

Недетские игры

# ДРОППЕРЫ

ЧЕМ ГРОЗИТ ТАКАЯ  
ПОДРАБОТКА



РОСКОМНАДЗОР

# ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ДРОППЕРОМ?

Не молчите! Сразу обратитесь в полицию и банк. Чем быстрее вы сообщите, тем меньше будут последствия. Нужна юридическая помощь? Мы рядом! Центр правовой помощи гражданам в цифровой среде:

**ВСЕ УСЛУГИ  
БЕСПЛАТНЫ!**

[4people.grfc.ru](https://4people.grfc.ru)



[4people@grfc.ru](mailto:4people@grfc.ru)



+7 (499) 550-80-03



**РОСКОМНАДЗОР**

# КАК НЕ СТАТЬ ДРОППЕРОМ?

Не принимайте предложения о легком заработке, если вас просят открыть банковский счет или перевести деньги для кого-то.



Не давайте никому свои банковские данные или документы.



Будьте осторожны, если вам предлагают работу с деньгами в интернете, особенно если все выглядит слишком легко.



# КТО ПОД ПРИЦЕЛОМ?

Школьники старших классов, студенты, мигранты и другие уязвимые слои населения

В вакансиях мошенники **обещают легкий заработок и удобный график**. Вот несколько примеров:



Открыть несколько банковских счетов и перевести деньги за небольшую комиссию.



Стать администратором «лотереи» и переводить деньги «победителям».



Сдать в аренду свою банковскую карту для тестирования новых финансовых сервисов.

# ЧЕМ ГРОЗИТ СОТРУДНИЧЕСТВО?

## Проблемы с законом



Полиция легко устанавливает дропперов, на чьи имена оформлены карты или счета. Если потерпевший обращается в суд, дропперов могут привлечь к гражданско-правовой ответственности и взыскать похищенные средства. Помимо этого, дропперу может грозить уголовная ответственность за соучастие в преступлении.



Став дроппером, вы не только нарушаете закон, но и подвергаете себя реальным физическим угрозам. Потеряв доступ к деньгам при блокировке карты, мошенники требуют их от дроппера. В ход идут все средства: шантаж, физическое насилие, похищение.

# ЧЕМ ГРОЗИТ СОТРУДНИЧЕСТВО?

## Финансовые потери

Злоумышленники уверяют потенциальных дропперов в безопасности такой «работы». Однако на деле это далеко не так.

Дропперы рискуют попасть в черные списки банков.



Имея личные данные «помощников», мошенники могут оформить на них кредит.



# Сообщай информацию осознанно



- ! Не говори по телефону то, что ты не был бы готов сказать при общении лицом к лицу. Не отвечай на сообщения, руководствуясь эмоциями.
- ! Помни, что все отправленные текстовые сообщения, фотографии и видео могут быть скопированы и распространены, оставаясь в сети практически навсегда.
- ! Никогда не отправляй и не пересылай то, чего бы тебе не хотелось, чтобы увидели все в твоей школе
- ! Всегда спрашивай разрешение перед тем, как сделать фотографию или видео, и перед тем, как переслать какую-либо информацию

# Знай о том, что знают твои приложения



- ! Внимательно изучи все разрешения приложений перед установкой.
- ! Если приложение хочет получить доступ к твоему местоположению, контактам, календарю, камере или сообщениям для публикации в вашем профиле в социальных сетях - подумай, действительно ли приложению нужны такие данные для работы.
- ! Посоветуйся с родителями перед установкой нового приложения.



## Другие полезные советы



**!** Не отвечай на спам-сообщения. Не сообщай в телефонном разговоре незнакомым людям информацию о себе. Используй функцию блокировки телефонных номеров, с которых идёт спам.

**!** Не позволяй телефону становиться преградой для реальных взаимодействий с людьми. Ничто не заменит общение лицом к лицу.

# Позаботься о конфиденциальности



- ! Перед тем, как делиться своим местоположением, убедись в том, что эта информация была доступна только тем, кому ты желаешь её передать.
- ! Информацией о своём местоположении следует делиться только со своей семьёй и с проверенными друзьями.
- ! Не публикуй свой номер телефона и не делись им с теми, кому ты не доверяешь.
- ! Блокируй телефон, когда не пользуешься им. Используй уникальные и надёжные пароли. Делиться этими паролями можно только с родителями.

