

Признаки:

- Поставщик услуг (банк или поликлиника) сообщает, что взломали базу данных и номер вашей кредитной карты или историю болезни могли украсть;
- С вашей кредитной карты производят несанкционированные платежи;
- В кредитных отчетах вы видите заявки на кредиты, которые вы не подавали;
- Ваша медицинская страховая компания обрабатывает заявки, которые вы не подавали;
- Вы получаете письма о просроченных платежах по счетам, которые не открывали.

Действия:

- Немедленно свяжитесь с организацией, выдавшей кредитные карты. Заблокируйте старые и закажите новые, эту услугу банки должны предоставлять бесплатно;
- Обратитесь к поставщику услуг. Например, если произошло мошенничество с услугами страховой компании или с банковским счётом, обратитесь в страховую компанию или банк напрямую;
- Во время любых обращений, всегда документируйте переговоры с датой, временем и фамилией сотрудника, с которым общались. Храните копии всех писем и отправляйте корреспонденцию заказным письмом для подтверждения доставки.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Некоторые ссылки были сокращены для удобства чтения с помощью сервиса TinyURL. Для повышения безопасности OUCH! всегда использует функцию предварительного просмотра TinyURL, которая показывает вам настоящий адрес, на который будет переадресована ссылка и запрашивает ваше разрешение для перехода по ней.

Как взломали мой компьютер:
http://preview.tinyurl.com/8q2jwsu
Бесплатные онлайн сканеры безопасности:
http://preview.tinyurl.com/9ky9s6w
Куда обращаться в случае интернет преступления:
http://www.ic3.gov/default.aspx
Кража личности: информационный портал:
http://www.idtheftcenter.org/
Facebook: Что делать, если ваша учётная запись взломана: www.facebook.com/help/hacked
Термины по безопасности:
http://preview.tinyurl.com/6wkpae5
Ежедневные советы Института SANS по безопасности: http://preview.tinyurl.com/6s2wrkp

УЗНАЙ БОЛЬШЕ

Подпишись на ежемесячную рассылку OUCH! по вопросам компьютерной безопасности для пользователей, просмотри архивы OUCH! и узнай больше о решениях в области компьютерной безопасности SANS, посетив наш сайт:

Наши авторы: Билл Уайман, Уолт Скривенс, Фил Хоффман, Ланс Спицнер, Кармен Рael Харди.
Перевод: Александр Котков