

Как быть, если аккаунт взломали? Алгоритм действий





Подумайте, можно ли украсть деньги через взломанный профиль

Преступники получили доступ к аккаунту в платежной системе? Срочно обратитесь в банк и заблокируйте карты и счета, до которых они могут добраться.

Альтернативный вариант — заблокировать саму учетную запись, однако это не всегда выходит сделать оперативно.

Взломали профиль, к которому привязана карта? Это тоже опасно. Если уверены, что без дополнительного подтверждения от вас ничего купить/перевести нельзя, хорошо. В ином случае заблокируйте платежное средство.



Верните аккаунт под свой единоличный контроль

Попробуйте сменить пароль для входа в профиль. Если злоумышленники не сделали этого раньше вас, они лишатся доступа к странице. **Также отвяжите от сервиса электронную почту,** к которой он был привязан, или установите новый пароль для этой почты.

Не можете изменить пароль, или у вас не получается войти в профиль в принципе? Попробуйте самостоятельно восстановить доступ к аккаунту. Для этого в большинстве сервисов предусмотрена специальная форма. При возникновении трудностей обратитесь в поддержку.



Аккаунт снова ваш, но этого недостаточно

Итак, вы изменили данные для входа в профиль (пароль и/или электронную почту). Отлично! **Теперь выйдите из аккаунта (завершите активные сеансы) со всех устройств, кроме текущего.** Обычно это можно сделать в разделе «Безопасность». Так вы наверняка «изгоните» злоумышленников, прервав их активные сеансы.

Если у вас «угнали» профиль в соцсети или мессенджере, сообщите о взломе всем, кому сможете. Сделайте общую рассылку и, при возможности, разместите на странице пост с рассказом о случившемся. Так вы убережете от мошенников близких и знакомых.



Лучше перестраховаться

Основные угрозы устранены, но расслабляться рано. Кто знает, что успели сделать злоумышленники, пока владели вашим аккаунтом? Чтобы избежать неприятных сюрпризов, перестрахуйтесь.

Смените все пароли, совпадающие с паролем от взломанного аккаунта. И, пожалуйста, на этот раз используйте разные пароли для каждого сайта или приложения. Также вспомните, к каким важным сервисам был привязан взломанный аккаунт, отвяжите их от скомпрометированной учетной записи и выберите новые пароли.



РОЦИТ



Время стереть следы преступления

Злоумышленники, конечно, ушли из вашего аккаунта, но следы их присутствия могли остаться.

Проверьте, все ли в порядке. Смело удаляйте незнакомые расширения, игры, группы и так далее.

Проверьте устройства на наличие вирусов. Возможно, именно вредоносная программа стала причиной того, что ваш аккаунт взломали.



Лучше перестраховаться

Взлом и похищение аккаунта можно предотвратить, если внимательно отнестись к его безопасности. Помните:

- ✦ Двухфакторная аутентификация — ваш лучший друг. Она в разы усилит защиту аккаунта от несанкционированного проникновения.
- ✦ Создавайте сложные и уникальные для каждого(!) аккаунта. Не обязательно самим ломать голову над комбинациями знаков и исписывать блокнот. Для удобства можно использовать генераторы и менеджеры паролей.



Лучше перестраховаться

- ✦ Не передавайте данные для входа третьим лицам. Даже если у вас самый надежный на свете пароль, он никак не спасет от фишинга. Оградить от мошенников может лишь критическое мышление.
- ✦ Не переходите по подозрительным ссылкам и не скачивайте сомнительные приложения. Существует вредоносное ПО, способное украсть учетные данные. Защитить от него может бдительность и хороший антивирус.
- ✦ Не используйте VPN-сервисы. Известно немало примеров утечек данных, собранных VPN. Порой в слитых базах оказывается чувствительная информация пользователей, в том числе касающаяся учетных записей.