Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Признаки взлома
- Что предпринять в случае взлома

Мой компьютер взломали. Что делать?

Обзор

Мы знаем, что вы заботитесь о безопасности вашего компьютера или мобильного устройства. Но, несмотря на все меры предосторожности, рано или поздно ваш компьютер взломают или «скомпрометируют». В этом выпуске мы поговорим о том, как определить, был ли взломан ваш компьютер или устройство и что делать дальше в случае взлома. Прежде всего, чем быстрее вы обнаружите что-то странное и примите меры, тем меньший вред взломщики смогут вам причинить.

Об авторе

Саманта Дэвисон (**@sam_e_davison**) - менеджер по обучению основам информационной безопасности компании Uber, сотрудники которой работают более чем в 350 городах мира.

Признаки взлома

Иногда понять, что вас взломали достаточно сложно, так как нет единственного отчетливого признака. Но есть ряд ключевых признаков, так называемых индикаторов, указывающих на взлом. Если в вашей системе происходит что-то подобное, то, возможно, её взломали.

- Ваш антивирус выдаёт сообщение, что система инфицирована, также вы не можете удалить инфицированные файлы или поместить их в карантин.
- Стартовая страница вашего браузера изменилась без вашего участия или вы попадаете не на ту страницу, на которую собирались зайти.
- Вы обнаружили новые учетные записи, которые вы не создавали, или система запускает новые программы, которые вы не устанавливали.
- Система или приложения ведут себя необычно, вы нашли новые иконки или странные всплывающие окна.
- Программа запрашивает разрешение на изменения в конфигурации системы, хотя вы ничего не устанавливаете и не обновляете.
- Ваш пароль перестает работать, вы не можете войти с ним в систему или в интернет приложение, хотя вы точно знаете, что пароль правильный.
- Ваши друзья говорят, что вы спамите их по электронной почте, но вы не отправляли им никаких писем.
- Ваше мобильное устройство без вашего участия рассылает платные смс сообщения.

Мой компьютер взломали. Что делать?

- Ваше мобильное устройство использует необъяснимо много сетевых ресурсов или батарейка слишком быстро разряжается.

рано или поздно ваш компьютер или устройство взломают. Чем раньше вы это обнаружите и примите меры, тем лучше.

Что предпринять в случае взлома

Если вы обнаружили, что ваше устройство взломали, то действовать нужно как можно быстрее. Если это рабочий компьютер или устройство, то не пытайтесь устранить проблему самостоятельно. Не потому, что вы можете навредить ещё больше, просто вы случайно можете удалить следы, по которым будут расследовать инцидент. Немедленно сообщите вашему работодателю об инциденте, свяжитесь со Службой Поддержки, Службой безопасности или с непосредственным руководителем. Если по какой-то причине вы не можете связаться с работодателем, или вы беспокоитесь, что потеряете много времени, то первым дело отключите компьютер или устройство от сети и включите режим сна, ожидания или режим «самолет». Даже если вы не уверены окончательно, что вас взломали, все равно следует сообщить о своих подозрениях. Если это ваш личный компьютер или устройство, то следует предпринять следующее.

- **Смените пароли**: мы говорим не только о смене пароля доступа к компьютеру или мобильному устройству, но и пароли ко всем своим учетным записям. Убедитесь, что для смены паролей вы не используете взломанный компьютер, следует воспользоваться другим компьютером или устройством.
- **Антивирус**: Если ваш антивирус сообщает об инфицировании системы, вам следует сделать следующее. Файл помещают в карантин, чистят или удаляют. Большинство антивирусных программ содержат ссылки на сайты, на которых можно узнать больше о видах вирусов. Если есть подозрительный файл, поместите его в карантин, если это сделать не получается, то удалите его.
- **Переустановка системы**: Если вы не можете справиться с вирусом или хотите быть абсолютно уверены, что система чистая, то переустановите её. В компьютерах есть инструкция производителя. В других случаях воспользуйтесь встроенной функцией переустановки системы. Если эта функция не работает, повреждена или инфицирована, поищите инструкцию производителя или зайдите на его сайт. Не используйте для переустановки операционной системы резервную копию, так как в ней могут быть уязвимые места, через которые злоумышленники могут получить доступ к системе ещё раз. Резервную копию следует использовать только для восстановления данных. В случае с мобильными устройствами,

Мой компьютер взломали. Что делать?

следуйте рекомендациям производителя или провайдера услуг, скорее всего, информация доступна на их сайте. В большинстве случаев, достаточно вернуться к настройкам производителя. Если вы сомневаетесь в правильности своих действий, обратитесь за помощью к профессионалам. Если ваш компьютер или мобильное устройство старые, в некоторых случаях дешевле будет купить новое устройство. Когда вы переустановите систему или купите новое устройство, убедитесь, что используете последнюю версию, регулярно обновляетесь или настроили автоматическое обновление.

- **Резервное копирование**: Один из важнейших шагов, который вы можете сделать для защиты и экономии времени в будущем – это регулярное создание резервных копий. Чем чаще вы их делаете, тем лучше. Некоторые современные технологии позволяют делать резервные копии каждый час или при каждом изменении. Периодически проверяйте возможность восстановления данных из этих копий. И ни в коем случае не используйте резервные копии для восстановления системы в случае взлома, это шаг к следующему взлому.
- **Правоохранительные органы**: если вам угрожают, происходит что-то противозаконное, сообщите об инциденте в правоохранительные органы.

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

Резервное копирование и восстановление данных:	https://securingthehuman.sans.org/ouch/2015#august2015
Паролевые фразы:	https://securingthehuman.sans.org/ouch/2015#april2015
Что такое вредоносные программы:	https://securingthehuman.sans.org/ouch/2016#march2016
Безопасность планшета:	https://securingthehuman.sans.org/ouch/2016#january2016

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова