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

4people@grfc.ru

+7 (499) 550-80-03

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

4people@grfc.ru

+7 (499) 550-80-03

РОСКОМНАДЗОР

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.

РОСКОМНАДЗОР

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.

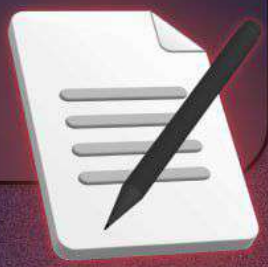
РОСКОМНАДЗОР

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.

РОСКОМНАДЗОР

Сообщай информацию осознанно

Белый Интернет

❗ 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

Белый Интернет

❗ 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.

Знай о том, что знают твои приложения

Белый Интернет

❗ 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

Белый Интернет

❗ 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.

Белый Интернет

Использование смартфона: советы для детей

Позаботься о конфиденциальности

Белый Интернет

❗ 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 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.

РОСКОМНАДЗОР

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.

РОСКОМНАДЗОР

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.**

РОСКОМНАДЗОР

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, 8 (800) 200-00-10. Помощь омбудсмена для граждан бесплатна, а принятое им решение обязательно к исполнению финансовой организацией;
- **Обратиться в суд.**

РОСКОМНАДЗОР

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.**

РОСКОМНАДЗОР

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
- напишите на электронную почту: 4people@grfc.ru
- позвоните: +7 (499) 550-80-03
- или приходите на личный прием в Москве, Нижнем Новгороде, Новосибирске или в Санкт-Петербурге.

РОСКОМНАДЗОР

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

Как распознать скам-ресурсы и защитить себя

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

РОЦИТ

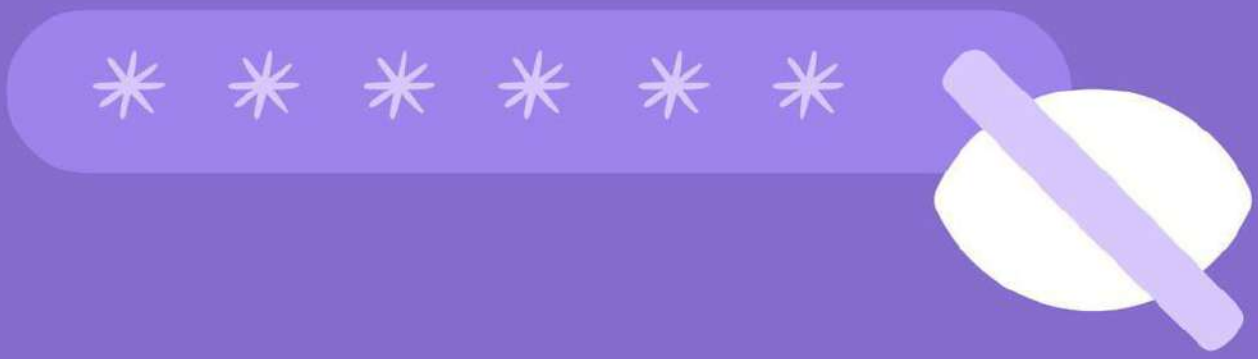
Подозрительное предложение

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.

РОЦИТ

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.



РОЦИТ

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.

РОЦИТ

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.

Ссылки от незнакомцев

- Не переходите по ссылкам от незнакомых людей в мессенджерах или почте, а также всегда обращайте 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.

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.

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.

РОЦИТ

Несуществующая «Единая медицинская служба»

Мошенники начали представляться сотрудниками «Единой медицинской службы». Однако такой организации не существует.

Злоумышленники звонят потенциальной жертве, чтобы поинтересоваться у нее, когда она проходила флюорографию. Если человек отвечает, что обследование он прошел в 2024 году, аферисты сообщают ему, что в системе организации произошел сбой, поэтому в ее базе остались результаты только за 2022 год. В связи с этим мошенники просят человека продиктовать СНИЛС или код из SMS.

Цель таких манипуляций - получить доступ к аккаунту пользователя на портале «Госуслуги».

Угрозы «серых» SIM-карт и VPN-сервисов

Эксперты РОЦИТ напоминают:

чтобы обезопасить свои персональные данные и деньги, ***не стоит использовать «серые» SIM-карты и VPN-сервисы*** для совершения покупок, входа в банковские приложения, на портал «Госуслуги» и иные ресурсы, где ***содержится ваша чувствительная информация.***

РОЦИТ

Сомнительные предложения об удаленной работе в ИТ

Бывает, что аферисты предлагают человеку сразу же связаться с HR-менеджером, чтобы пройти собеседование.

