OUCH! Февраль 2021

SANS SECURITY AWARENESS

Ежемесячный информационный бюллетень по безопасности

Меня взломали. Что теперь?

Разве я был взломан?

Независимо от того, насколько вы защищены, рано или поздно вы можете попасть ситуацию и стать жертвой взлома. Ниже приведены ключи вы, возможно, были взломаны, и если да, то что делать.

Ваши онлайн-аккаунты

- Семья или друзья сообщают, что получают от вас необычные сообщения или приглашения, которые, как вы знаете, не отправляли.
- Ваш пароль к учетной записи больше не работает, даже если вы знаете, что пароль правильный.
- Вы получаете уведомления с веб-сайтов о том, что кто-то вошел в вашу учетную запись, когда вы знаете, что не выполняли вход самостоятельно. Не переходите по ссылкам в таких уведомлениях, чтобы проверить свою учетную запись; вместо этого введите адрес веб-сайта самостоятельно в браузере, используйте ранее сохраненную закладку или войдите в свою учетную запись из мобильного приложения.

Ваш компьютер или мобильное устройство

- Ваша антивирусная программа выдает предупреждение о заражении вашей системы. Убедитесь, что это ваше антивирусное программное обеспечение генерирует предупреждение, а не случайное всплывающее окно с веб-сайта, пытающегося обманом заставить вас позвонить по номеру или установить что-то еще. Не уверены? Откройте и проверьте свою антивирусную программу, чтобы убедиться, что ваш компьютер действительно заражен.
- Вы увидите всплывающее окно с сообщением, что ваш компьютер зашифрован, и вам нужно заплатить выкуп, чтобы вернуть свои файлы.
- Приложения кажутся случайными или загружаются очень медленно.
- При просмотре веб-страниц вы часто будете перенаправлены на страницы, которые вы не хотите посещать, или появляются новые, нежелательные страницы.

Финансовые

- С вашей кредитной карты или банковского счета идут подозрительные или неизвестные расходы, которые вы не делали.

Что теперь? - Как вернуть контроль

Если вы подозреваете, что вы были взломаны, сохраняйте спокойствие; вы пройдете через это. Если взлом связан с работой, не пытайтесь решить проблему самостоятельно; немедленно сообщите об этом. Если взломана личная система или учетная запись, вы можете предпринять следующие шаги:

- **Восстановление ваших онлайн-аккаунтов:** Если у вас все еще есть доступ к своей учетной записи, войдите в систему с надежного компьютера, который, как вы уверены, не заражен, и сбросьте пароль. После входа в систему не забудьте установить новый, уникальный и надежный пароль, чем длиннее, тем лучше. Помните, что у каждой из ваших учетных записей должен быть свой пароль. Если вы не можете отслеживать их все, рекомендуем использовать менеджер паролей. Кроме того, если это возможно, включите многофакторную аутентификацию (MFA) для своих учетных записей, чтобы кибер-злоумышленники не смогли вернуться в систему. Если у вас больше нет доступа к своей учетной записи, свяжитесь с веб-сайтом и сообщите им, что ваша учетная запись была взломана.
- **Восстановление вашего персонального компьютера или устройства:** Если ваша антивирусная программа не может исправить зараженный компьютер или вы хотите быть уверены в безопасности своей системы, подумайте о переустановке операционной системы и восстановлении компьютера. Часто для этого требуется стереть или заменить диск, а затем переустановить и обновить операционную систему. Не переустанавливайте операционную систему из резервных копий. Резервные копии следует использовать только для восстановления ваших личных файлов. Если вы чувствуете затруднение при восстановлении, подумайте об использовании профессиональных услуг. Или, если ваш компьютер или устройство устарело, возможно, пришло время купить новое.
- **Восстановление ваших финансовых счетов:** По вопросам, связанным с вашей кредитной картой или любыми финансовыми счетами, сразу звоните в свой банк или эмитент кредитной карты. Позвоните им, используя надежный номер телефона, например номер, указанный на обратной стороне вашей банковской карты, номер, указанный в вашей финансовой отчетности, или посетите их веб-сайт. Следите за своими выписками и кредитными отчетами. Кроме того, рассмотрите возможность заморозить свой кредитный отчет.

Если вы понесли финансовый ущерб или чувствуете какую-либо угрозу, сообщите об этом в местные правоохранительные органы.

Приглашенный редактор

Максим Девеердт (Twitter @alfasec) является сертифицированным инструктором в институте SANS, в основном преподает курсы по киберзащите. Он также является главным консультантом в NVISO, где специализируется на проектах по отслеживанию угроз, реагированию на инциденты и SOC.

Ресурсы

Обновление: : https://www.sans.org/security-awareness-training/resources/power-updating
Резервные копии: https://www.sans.org/security-awareness-training/resources/got-backups
Создание простых паролей: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Программы-вымогатели: https://www.sans.org/security-awareness-training/resources/ransomware
Сообщить о краже личных данных: https://www.identitytheft.gov
Заморозить кредитный отчет: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

Переведено для сообщества: Роман Поляков