ЧЕЛОВЕЧЕСКИЙ ФАКТОР В АНТИФРОДЕ И БЕЗОПАСНОСТИ

КАТЕРИНА НИКЕРИНА

Antifraud PO | Avito

Авито – крупнейший классифайд в мире.
Авито в цифрах:

- MAU = 60 млн пользователей
- 150 млн объявлений ежемесячно
- 10 сделок в секунду

Основная миссия антифрод-команды: безопасность пользователей, борьба с нарушениями, противодействие угрозам бизнеса.

КАТЕРИНА НИКЕРИНА

поговорим про фрод

ФРОД – ЭТО МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

ФРОД

Сюда относится

- Неправомерное использование ресурсов
- Доступ к банковскому счету, ворованные карты
- Оплата на подменные реквизиты
- Проникновение в аккаунт

Везде, где могут быть мошенники, нужен антифрод. Хороший антифрод блокирует мошенников, но не трогает хороших пользователей и их **ценные аккаунты**.

КАК ПОЛУЧИТЬ ДОСТУП К ЦЕННОМУ АККАУНТУ

01.
Простые пароли

02.
Переход по ссылке

03.
Фишинговые письма

04.
Неактуальные номера телефонов

05.
Социальная инженерия

06.
Боты и приложения для проверки

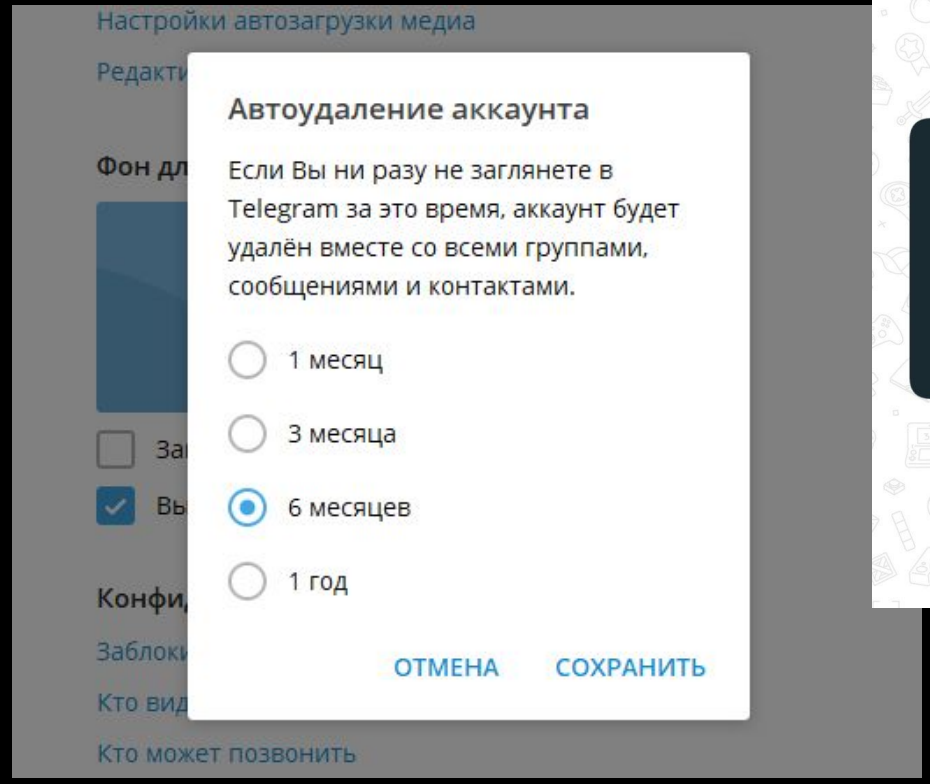
07.
Создание “ценного” профиля (прогрев)

