

ДРОППЕРЫ: как не стать помощником кибермошенников



Дроппер — это человек, который за вознаграждение предоставляет свои банковские карты, доступ к онлайн-банку или персональные данные для проведения незаконных финансовых операций. Такие действия делают его соучастником преступления, даже если он не осознавал противоправный характер действий.

Как не стать дроппером

- **Не передавайте третьим лицам свои банковские карты, данные для доступа к онлайн-банку, логин, пароль, CVV-код, коды подтверждения.** Даже если вам предлагают вознаграждение.

- **Игнорируйте подозрительные предложения о «лёгком заработке»,** связанных с переводами или обналичиванием денег. Признаки мошенничества: обещание высокого дохода без опыта, отсутствие конкретики в описании обязанностей, требование открыть счёт или оформить кредит «для компании».

- **Не соглашайтесь на просьбы незнакомцев** снять наличные в банкомате, перевести деньги по указанным реквизитам или вернуть случайно полученные средства.

- **Проверяйте получателей платежей** перед отправкой денег.

- **Контролируйте активность на счетах:** регулярно проверяйте выписки и уведомления от банка, чтобы вовремя заметить подозрительные транзакции.

- **Используйте двухфакторную аутентификацию** — это дополнительный уровень защиты от несанкционированного доступа к банковским счетам.

Последствия участия в дропперских схемах

- **Уголовная ответственность.** С 2025 года за передачу банковской карты или её реквизитов грозит штраф до 300 тыс. рублей, принудительные работы или лишение свободы до 3 лет. Организаторы таких схем могут получить до 6 лет лишения свободы и штраф до 1 млн рублей.

- **Блокировка банковских счетов.** Банки имеют право блокировать счета, замеченные в подозрительных операциях.

- **Репутационный ущерб.** Информация о причастности к мошенническим схемам может испортить репутацию.

- **Ухудшение кредитной истории, трудности при трудоустройстве и ограничения на банковские переводы.**

Что делать, если вас пытаются вовлечь в дропперскую схему

- **Откажитесь категорически** от таких предложений.

- **Сохраните переписку или запись разговора** — это может помочь в расследовании.
- **Немедленно обратитесь в банк и полицию.** Заблокируйте карту и дистанционный доступ к счетам, зафиксируйте ситуацию официально.
- **Позвоните на горячую линию Банка России: 8 800 300-30-00** (короткий номер 300 с мобильного).
- **Проверьте, есть ли вы в базе подозреваемых.** На портале «Госуслуги» есть услуга «Получение информации о наличии сведений в базах данных».
- **Важно:** если нарушение совершил несовершеннолетний, за его действия будут отвечать родители или законные представители.

Расскажите близким — пожилые люди и подростки тоже в зоне риска!