Затем, когда оно успешно пройдено, с человеком уже связывается якобы сотрудник бухгалтерии ИТ-компании. Он предлагает будущему работнику привязать телефонный номер корпоративной SIM-карты к личному кабинету банка, чтобы тот сразу начал получать зарплату с первого дня трудовой деятельности.

Если человек это делает, мошенники незамедлительно крадут его деньги с банковского счета.

МОШЕННИКИ НЕ ДРЕМЛЮТ: НОВЫЕ СХЕМЫ ОТ ЗЛОУМЫШЛЕННИКОВ

Комментируют эксперты РОЦИТ

РОЦИТ

Простые пароли для входа в личный кабинет на маркетплейсах

Мошенники создают на маркетплейсах фальшивые аккаунты продавцов, чтобы красть деньги у людей.

Для этого киберпреступники взламывают личные кабинеты пользователей на маркет-плейсах, чтобы оформить заказы у таких продавцов.

Таким образом, все деньги с банковской карты, которая привязана к взломанному профилю, попадают в руки мошенников.

Не храните пин-код вместе с банковской картой и не записывайте его на «пластик»

Если у вас несколько банковских карт, для каждой установите свой пин-код. Не устанавливайте простые числовые комбинации вроде 1234, 0000, 1111. Злоумышленники могут легко их разгадать.

РОСКОМНАДЗОР | Банк России

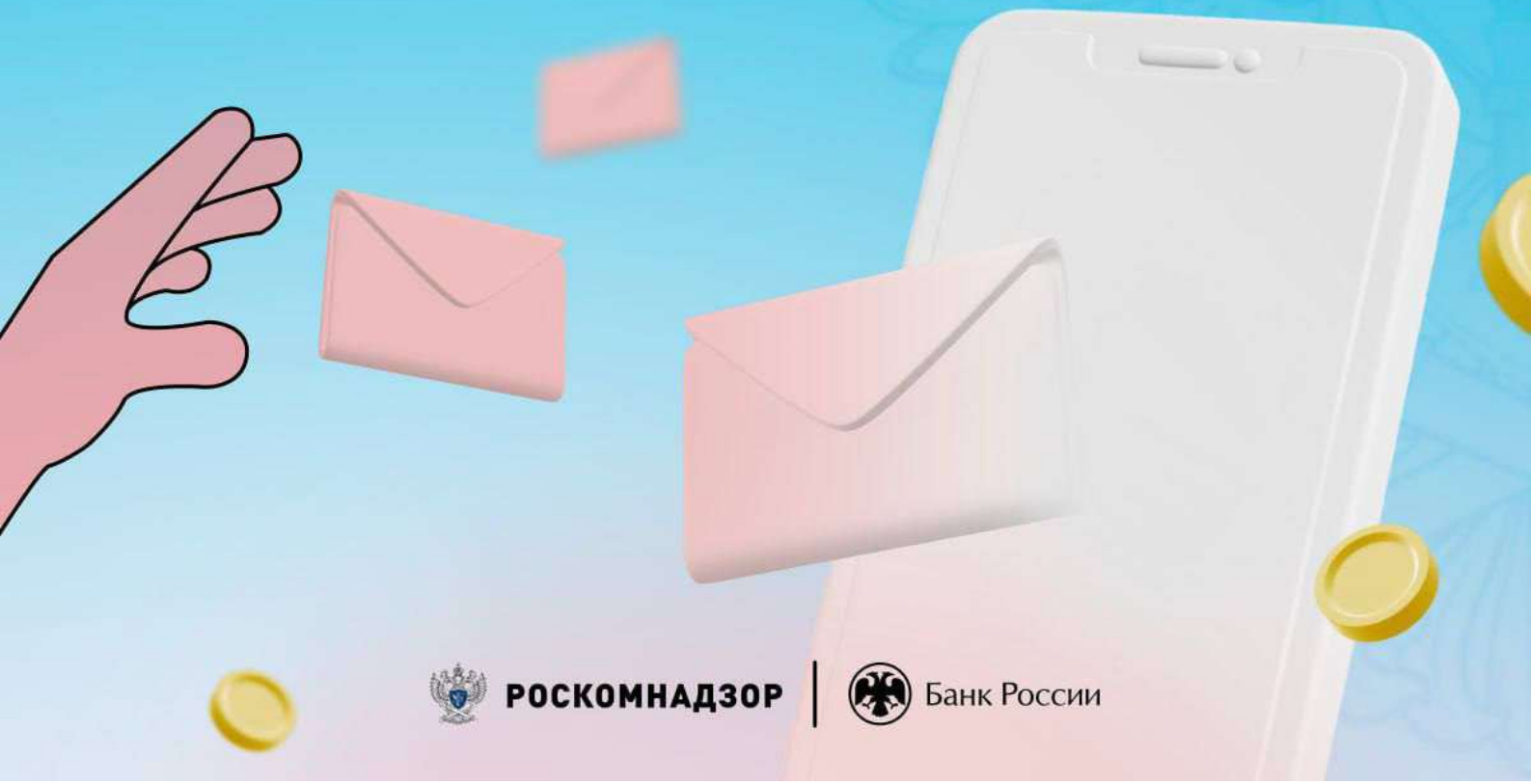
Не привязывайте банковские карты к сайтам и сервисам

