КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

Памятка Следственного департамента МВД России

МОЛЧАНИЕ - ЗОЛОТО!

Не разговаривайте с незнакомыми людьми, положите трубку.

Если звонят и представляются сотрудниками МВД России, других правоохранительных органов, банков или сообщают, что родственник попал в ДТП, или используют другие уловки, прервите разговор. Перезвоните на номера, указанные на официальных сайтах организаций, посоветуйтесь с родственниками.

Используйте приложения по блокировке спам-звонков или подключите подобную опцию через операторов сотовой связи.

Не выкладывайте и не сохраняйте в сети Интернет персональные данные.

Ни при каких обстоятельствах не передавайте посторонним лицам сведения о своих счетах и банковских картах, вкладах, не совершайте с ними действий, о которых просят незнакомые лица по телефону.

Запомните!

Пока вы соблюдаете требования договора банковского обслуживания, ответственность за ваши денежные средства несёт кредитно-финансовая организация. Как только вы нарушили условия договора - ответственность уже лежит на вас.

РАПСИ Российское агентство правовой и судебной информации

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА БАНКА»:

Прекратите разговор.
Самостоятельно позвоните в банк.
(чаще всего номер телефона указан на банковской карточке)

1

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА БАНКА»:

Не надо сразу выполнять рекомендации, которые дает лицо, представляющееся сотрудником банка.

(вас торопят? задумайтесь!!!)

3

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА БАНКА»:

Не сообщайте свои персональные данные, а также:

* коды из смс;
* трёхзначный код на оборотной стороне карты (CVV/CVC);
* PIN-код;
* пароли/логины к банковскому приложению и онлайн-банку;
* кодовое слово.

2

ВАЖНО ЗНАТЬ:

Настоящий сотрудник банка обладает всеми необходимыми ему сведениями о вас и ваших счетах.

Никаких „безопасных счетов”, о которых говорят лица, представляющиеся сотрудниками банка, не существует.

Для того, чтобы „обезопасить средства” - глупо брать кредиты!

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ»:

Позвоните в полицию и сообщите о странном звонке.

2

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ»:

В первую очередь, уточните полные данные лица, представляющегося сотрудником „правоохранительных органов”, а также причину звонка.

Прекратите разговор.

1

ВАЖНО ЗНАТЬ:

Настоящие сотрудники правоохранительных органов не привлекают граждан к содействию путем телефонных звонков или по видеосвязи.

3

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

КЕМ ПРЕДСТАВЛЯЮТСЯ МОШЕННИКИ

ЦЕНТРАЛЬНЫЙ БАНК

СБЕРБАНК

СОТРУДНИКАМИ БАНКА

МВД

ПРОКУРАТУРА

ФСБ

ФСИН

ПОЛИЦИЯ

СЛЕДСТВЕННЫЙ КОМИТЕТ

СОТРУДНИКАМИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

!!! ВНИМАНИЕ МОШЕННИКИ !!!

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

НЕ ОТКРЫВАЙТЕ ДВЕРЬ
незнакомым людям,
даже если они представляются
работниками социальных,
газовых, электроснабжающих служб,
полиции, поликлиники, ЖКХ и т.д.
Перезвоните и уточните,
направляли ли к Вам
этого специалиста.

НЕЗНАКОМЕЦ ПРЕДСТАВЛЯЕТСЯ СОЦИАЛЬНЫМ РАБОТНИКОМ
и сообщает о надбавке к пенсии,
перерасчете квартплаты, премии
ветеранам, срочном обмене денег
на дому, якобы
«только для пенсионеров».
**НЕ ВЕРЬТЕ –
ЭТО МОШЕННИЧЕСТВО!**

НЕ ДОВЕРЯЙТЕ,
если Вам звонят и сообщают,
что Ваш родственник
или знакомый попал в аварию,
в больницу или
совершил ДТП, и теперь за него
нужно внести залог, штраф,
взятку – в общем откупиться.
ЭТО ОБМАН!

**БУДЬТЕ БДИТЕЛЬНЫ,
НЕ ДОВЕРЯЙТЕ
НЕЗНАКОМЫМ ЛЮДЯМ!**
Если Вас встречают на улице
и предлагают избавить от порчи,
просят для проведения ритуала
передать им на время деньги
или ценности,
ЭТО МОШЕННИКИ!

