

Что делать, если вас взломали

Как только вы обнаружили взлом – отложите свой телефон или ноутбук. Все последующие действия вы должны выполнять с другого устройства: злоумышленник может видеть, что вы делаете.

Полиция круглосуточно

Позвоните в дежурную часть.

Скажите:

«Неизвестные получили доступ к моим Госуслугам, электронной подписи, банковским счетам и счетам юридических лиц»

Звонок необходим, чтобы зафиксировать факт: потом пригодится для банков и налоговой. Не бойтесь, что «мало доказательств»: фиксация – это стандартная процедура.

ИТ и ИБ вашей компании

Немедленно сообщите руководителю службы ИБ и ИТ-директору.

Скажите:

«Возможна компрометация моей учётной записи и электронной подписи. До отдельного распоряжения не проводите платежи, не меняйте реквизиты, не выдавайте доверенности от моего имени»

Позвоните по телефону: 8 (495) 956 79 37, доб. 1111

Госуслуги

Позвоните в Госуслуги.

Скажите:

«Произошёл несанкционированный доступ к моей учётной записи»



ВАЖНО

Если оператор начинает переводить вас по меню – не вешайте трубку, попросите соединить со специалистом по безопасности учётных записей.

Попросите:

- зафиксировать ваше сообщение о взломе
- объяснить, как выбросить посторонних из сессий
- сказать, нужен ли визит в МФЦ

Позвоните по телефону: 8 800 100 70 10 или 115

Мобильная связь

Позвоните всем операторам своих SIM/eSIM.

Скажите:

«Подозреваю компрометацию номера»



ВАЖНО

Попросите установить дополнительный пароль на номер – тогда без него никто не сможет сделать дубликат SIM.

Попросите:

- не выпускали ли новую SIM на ваш номер
- не включали ли переадресацию
- не менялись ли ваши паспортные данные или кодовое слово
- не заходили ли незнакомые люди в ваш личный кабинет



«Р-Фарм» –
люди действия

Банки личные счета

Позвоните
в банк.

Скажите:
«Мои данные и электронная
подпись могли утечь»



ПРОВЕРЬТЕ
Последние операции, входящие переводы,
заявки на кредиты, новые счета, добавленные
устройства, изменение лимитов.

Попросите:

- зафиксировать факт мошенничества
- завершить все активные сессии (выбросить всех, кто сейчас сидит в личном кабинете)
- заблокировать незнакомые устройства
- не давать оформлять кредиты и выпускать карты удалённо

Банки счета компании

Позвоните
в круглосуточную
корпоративную
поддержку
каждого банка.

Скажите:
«Скомпрометированы данные
руководителя и электронная
подпись»



ЕСЛИ ОТКАЗЫВАЮТ
Попросите поставить отметку «повышенный
риск» и временно ограничить расходные
операции (это тоже работает).

Попросите:

- приостановить дистанционное банковское обслуживание
- завершить все сессии
- заблокировать токены
- запретить добавление пользователей, выпуск карт, смену подписантов и изменение реквизитов до вашего личного подтверждения

Удостоверя- ющий центр электронная подпись

Звоните, только
если потеряли
физический
носитель — токен
или флешку
с подписью.

Скажите:
«Утерян закрытый ключ, требую
немедленный отзыв сертификата»

Если токен лежит у вас дома
в ящике — звонить не нужно, просто
не используйте его до окончания
разбирательств.

ДОКАЗАТЕЛЬСТВА

Не удаляйте подозрительные приложения и файлы.
Отключите телефон от сети (включите авиарежим), обесточьте ноутбук
и передайте службе ИТ или следователям для анализа.
Удалённые данные восстановить сложнее.



«Р-Фарм» —
люди действия

Восстановление контроля

Что взять с собой: паспорт, СНИЛС, ИНН, документы на компании, токен электронной подписи.

МФЦ

Лично посетите МФЦ при первой возможности.

Скажите:

«Учётная запись могла быть похищена. Прошу восстановить доступ и исключить посторонних»

После восстановления:

- сразу смените пароль
- проверьте, какой телефон и почта привязаны
- завершите все сессии
- проверьте заявления, доверенности и согласия, поданные от вашего имени
- включите усиленную защиту

Банки

Лично посетите банки при первой возможности.

Потребуйте письменную фиксацию:

- факта компрометации
- запрета на дистанционное восстановление доступа
- блокировки незнакомых устройств
- проверки операций

По счетам компании потребуйте:

- замену ключей для дистанционного банковского обслуживания
- блокировку старых токенов
- проверку платежей
- запрет на изменение подписантов

МВД

Повторно позвоните или придите в отделение. Узнайте статус проверки, спросите, нужна ли ваша явка.

Обязательно получите:

- талон-уведомление
- номер КУСП (книга учёта заявлений и сообщений о преступлениях)
- дату и время регистрации
- данные сотрудника, который принял обращение

ФНС

Федеральная налоговая служба

Уточните:

- куда подать сообщение о компрометации электронной подписи
- какие инспекции ведут ваши ООО
- как проверить, не подавали ли мошенники регистрационные заявления от имени ваших компаний
- куда направить письменное возражение, если найдёте поддельные заявления

Позвоните по телефону: 8 800 222 22 22.



«Р-Фарм» —
люди действия

МЧД

Машиночитаемые доверенности

Проверьте реестр доверенностей ФНС.

Полный список выданных доверенностей не показывают по соображениям безопасности, но вы можете проверить через доступные интерфейсы, есть ли доверенности на ваше имя.

Если найдёте незнакомые – отзовите их и зафиксируйте факт отзыва (скриншот, распечатка).

Кредиты и недвижимость

Сделайте:

- установите самозапрет на кредиты через Госуслуги
- запросите кредитный отчёт в бюро кредитных историй (БКИ)
- через МФЦ подайте заявление в Росреестр о невозможности регистрации сделок с вашей недвижимостью без вашего личного участия

Если что-то не получается или вы застряли на каком-то шаге – обратитесь к службе ИБ компании.

Это их работа – они знают, что делать дальше.

Звоните по номеру 8 (495) 956 79 37 (доб. 1111), используя любой доступный способ связи.



«Р-Фарм» –
люди действия