

Аренда аккаунтов в соцсетях

Ответственность



Почему злоумышленники арендуют аккаунты?

После введения ограничений по количеству SIM-карт на человека в России, злоумышленникам стало сложнее самостоятельно регистрировать аккаунты.

Помимо этого, большинство мошеннических аккаунтов блокируется, поэтому они ищут новые способы совершения преступлений.

Арендованные аккаунты могут использоваться для:

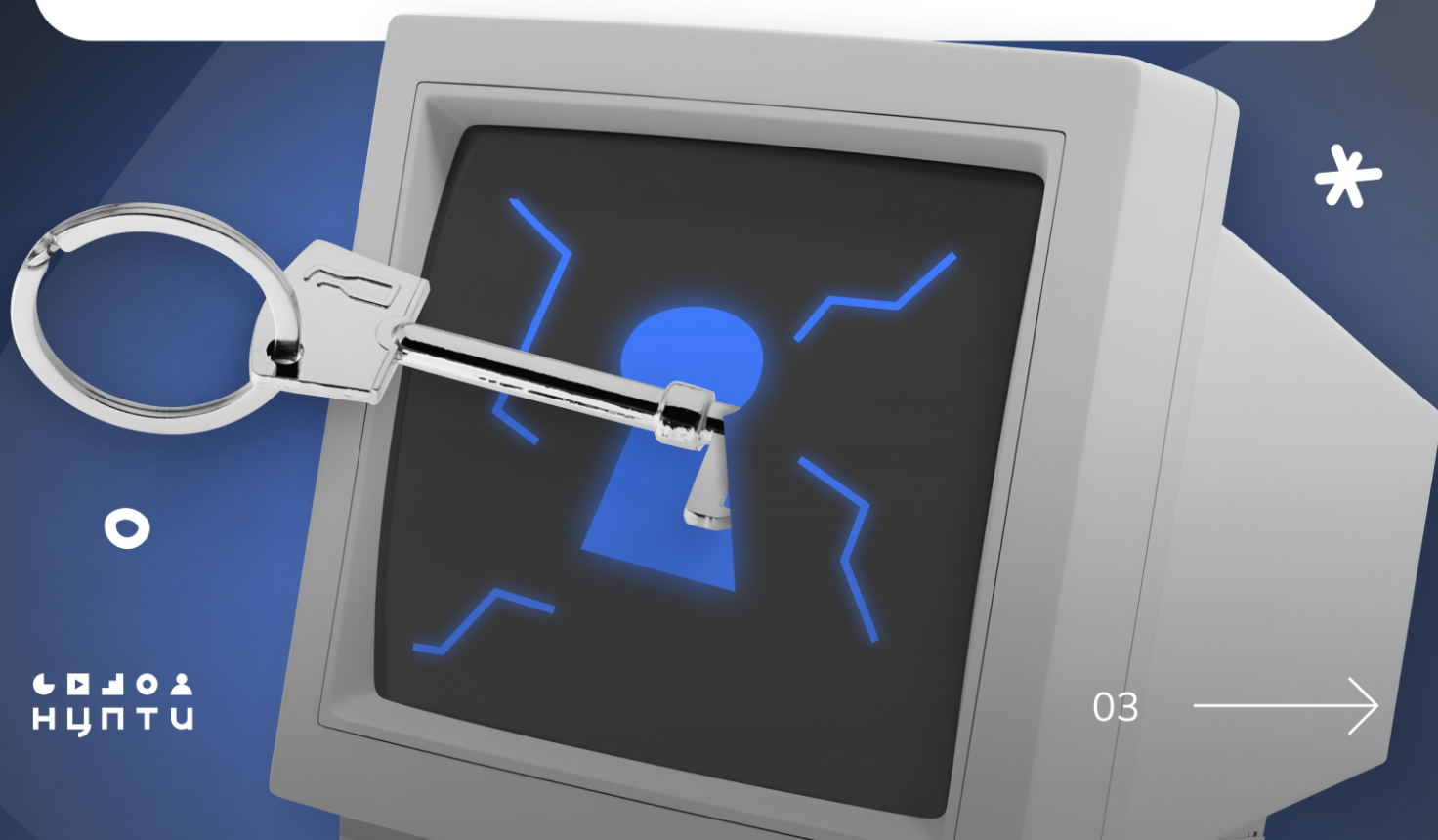
- Организации особо тяжких преступлений
- Работы мошеннических колл-центров
- Рассылки фишинговых ссылок
- Оформления кредитов
- Вымогательства денег
- Вербовки в запрещенные организации
- Кражи личных данных



Предложения с такой «подработкой» могут появляться почти везде: в мессенджерах, соцсетях, онлайн-играх, блогерских сообществах, на форумах и сайтах с вакансиями.