1

## Обратиться в банк и заблокировать карту

Вам необходимо немедленно **позвонить в банк**, в котором открыт счет (по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка), и **сообщить о списании без вашего согласия денег со счета, а также заблокировать карту.**

Заблокировать карту можно в том числе через мобильное приложение кредитной организации, личный кабинет на официальном сайте банка или в любом отделении финансовой организации.





1

2

## Написать в банк заявление о несогласии с операцией



Обратиться с таким уведомлением необходимо на месте в отделении банка и не позднее **1 дня** с даты получения сообщения от банка о совершенной операции.



Запросите у банка заверенную выписку по счету. Банк рассмотрит ваше уведомление в срок, предусмотренный договором, но не более 30 дней со дня получения уведомления или не более 60 дней в случае трансграничного перевода.

1

2

3

## Условия возврата средств банком

В силу закона банк обязан вернуть списанную со счета сумму в двух случаях:



Клиент не нарушил правила безопасного использования электронного средства платежа (например, банковской карты) и сообщил банку о несанкционированной операции не позднее 1 дня после получения от него уведомления о совершении операции;



Банк совершил перевод на счет получателя, сведения о котором находятся в базе данных Банка России о мошеннических операциях, не уведомив клиента об опасности и не приостановив перевод на два дня.

1

2

3

4

## Написать заявление в полицию

Незамедлительно обратитесь в полицию с заявлением о хищении денежных средств с вашего счета (желательно к заявлению приложить копию договора с банком и выписку по счету). Чем больше людей подадут заявления, тем выше вероятность, что преступников поймают.

1

2

3

4

5

## Банк не возместил деньги, что дальше?

Если банк отказал в возмещении списанных без вашего согласия денежных средств, для защиты ваших прав и законных интересов следует:



Обратиться к финансовому уполномоченному (омбудсмену) для досудебного урегулирования спора: [finombudsman.ru](http://finombudsman.ru), 8 (800) 200-00-10.

Помощь омбудсмана для граждан бесплатна, а принятое им решение обязательно к исполнению финансовой организацией;



Обратиться в суд.



# Мошенники похитили деньги со счета в банке?

Что делать: пошаговая  
инструкция



**РОСКОМНАДЗОР**



Не получается  
справиться  
с ситуацией  
самостоятельно?



**РОСКОМНАДЗОР**

**Если вы или ваши близкие пострадали от неправомерных действий в интернете, обращайтесь в Центр правовой помощи гражданам в цифровой среде:**



заполните форму обратной связи на сайте: [4people.grfc.ru](https://4people.grfc.ru)



напишите на электронную почту: [4people@grfc.ru](mailto:4people@grfc.ru)



позвоните: **+7 (499) 550-80-03**



или приходите на личный прием в Москве, Нижнем Новгороде, Новосибирске или в Санкт-Петербурге.



# Как распознать скам-ресурсы и защитить себя

Комментирует сопредседатель комиссии РОЦИТ по развитию электронной коммерции, заместитель управляющего директора Ozon Алексей Минаев