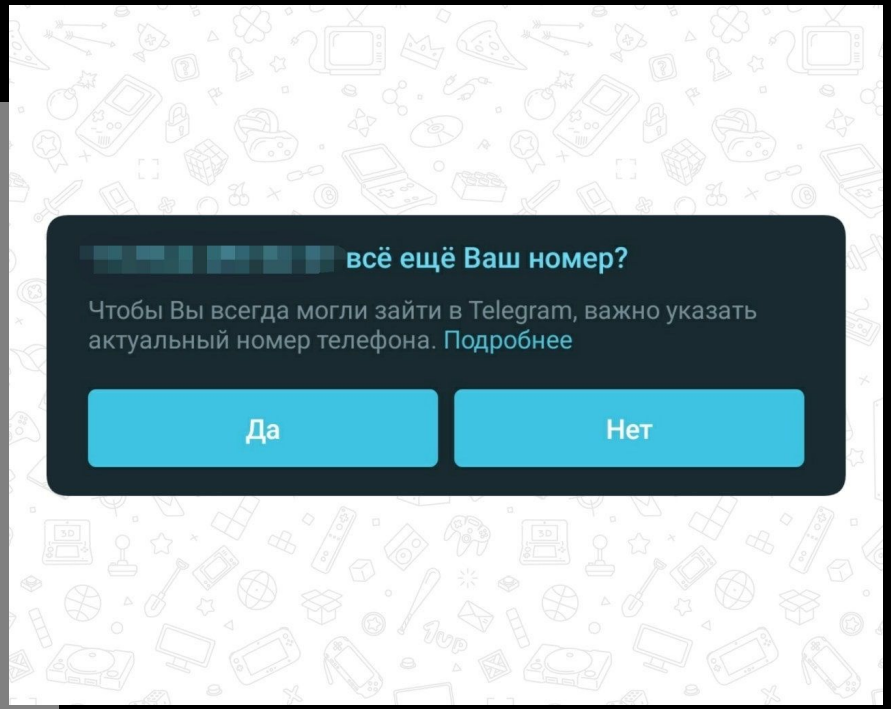
08.
Ещё много хитрых и нехитрых методов

КАК ПОЛУЧИТЬ ДОСТУП К ЦЕННОМУ АККАУНТУ

04.

Неактуальные номера телефонов





КАК ПОЛУЧИТЬ ДОСТУП К ЦЕННОМУ АККАУНТУ

07.

Создание “ценного” профиля (прогрев)

Авито отзывы | Накрутка отзывов

Накрутка отзывов Авито:

10 отзывов - 2000
30 отзывов - 5000
50 отзывов - 8500
100 отзывов - 15000

✅ Оплата после результата! 🔥

ИНСАЙТЫ ОБ ИНФРАСТРУКТУРЕ КОМПАНИИ

Рассылки про новый функционал

Информация об обновлениях

Служба поддержки

Судебные решения

поговорим про антифрод

КАК ПОЛУЧИТЬ ИНФОРМАЦИЮ О РАБОТЕ АНТИФРОД-СИСТЕМ

поговорим про антифрод

ПРИМЕРЫ

ВОССТАНОВЛЕНИЕ ДОСТУПА ЧЕРЕЗ СЛУЖБУ ПОДДЕРЖКИ

1. Как мы можем быть уверены, что нам звонит именно владелец учетной записи?

2. Как мы можем быть уверены, что его почта и телефон не скомпрометированы?

3. Как мы можем быть уверены, что он не на связи с мошенником прямо сейчас?

ВОССТАНОВЛЕНИЕ ДОСТУПА ЧЕРЕЗ СЛУЖБУ ПОДДЕРЖКИ

1. Как мы можем быть уверены, что нам звонит именно владелец учетной записи?
2. Как м
   телеф
3. Как мы можем быть уверены, что он не на связи с мошенником прямо сейчас?

ЧАСТО МЫ ОСТАВЛЯЕМ ЭТО НА ОТКУП ЮЗЕРА

ВОССТАНОВЛЕНИЕ ДОСТУПА ЧЕРЕЗ СЛУЖБУ ПОДДЕРЖКИ

1. Как мы можем быть уверены, что нам звонит имен
2. Как м
теле
3. Как мы можем быть уверены, что он не на связи с мошенником прямо сейчас?