Если сайт взломают или произойдет утечка данных, то платежные реквизиты окажутся в руках мошенников.

РОСКОМНАДЗОР | Банк России

Не пересылайте в мессенджерах и соцсетях фото банковских карт и документов

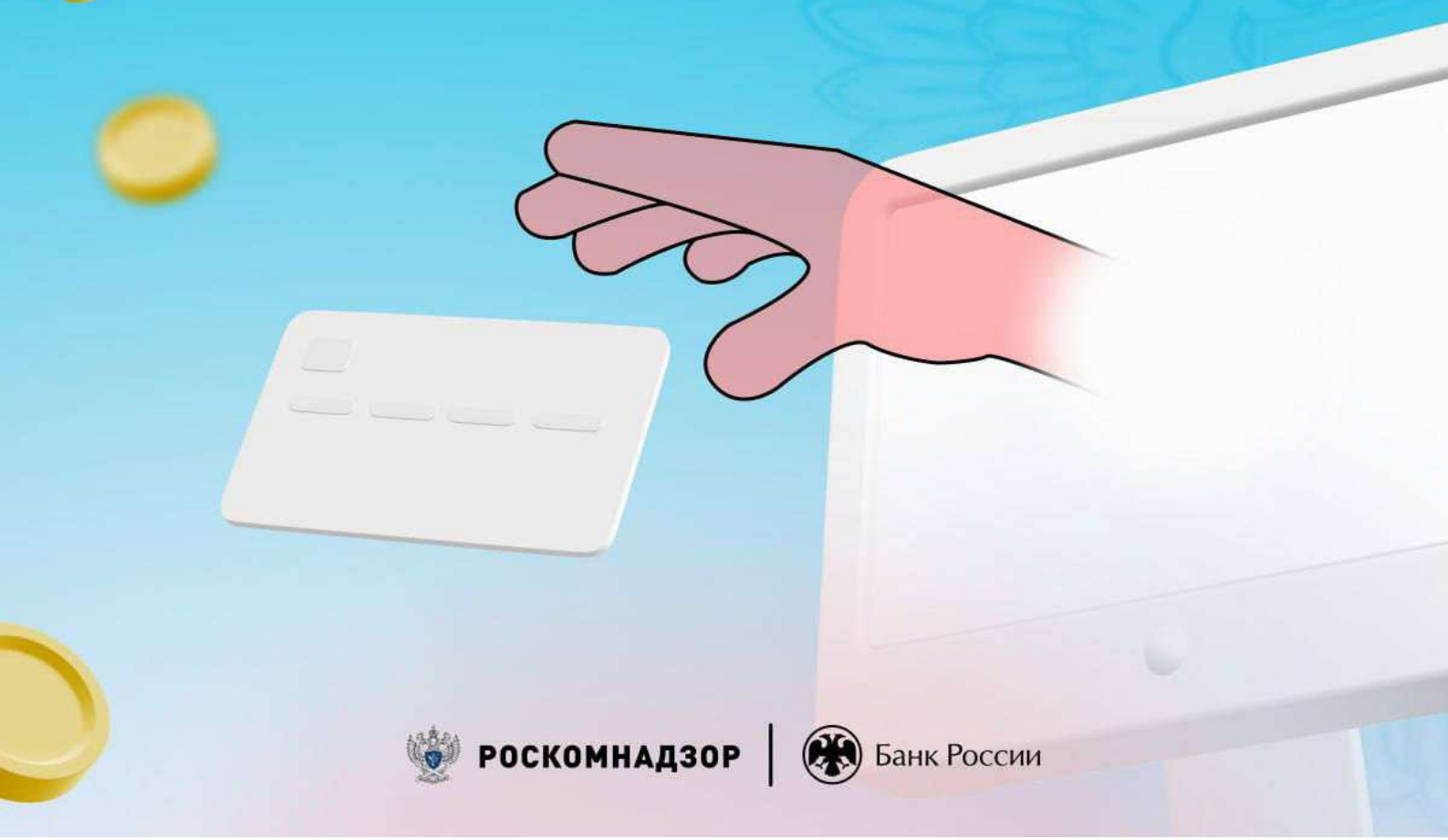
Если личные и финансовые данные окажутся в руках киберпреступников, они могут воспользоваться конфиденциальной информацией в преступных целях.



