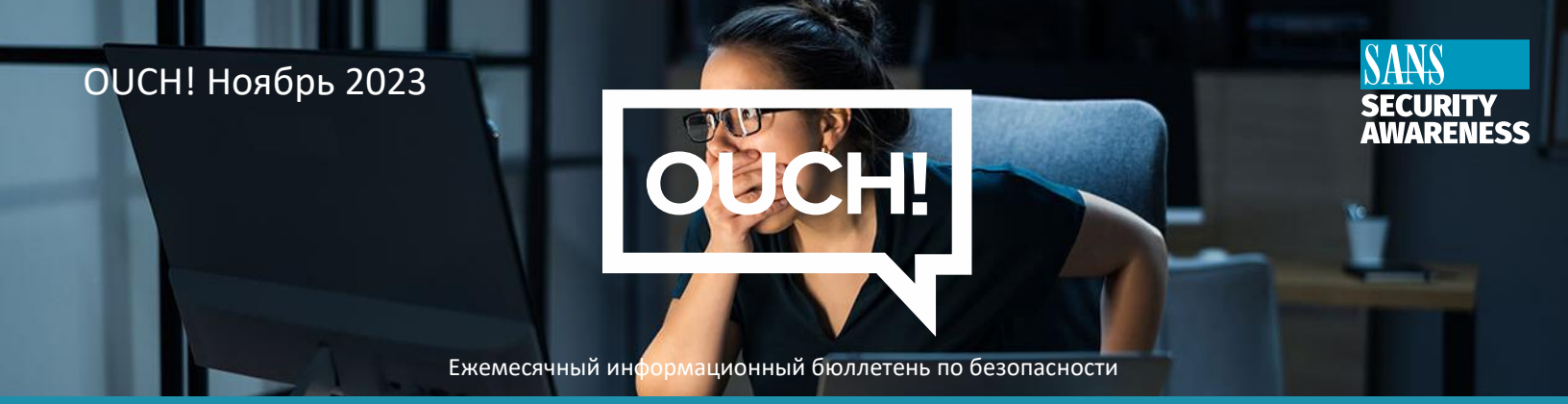
OUCH! Ноябрь 2023



Ежемесячный информационный бюллетень по безопасности

Меня взломали, что делать?

Разве я был взломан?

Интернет может быть подавляющим, поскольку новые технологии постоянно меняются. Независимо от того, насколько вы пытаетесь обеспечить безопасность, рано или поздно вам может не повезти, и вас взломают. Чем раньше вы обнаружите, что произошло что-то плохое, и чем быстрее вы отреагируете, тем больше вы сможете минимизировать последствия. Ниже приведены признаки того, что вас могут взломать, а также, предложения по устранению этой проблемы.

Признаки того, что одна из ваших онлайн-учетных записей могла быть взломана

- 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.
- Вы получаете электронные письма с подтверждением изменений в вашем онлайн-профиле, которые вы не вносили.

Признаки того, что ваш компьютер или мобильное устройство взломали

- 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.
- При просмотре веб-страниц вы часто будете перенаправлены на страницы, которые вы не хотите посещать, или появляются новые, нежелательные страницы.
- Вы увидите всплывающее окно с сообщением, что ваш компьютер зашифрован, и вам нужно заплатить выкуп, чтобы вернуть свои файлы.

Признаки того, что ваша кредитная карта или финансы были взломаны

- 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 вас взломали, сохраняйте спокойствие. Вы пройдете через это. Если взлом связан с работой, не пытайтесь решить проблему самостоятельно. Вместо этого 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 доверенного компьютера и сбросьте пароль, используя новый, уникальный и надежный пароль — чем длиннее, тем лучше. Если у вас не включена многофакторная аутентификация (MFA), сейчас самое время включить ее. Если у вас больше нет доступа к своей учетной записи, свяжитесь с веб-сайтом и сообщите им, что ваша учетная запись была взломана. Если у вас есть другие учетные записи с тем же паролем, что и ваша взломанная учетная запись, немедленно измените пароль.
- **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. Или, если ваш компьютер или устройство устарело, возможно, пришло время купить новое.
- **Финансовые последствия:** По вопросам, связанным с вашей кредитной картой или любыми финансовыми счетами, сразу звоните в свой банк или эмитент кредитной карты. Чем раньше вы позвоните им, тем больше вероятность, что вы сможете вернуть свои деньги. Позвоните, 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. Если возможно, включите автоматические уведомления при списании средств или переводе денег.

Что делать, чтобы опередить киберзлоумышленников?

Информационный бюллетень OUCH Security Awareness публикуется ежемесячно и содержит целую серию статей о том, как обезопасить себя. В разделе «Ресурсы» ниже мы перечисляем наиболее важные информационные бюллетени OUCH, которые стоит прочитать, чтобы защитить себя. Эти ресурсы посвящены трем ключевым шагам:

1. Постоянно обновляйте все свои системы и устройства до последней версии.
2. Используйте надежные и уникальные пароли для каждой из своих учетных записей, управляйте этими учетными записями с помощью диспетчера паролей и включите MFA.
3. Будьте скептичны — следите за приемами социальной инженерии, такими как фишинговые электронные письма.

Приглашенный редактор

Сара Моралес — (@SarahManley) старший менеджер программы в отделе конфиденциальности, безопасности и защиты Google. Она возглавляет внешнее взаимодействие, уделяя особое внимание построению сообщества, сотрудничеству и партнерству. Она является членом правления Wicys и активно участвует в усилиях DEI в сообществе кибербезопасности.

Ресурсы

Менеджеры паролей: https://www.sans.org/newsletters/ouch/power-password-managers
MFA: один простой шаг к защите ваших учетных записей: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Эмоциональные триггеры: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Фишинговые атаки становятся все более изощренными: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Роман Полаков