ЧТО ПРОВЕРЯЮТ:
КАК МОЖНО ВОССТАНОВИТЬСЯ ВМЕСТО ПОЛЬЗОВАТЕЛЯ

КЕЙС ОТ БАНКА

Как мне потом объяснили и я ещё нашёл статью, датируемую от 2020 года, декабря (https://vc.ru/claim/183059-tinkoff-ban...mu-klientu), где была аналогичная проблема. Оказывается, если позвонить в тиньков в техподдержку с телефона другого человека, то в какой-то момент система будет проверять на дубли и может объединить ваши учётки, потому что тот номер записался как контактный, а у тинька нет понятия доп номера. Мы хотим - мы объединяем. Сейчас ситуация выходит довольно таки странная, потому что у меня нет счетов. У жены есть только те, которыми я с ней делился - и они на её ФИО. Она пишет
хрена они на меня, но я их не вижу. Они отве
другого номера или ждите объединения учёт

Владимир Zosim
8.09.2022

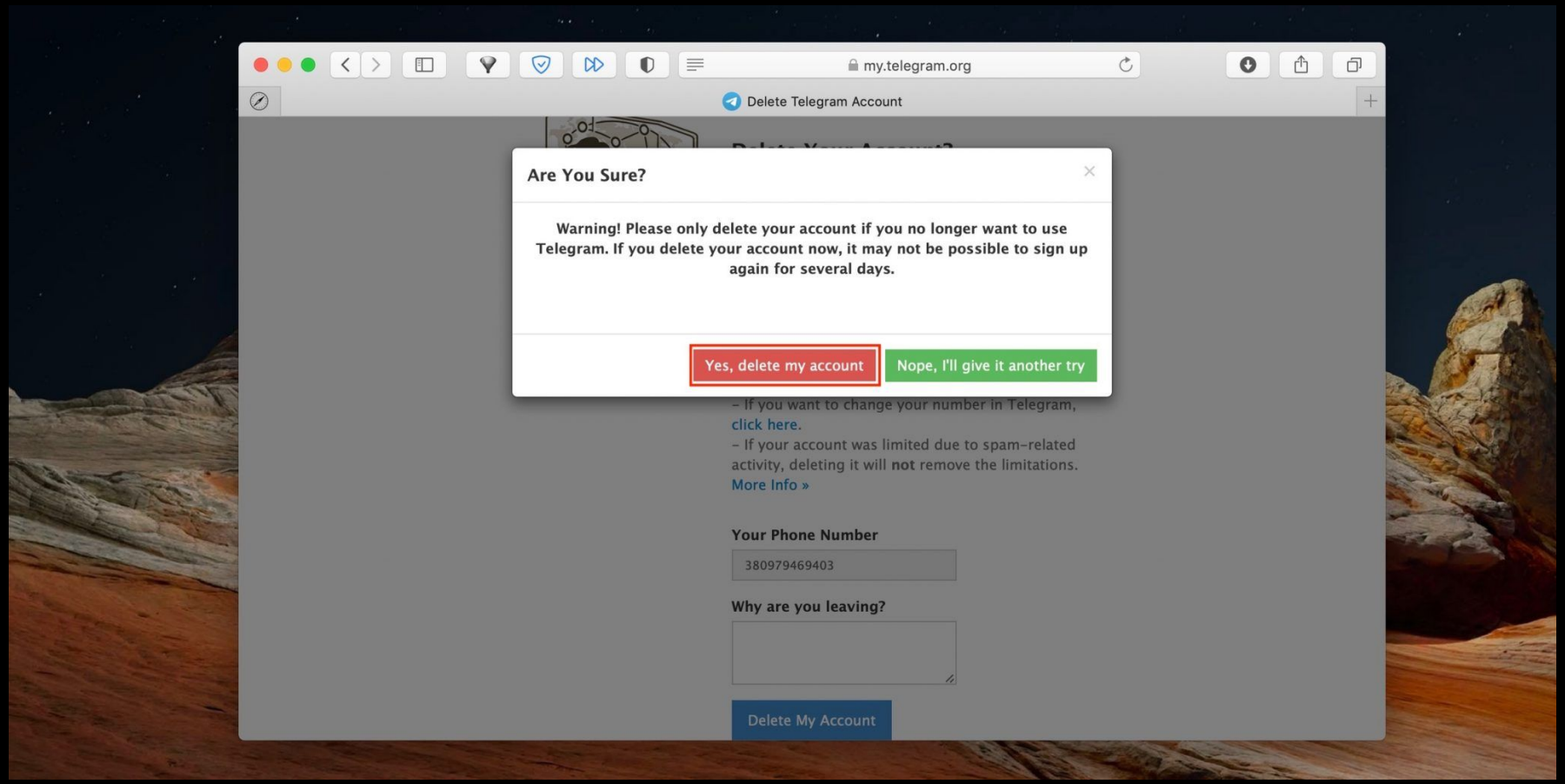
а это лайфхак, позвонить со своего номера по обращению другого клиента, получить доступ к его счетам и напиздеть денях.