ПОЛИЦИЯ ИНФОРМИРУЕТ!
Мошенники находят своих жертв
через интернет объявления
о продаже или покупке товаров.
Просят сказать им данные
банковской карты, якобы
для предоплаты. Не называйте
незнакомцам данные своих
банковских карт и
**НИКОМУ НЕ СООБЩАЙТЕ
СМС-КОДЫ, ПРИХОДЯЩИЕ
НА ВАШ ТЕЛЕФОН!**

БУДЬТЕ БДИТЕЛЬНЫ!
Злоумышленники звонят
на мобильные телефоны и
сообщают о блокировке карты,
списании денежных средств,
сомнительных операциях!
**НЕ ПЕРЕЗВАНИВАЙТЕ
ПО УКАЗАННОМУ НОМЕРУ,
НЕ СООБЩАЙТЕ ДАННЫЕ
СВОИХ КАРТ, ТРЕХЗНАЧНЫЙ
КОД НА ОБОРОТНОЙ
СТОРОНЕ КАРТЫ!**
Узнать о всех операциях Вы
можете позвонив по номеру
телефона, указанному на ВАШЕЙ
банковской карте, придя
в банк лично, а также проверив
баланс через банкомат
или с помощью онлайн-банка.

**БУДЬТЕ БДИТЕЛЬНЫ И
НЕ ПОДДАВАЙТЕСЬ
НА УЛОВКИ МОШЕННИКОВ!**

По всем перечисленным фактам и
при подозрении на мошенничество обращайтесь
в ПОЛИЦИЮ по круглосуточным номерам

02, 112

РОСКОМНАДЗОР

Осторожно, мошенники

Раскрываем популярные схемы злоумышленников

Сообщение от босса в Telegram

Злоумышленники представляются высшими руководителями организаций и их заместителями. Для этих целей используют **ложные аккаунты в Telegram**.

Мошенники сообщают об утечке персональных данных в организации и просят оказать содействие **«следователям»**.

Дальше полицейские сообщают о мошеннических кредитах, которые оформили на имя человека, обещают разобраться в вопросе и **выманивают деньги**.

РОСКОМНАДЗОР

Звонок от оператора сотовой связи

Схема 1

Заканчивается срок действия договора на сотовую связь. **Номер** будет **заблокирован**.

Схема 2

От имени абонента подали заявку на **перенесение номера** к другому оператору (услуга MNP).

Чтобы избежать «неприятностей», продиктуйте **СМС-код**.

С помощью кода преступники получают доступ к номеру жертвы, а следовательно, к **личному кабинету** банков, Госуслуг и других сервисов.

Помните, что договор с оператором связи бессрочный! При всех подозрительных звонках свяжитесь с вашей компанией по официальным каналам.

РОСКОМНАДЗОР

Звонок из банка

Мошенники **звонят и сбрасывают** звонок в ожидании того, что им перезвонят.

Если это происходит, звонящий слышит **музыку** из рекламного ролика банка.

Дальше стандартная схема: убеждают назвать **код из СМС** или сообщить **логин и пароль** для входа в учетную запись онлайн-банка. Мошенники получают доступ к счету клиента и выводят с него деньги.

РОСКОМНАДЗОР

Звонок от сотрудника силовых органов

«Вам **грозит** до 20 лет тюрьмы!»
С такой фразы начинается разговор.

«Сотрудник» органов заявляет, что кто-то украл ваши данные и сделал перевод для помощи иностранному государству в деятельности против России. А это квалифицируется как **госизмена**.

Чтобы вычислить «предателя», нужно **перевести средства** на некий счет. Иногда и этого мало. Злоумышленники начинают шантаж и втягивают человека в противоправные действия.

РОСКОМНАДЗОР

Звонок от сотрудника Госуслуг

Мошенники сообщают, что на ваше имя пришло **электронное письмо**.

Чтобы оно отобразилось в личном кабинете на «Госуслугах», нужно назвать **код из СМС**.

Злоумышленники получают **доступ к аккаунту**. Могут сменить пароль, запросить кредитную историю, получить справку о доходах, информацию о транспортных средствах или оформить займ.