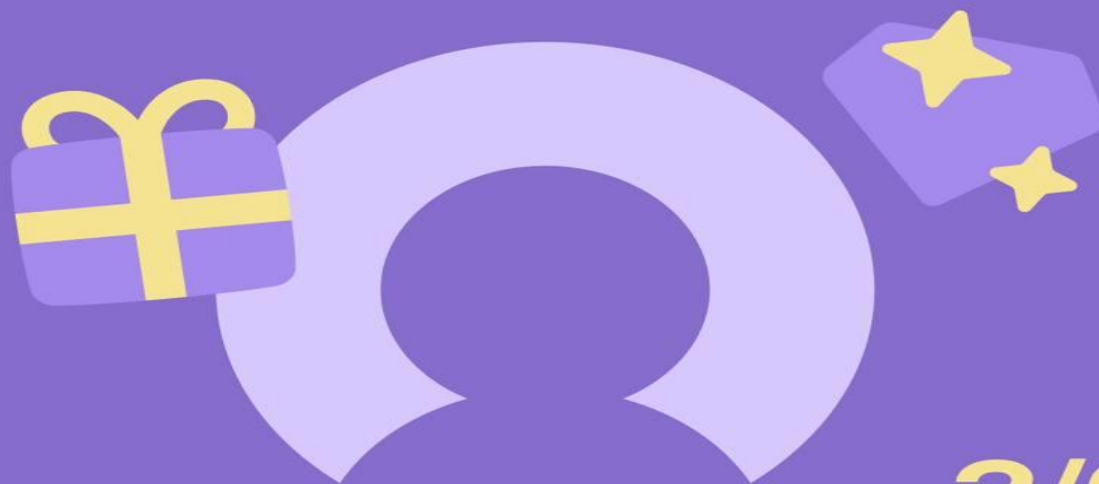


# Отличия официальных ресурсов от скам-сайтов

- \* Скам-сайты часто *маскируются под маркет-плейс* или проводят фейковые розыгрыши на ресурсе, выдающем себя за официальный.
- \* Внешне скам-сайт может копировать настоящий, но он будет отличаться незначительными деталями: *лишней буквой в названии сайта или нестандартной доменной зоной.*
- \* На официальном сайте *вы всегда сможете изменить фильтр и перейти в другие разделы.* На скам-ресурсе чаще всего действия ограничиваются одной страницей.

# Подозрительное предложение

Пользователя должно насторожить *предложение в мессенджере купить товары на Ozon со скидкой* или *сообщение от незнакомого человека с розыгрышем призов и ссылкой* — если перейти по ней, существует большая вероятность попасть на поддельный сайт.



# Ссылки от незнакомцев

- \* Не переходите по ссылкам от незнакомых людей в мессенджерах или почте, а также всегда обращайтесь внимание на адрес отправителя.
- \* Маркетплейс *не устраивает закрытых распродаж* или розыгрыши скидок, не отправляет *ссылки на оплату товаров в личные сообщения*.
- \* Также остерегайтесь *предложений о работе с чрезмерно высоким доходом* – скорее всего, пишут мошенники.

# Адрес сайта

Прежде чем ввести в какую-либо форму данные своей банковской карты — **изучите адрес сайта, поищите его в браузере и проверьте, когда он был создан.**

Можно совершать покупки безопасно через **официальное приложение**, которое вы скачали в магазине мобильных приложений.



<http://sbembank.ru>

# Персональные данные

Не передавайте свои персональные данные незнакомым людям, включая **адрес, номер телефона, пароли, одноразовые коды и любую другую личную информацию**, – даже если собеседник представляется специалистом службы поддержки или продавцом маркетплейса.





# Служба поддержки

Если подозреваете, что столкнулись с мошенническим ресурсом – **напишите в службу поддержки маркетплейса** в чате приложения или на сайте, специалисты помогут разобраться в ситуации.



# Сомнительные предложения об удаленной работе в ИТ

*Злоумышленники начали размещать в интернете от имени российских ИТ-компаний поддельные предложения об удаленной работе.*



Большая часть подобных предложений публикуется в профильных Telegram-каналах с вакансиями.

Если пользователя заинтересовало подобное приложение, мошенники предлагают ему перейти по ссылке, чтобы заполнить Google-форму. В ней он оставляет свои контактные данные.

## Надежный пароль и двухфакторная аутентификация

Важно придумать *надежный пароль* и по возможности *включить двухфакторную аутентификацию* для входа в личный кабинет на маркетплейсах.

Также *не стоит привязывать к профилю основную банковскую карту*. Лучше привязать ту, на которую будете переводить нужную сумму для покупки.

# Угрозы «серых» SIM-карт и VPN-сервисов



Дело в том, что *«серые» SIM-карты могут быть зарегистрированы на подставное физическое или юридическое лицо, то есть на мошенников.*

Что касается *VPN-сервисов, из-за них может произойти утечка персональных данных в открытый доступ.* Либо разработчик VPN-сервиса передаст ваши данные третьим лицам, среди которых могут оказаться злоумышленники.