4 Ответить ···

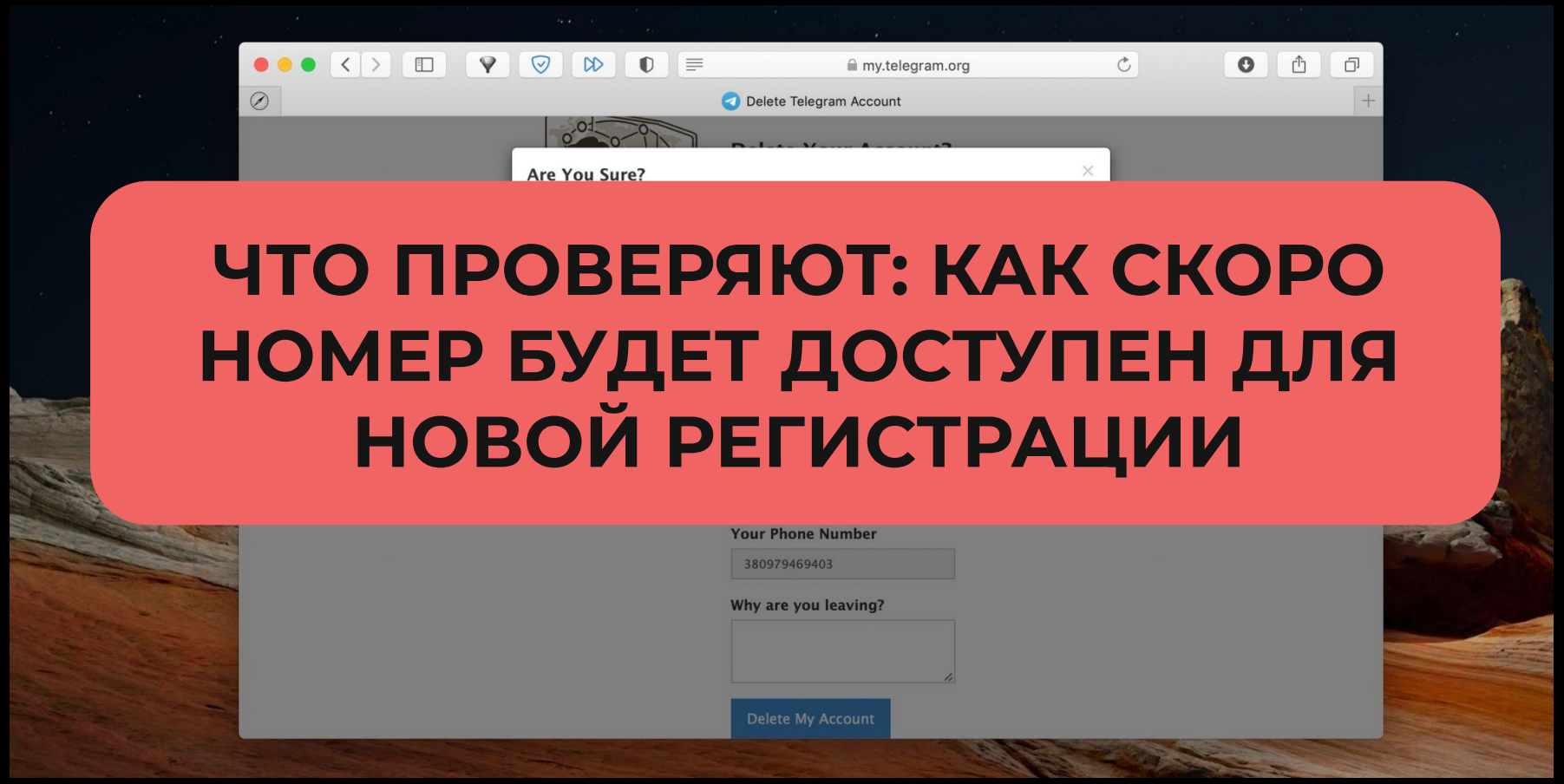
УДАЛЕНИЕ ПД (ПРОВЕРКА САНИТАЙЗЕРА)

1. Проверяется ли на дубли информация обо мне?
2. Если да, то по каким полям?
3. Что происходит после требования их удалить?
4. Есть ли санитарный период? Насколько большой?