РОСКОМНАДЗОР

Звонок из ЦБ

Мошенники предлагают **проверить подлинность** обновленной пятитысячной купюры.

Предлагают установить на телефон **приложение** «Банкноты Банка России».

Вместе с приложением пользователи скачивают **вредоносную программу**.

РОСКОМНАДЗОР

Звонок из пенсионного фонда

Легенда: подтвердите **списание** всех накопленных средств/вам **не начислили** доплаты/**выплатили** слишком много.

К пенсионерам обращаются по имени и отчеству, втираются в доверие и начинают **запугивать**.

Цель: получить **доступ к личному кабинету**, уговорить перевести деньги на другую банковскую карту или установить предлагаемый номер мобильного телефона в качестве доверительного, что позволит аферистам войти в мобильный банк пенсионера.

ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

Мама, я попал в аварию!

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

ВИРУС В ТЕЛЕФОНЕ

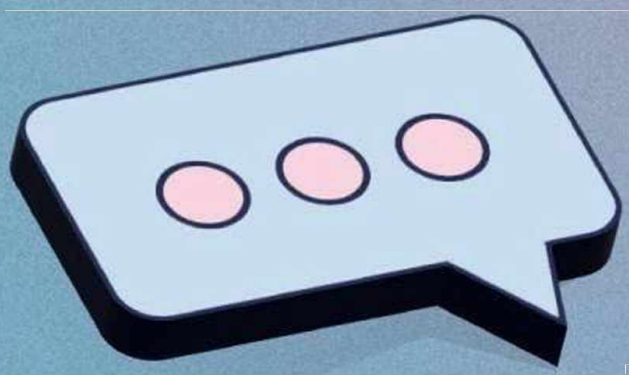
Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.

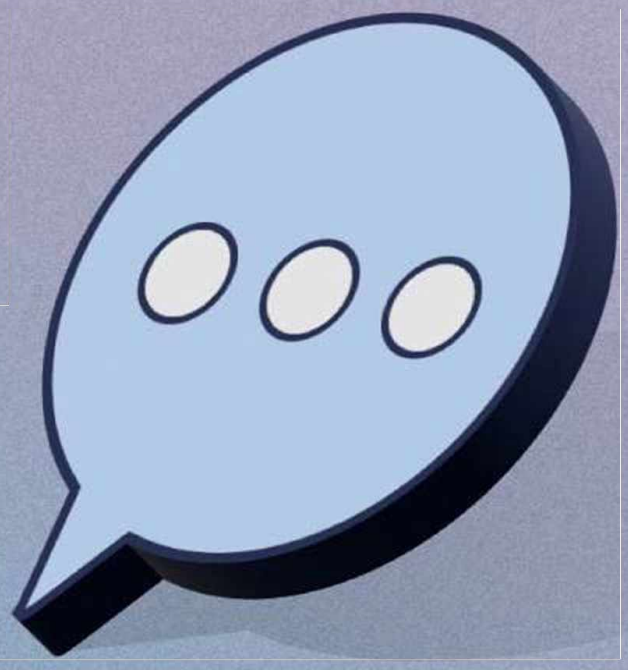
Банк России

Финансовая культура

Как распознать мошенника?

Финансовые аферисты постоянно меняют сценарии обмана. Однако есть фразы, которые выдают преступников. Мы собрали часто используемые.