РОСКОМНАДЗОР | Банк России

Не используйте зарплатную карту для онлайн-покупок

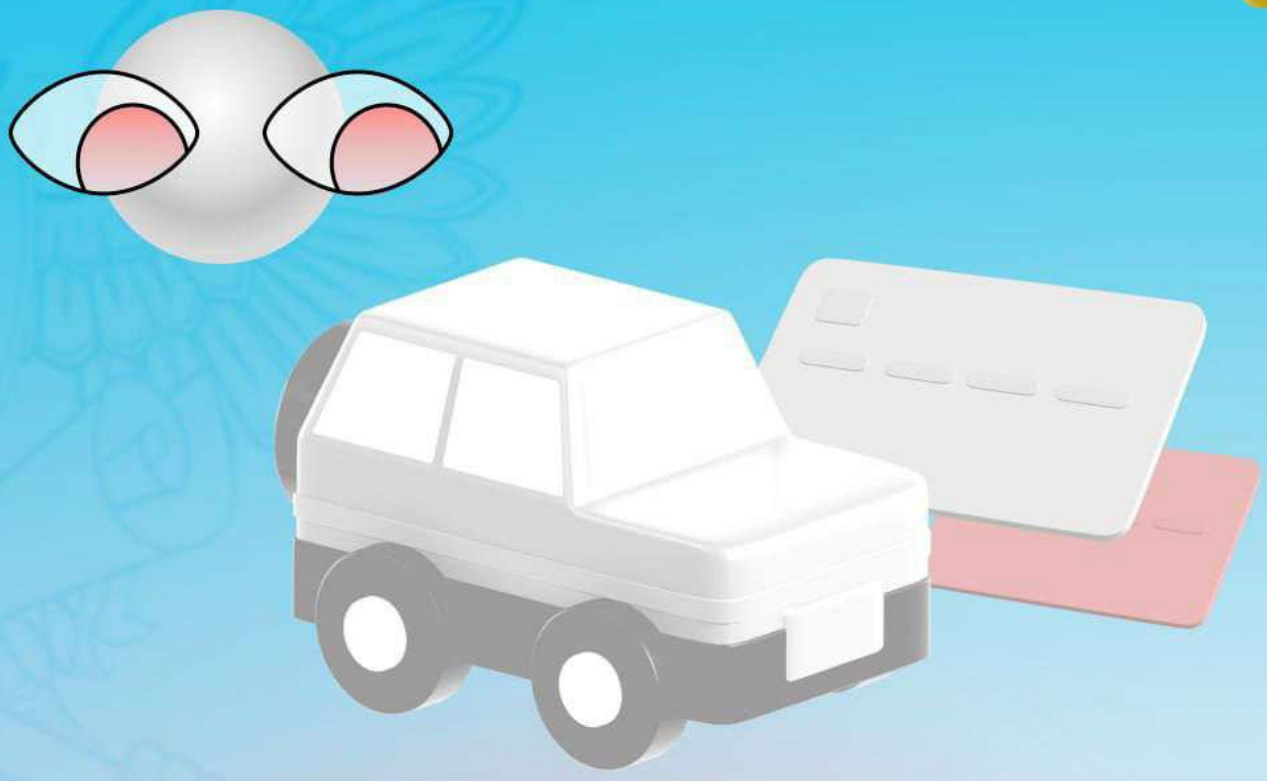
Для онлайн-шопинга заведите отдельную дебетовую карту и пополняйте ее ровно на ту сумму, которая нужна для оплаты.



РОСКОМНАДЗОР | Банк России

Не храните банковские карты, как и документы, в машине

На эти ценные вещи автомобильные воры обращают внимание в первую очередь.



РОСКОМНАДЗОР | Банк России