УДАЛЕНИЕ ПД (ПРОВЕРКА САНИТАЙЗЕРА)



УДАЛЕНИЕ ПД (ПРОВЕРКА САНИТАЙЗЕРА)



ЧТО ПРОВЕРЯЮТ: КАК СКОРО НОМЕР БУДЕТ ДОСТУПЕН ДЛЯ НОВОЙ РЕГИСТРАЦИИ

поговорим про антифрод

САМОЕ СЛАБОЕ МЕСТО В СИСТЕМЕ – ЛЮДИ

КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

Контент-менеджеры

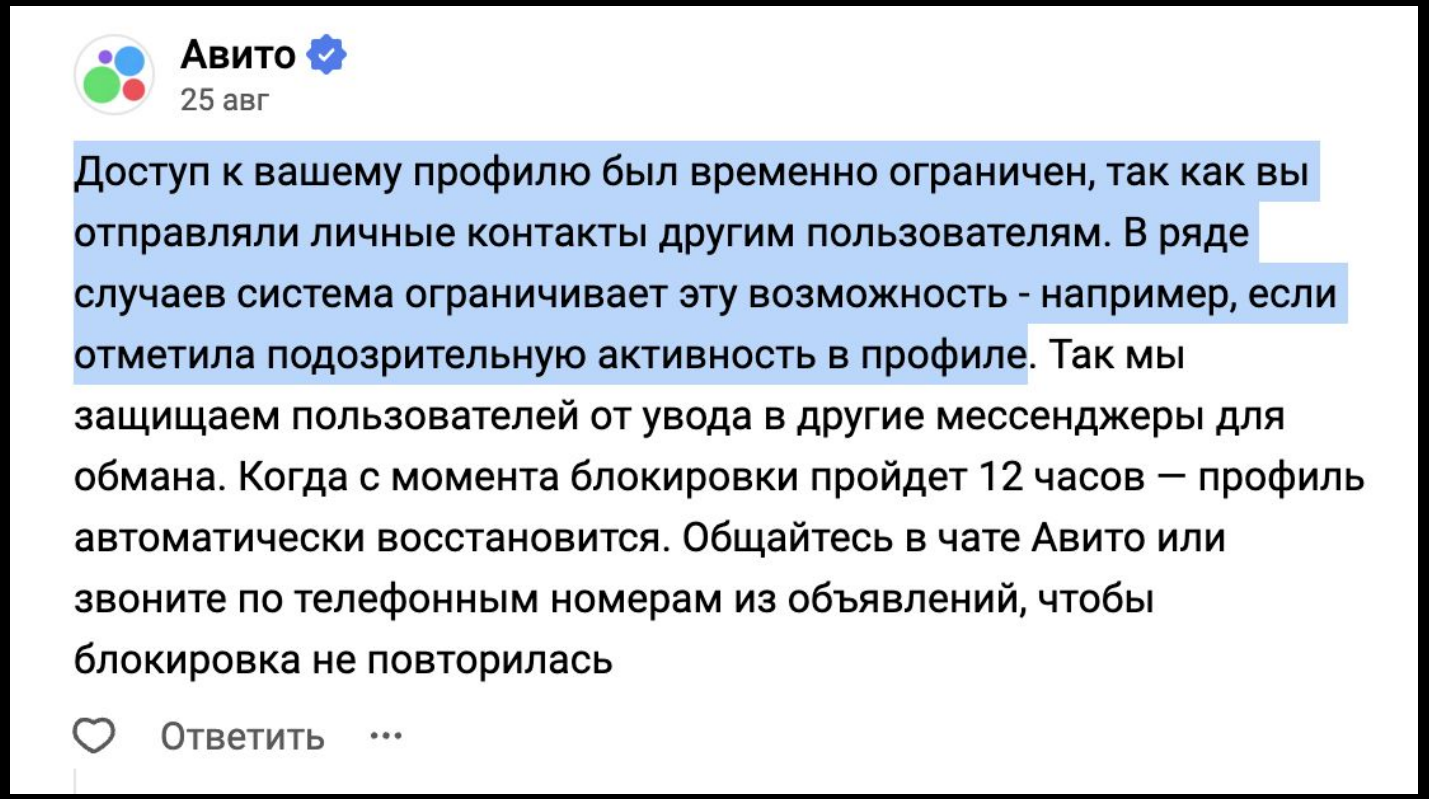
1. Необходимость раскрывать информацию
2. Неправильная отработка негатива в СМИ
3. Добыча информации через фейкового журналиста

КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

Контент-менеджеры

КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

Контент-менеджеры



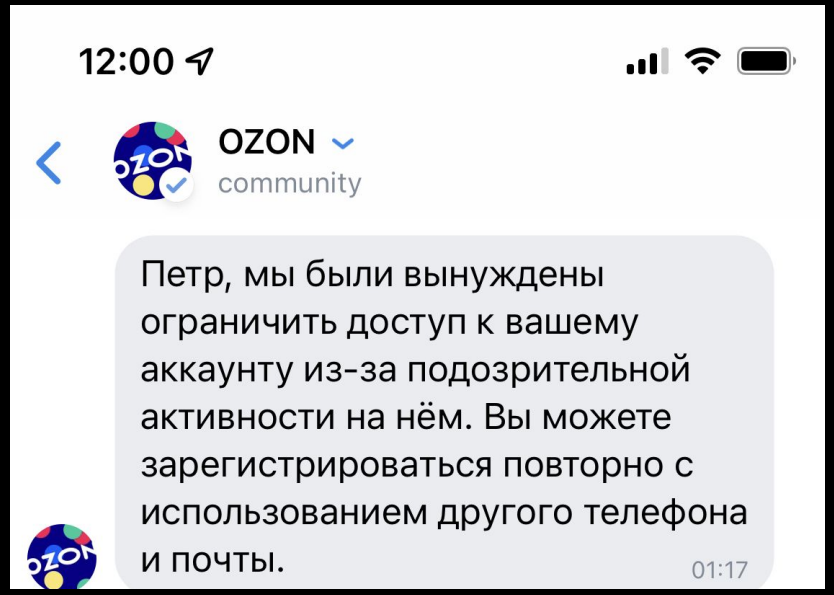
КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

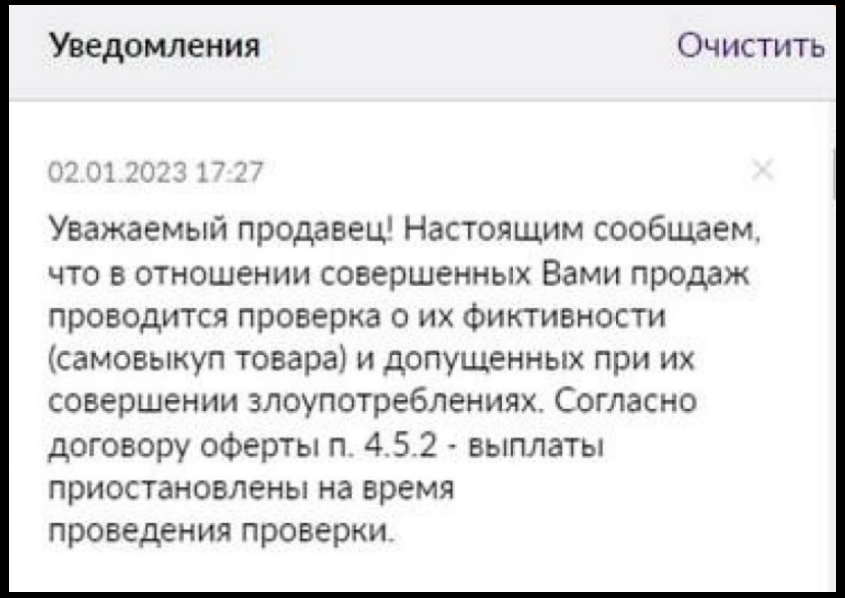
Служба поддержки

1. Зона ответственности / зона влияния
2. Доступ к данным
3. И в целом любая уязвимость в регламентах

КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

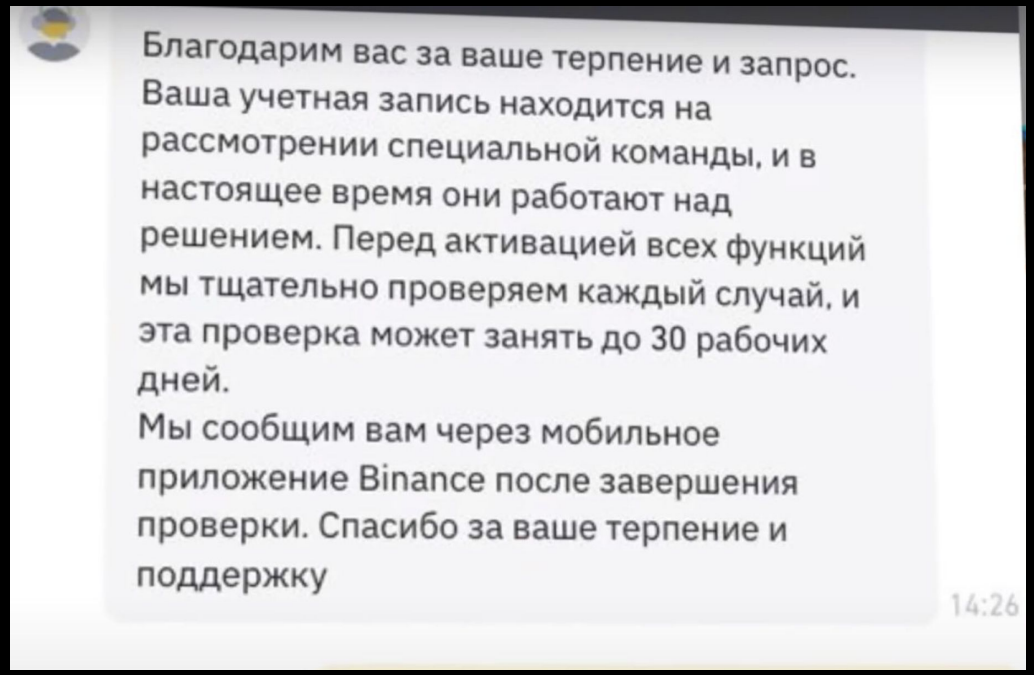
Служба поддержки





КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

Служба поддержки



КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

Персональные менеджеры

1. Торговля за условия
2. Подключение непроверенного сотрудника
3. Иммунитет к антифрод-защите

КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

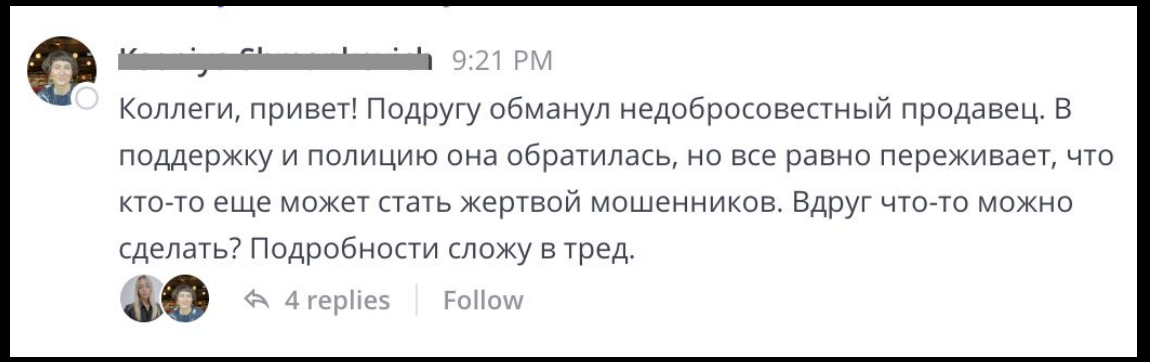
Сотрудники компании

1. Обращение по дружбе
2. Социальная инженерия
3. Продвижение “своих” клиентов

КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

Сотрудники компании

1. Обращение по дружбе
2. Социальная инженерия
3. Продвижение “своих” клиентов



КТО ВНУТРИ МОЖЕТ РАССКАЗАТЬ ЧУВСТВИТЕЛЬНУЮ ИНФОРМАЦИЮ

Спикеры
на конференциях

поговорим, что делать

МЕРЫ ПРОТИВОДЕЙСТВИЯ

МЕРЫ ПРОТИВОДЕЙСТВИЯ

01.

Валидация регламентов

02.

Контроль уровней доступа / NDA

03.

Корректная отработка инцидентов

04.

Менеджеры по безопасности в других департаментах

05.

Единая система обелений

06.

Развитие собственной антифрод-системы

Вопросы?

evnikerina@avito.ru

katyaturing

КАТЕРИНА
НИКЕРИНА