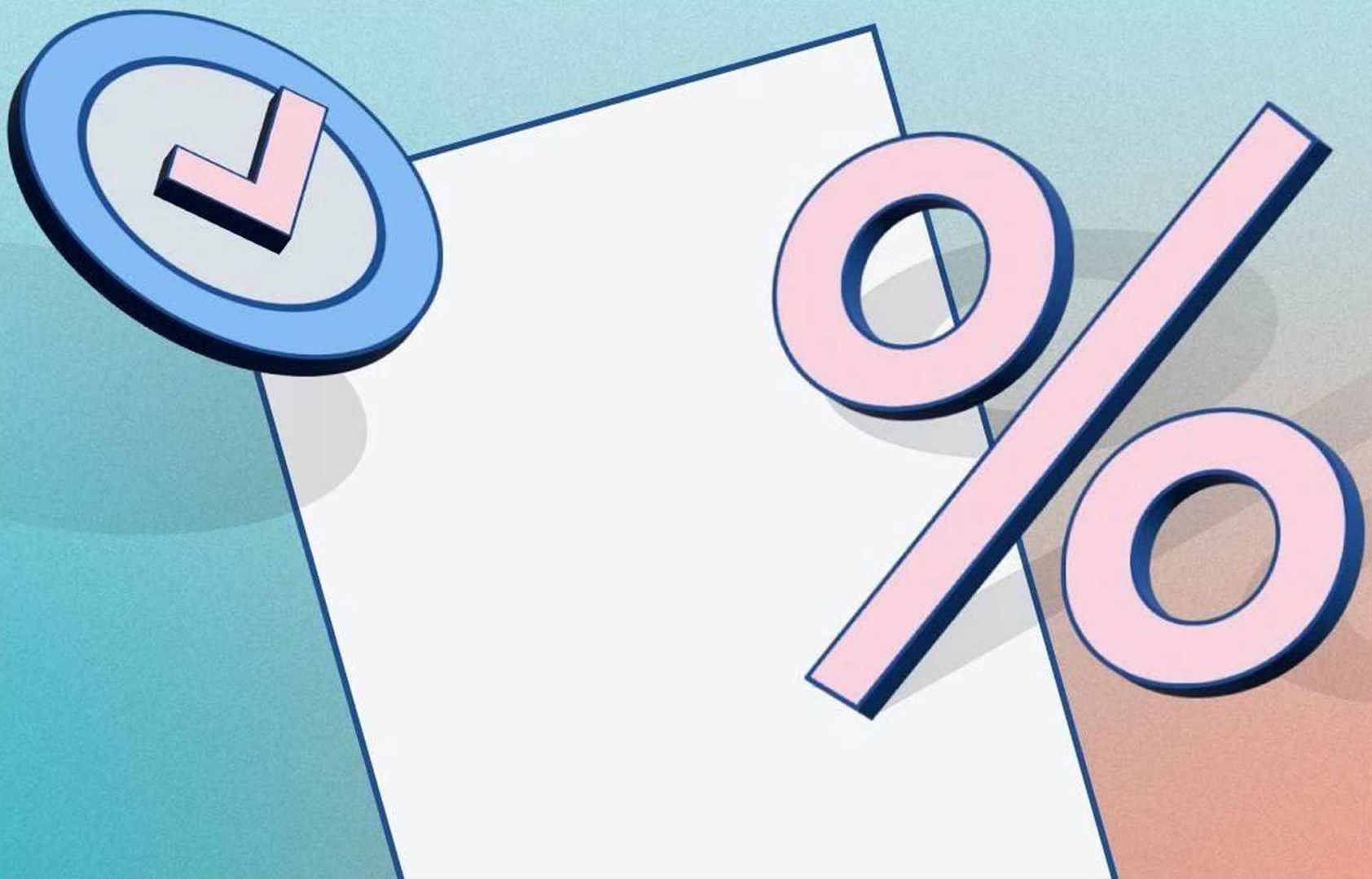


«Вас беспокоит специалист финансовой безопасности, сотрудник службы безопасности банка»

Отличить аферист от настоящего специалиста службы безопасности легко: первый будет интересоваться данными вашей карты или кодом из СМС.
К тому же он не сможет сообщить вам актуальный остаток по счету.