Легенды для аренды разные: «аккаунт нужен для тестирования нового сервиса», «хочу проверить, как работает реклама», «временно нужен аккаунт для корпоративных закупок» и пр. Жертву пытаются убедить, что это абсолютно легально и безопасно.

Чаще всего схемы направлены на школьников, студентов, людей без стабильного дохода, активных пользователей маркетплейсов. Самый молодой участник, вовлеченный в такую преступную схему, — 10-ти летний мальчик, который предоставил свой аккаунт колл-центру за 1,5 тысячи рублей.



Схемы вовлечения

В ТикТок школьникам через видеоролики предлагают за 10-15 тысяч рублей сдать в аренду аккаунт «крупному рекламному агентству для помощи большому бизнесу». Тех, кто согласился на эту «подработку», переводят в Telegram-бот для введения логина и пароля от учетной записи и последующего получения денег.

По итогу школьники:

- Не получают обещанного вознаграждения
- Нарушают условия сервисов
- Могут быть привлечены к ответственности, если злоумышленники совершили преступление с арендованного аккаунта



Схемы вовлечения

Также злоумышленники ищут новых жертв через Telegram-каналы, где ежедневно публикуют подобные предложения об аренде. Если человек откликнулся, то он передает свой номер телефона и код для входа в мессенджер. Взамен ему обещают почасовую оплату. Чаще всего обещанных денег никто не переводит, а когда мошенники выполняют свои задачи — просто игнорируют жертву и пропадают.

Уже более 100 тысяч подростков вовлечены в схемы аренды Telegram-аккаунтов, которые используются для работы нелегальных колл-центров.



Схемы вовлечения

Даже аккаунты на Авито интересны злоумышленникам. Профили с хорошей репутацией особенно привлекательны, поскольку высокий рейтинг вызывает доверие у аудитории.

Проверенные продавцы могут размещать объявления без ограничений или с минимальной модерацией. А если к арендованному аккаунту еще привязаны карты или кошельки, то деньги за продажи моментально выводятся на счет мошенника.

Аренду аккаунта просят для «осуществления благотворительных сборов», а по итогу размещаются ложные объявления с требованием предоплаты. Полученные деньги выводятся на счета злоумышленников, покупатели жалуются, аккаунт блокируют и владелец остается виновным.

Как защитить себя от вовлечения в преступные схемы?

1. **Никому не передавайте данные для входа в личные аккаунты или SIM-карты**, даже если предложение кажется безобидным или выгодным. По итогу ответственность будет нести владелец аккаунта.
2. **Не верьте предложениям с легким заработком**, особенно, если речь идет об аренде SIM-карты, банковских счетов или личных профилей.
3. **Защитите свои аккаунты**: установите двухфакторную аутентификацию, периодически меняйте пароли и не переходите по подозрительным ссылкам.



Если вы уже сдали аккаунт в аренду:

1. Смените пароль, удалите все связанные устройства, завершите активные сеансы.
2. Сделайте скриншоты всей переписки со злоумышленником, чтобы доказать, что за это время аккаунтом пользовались не вы.
3. Если вам уже перевели деньги за аренду аккаунта, не тратьте деньги и сохраните чеки.
4. Предупредите друзей и родственников, что ваш аккаунт в пользовании злоумышленников.
5. Чтобы проверить, совершал ли арендатор преступные действия с помощью вашего аккаунта, обратитесь в полицию.

Если злоумышленники все-таки совершили преступление, то это не дает гарантии, что с владельца полностью снимут ответственность, но эти пункты обязательно учтут в правоохранительных органах.



Ответственность

С 1 сентября 2025 года официально запрещено передавать свои SIM-карты и абонентские номера третьим лицам, за исключением близких родственников или случаев кратковременного использования без материальной выгоды. За это предусмотрен **административный штраф до 50 тысяч рублей.**

Административная ответственность наступает с 16 лет. Более того, если соучастник не достиг этого возраста, то к ответственности привлекут его родителей.



Ответственность

Также в зависимости от преступления, совершенного по итогу аренды аккаунта, может наступить ответственность по следующим статьям Уголовного Кодекса Российской Федерации:

- Ст. 159 УК РФ «Мошенничество» или 159.3 УК РФ «Мошенничество с использованием электронных средств платежа»
- Ст. 174 УК РФ «Легализация денежных средств»
- Ст. 183 УК РФ «Незаконное использование информации»

По каждой из статей следует наказание: от штрафа и обязательных работ до лишения свободы.



В интернете встречаются схемы вовлечения молодежи в преступления через сдачу в аренду личных аккаунтов и SIM-карт.

На первый взгляд всё может казаться безобидным: просто сдаешь аккаунт на время и получаешь деньги за аренду, однако это может иметь серьезные последствия для молодых людей и их семей. Подробнее — в карточках!

#нцпти_медиабезопасность