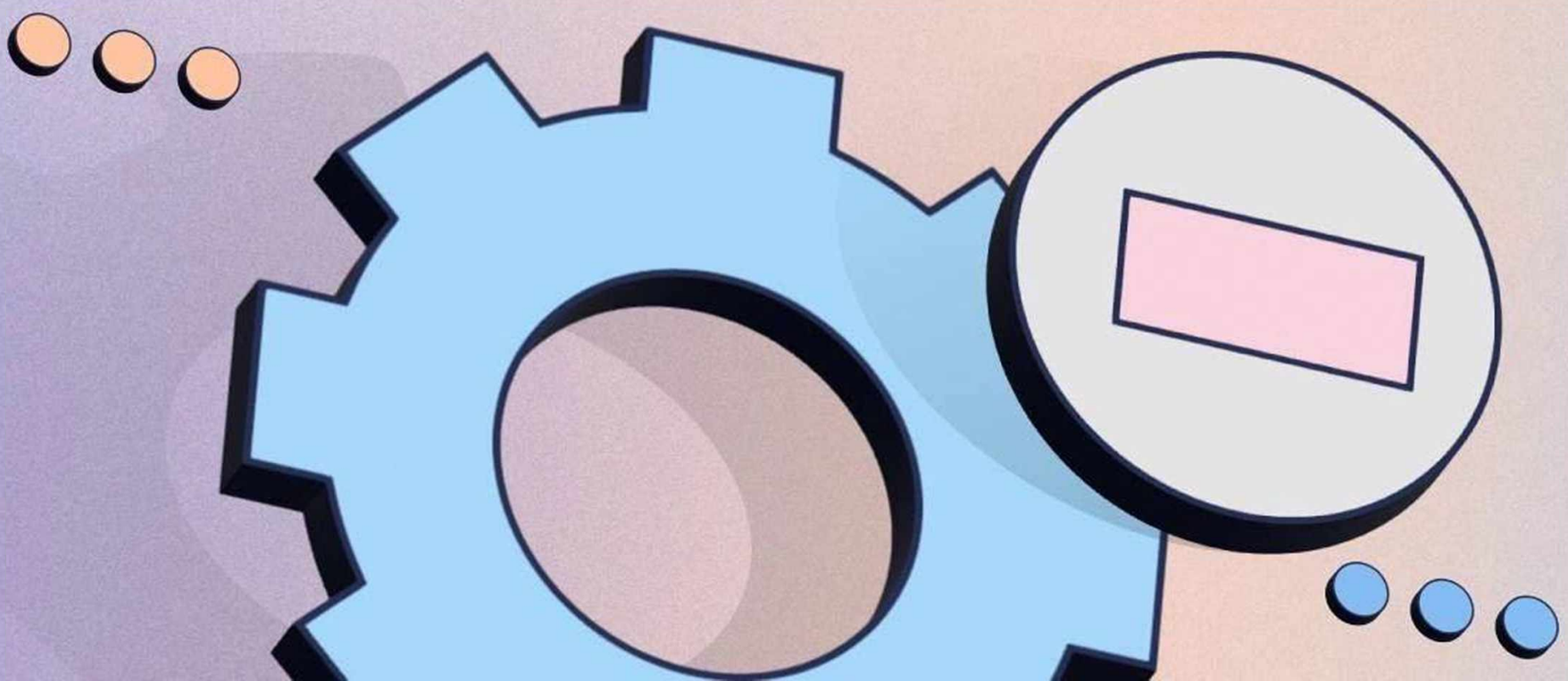
«Оформлена заявка на кредит»

Если вы не оставляли заявку, а вам сообщают о предварительно одобренном кредите, то просто кладите трубку. Не продолжайте разговор – иначе, сказав лишнего, вы точно поможете мошенникам оформить на вас кредит и похитить деньги.



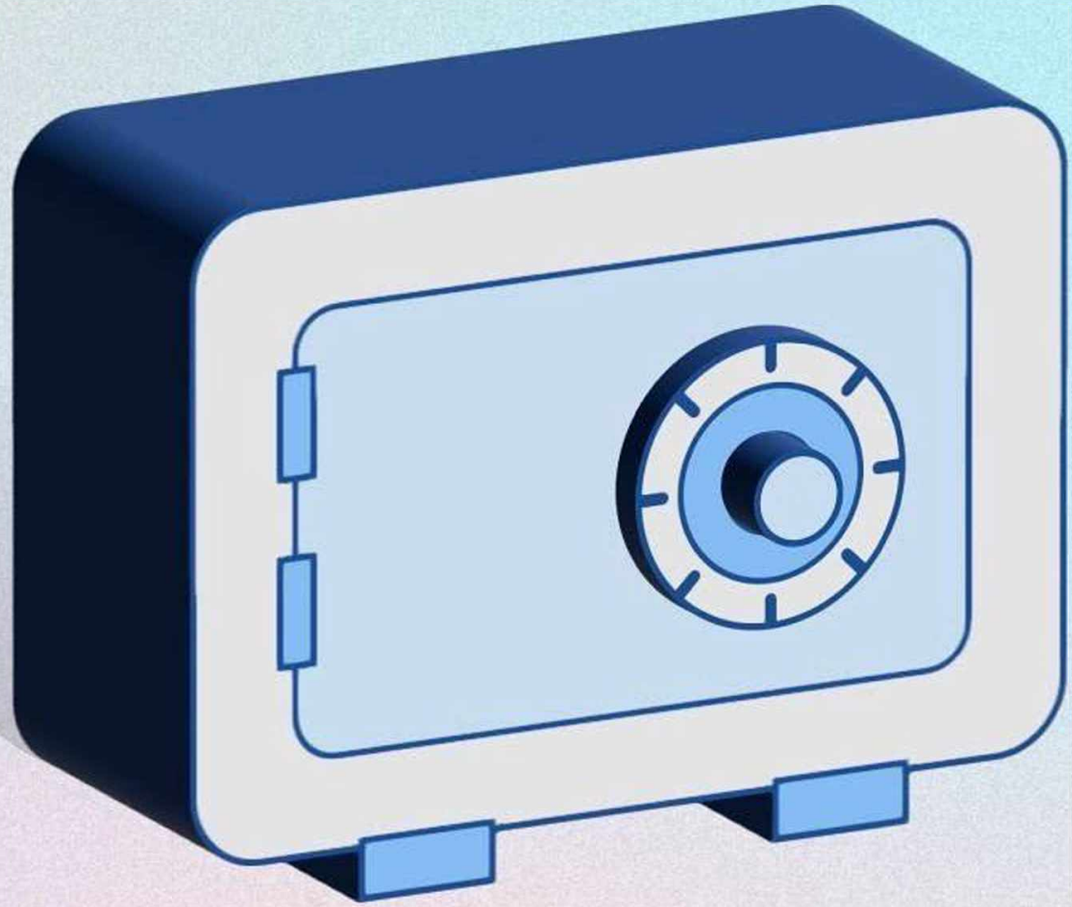
«Ваши деньги пытаются похитить, зафиксирована подозрительная операция»

Банки могут приостанавливать такие операции без участия клиента. Если у банка возникнут сомнения, его представитель может написать вам в онлайн-банке или позвонить для подтверждения операции.
Но, в отличие от жулика, настоящий работник банка звонит только с официального номера банка и никогда не просит совершить операции по карте.



«Специальный или безопасный счет»

Распространенная легенда аферистов, которые убеждают людей перевести сбережения на «специальный» счет – якобы для сохранности денег. Однако «специальных» («безопасных», «защищенных» и др.) счетов не существует.



Если с вами заговорили о деньгах и счетах, положите трубку и позвоните по официальному телефону организации или на горячую линию. Номер нужно набрать вручную.

Не поддавайтесь на уловки мошенников!

Банк России

Финансовая культура

МВД РОССИИ ПРЕДУПРЕЖДАЕТ!

Телефонные мошенники не только похищают деньги своих жертв, но и втягивают их в совершение преступлений

КАК РАСПОЗНАТЬ АФЕРИСТОВ?

- При разговоре злоумышленники сообщают, что неизвестные оформили от Вашего имени кредит и пытаются похитить денежные средства, однако есть возможность вернуть Ваши сбережения;

- Мошенники представляются сотрудниками правоохранительных органов и предлагают гражданам оказать содействие в поимке преступников;

- Предлагают хороший заработок в короткий срок абсолютно “легальным” способом.

- Иногда и вовсе злоумышленники напрямую угрожают своим собеседникам неприятностями или даже убийством их родных и близких.

СТОИТ ПОМНИТЬ!

**Каков бы ни был предлог звонивших,
их цель - подтолкнуть
вас к совершению преступления.**

**Как правило, это - поджог
объектов военной,
транспортной
или банковской
инфраструктуры.**

СТОИТ ПОМНИТЬ!

**Каков бы ни был предлог звонивших,
их цель - подтолкнуть
вас к совершению преступления.**

**Как правило, это - поджог
объектов военной,
транспортной
или банковской
инфраструктуры.**

БУДЬТЕ БДИТЕЛЬНЫ!

Внимательно относитесь ко всем звонкам и сообщениям, содержанием которых является требование совершить по инструкции собеседника какие-либо противозаконные действия.

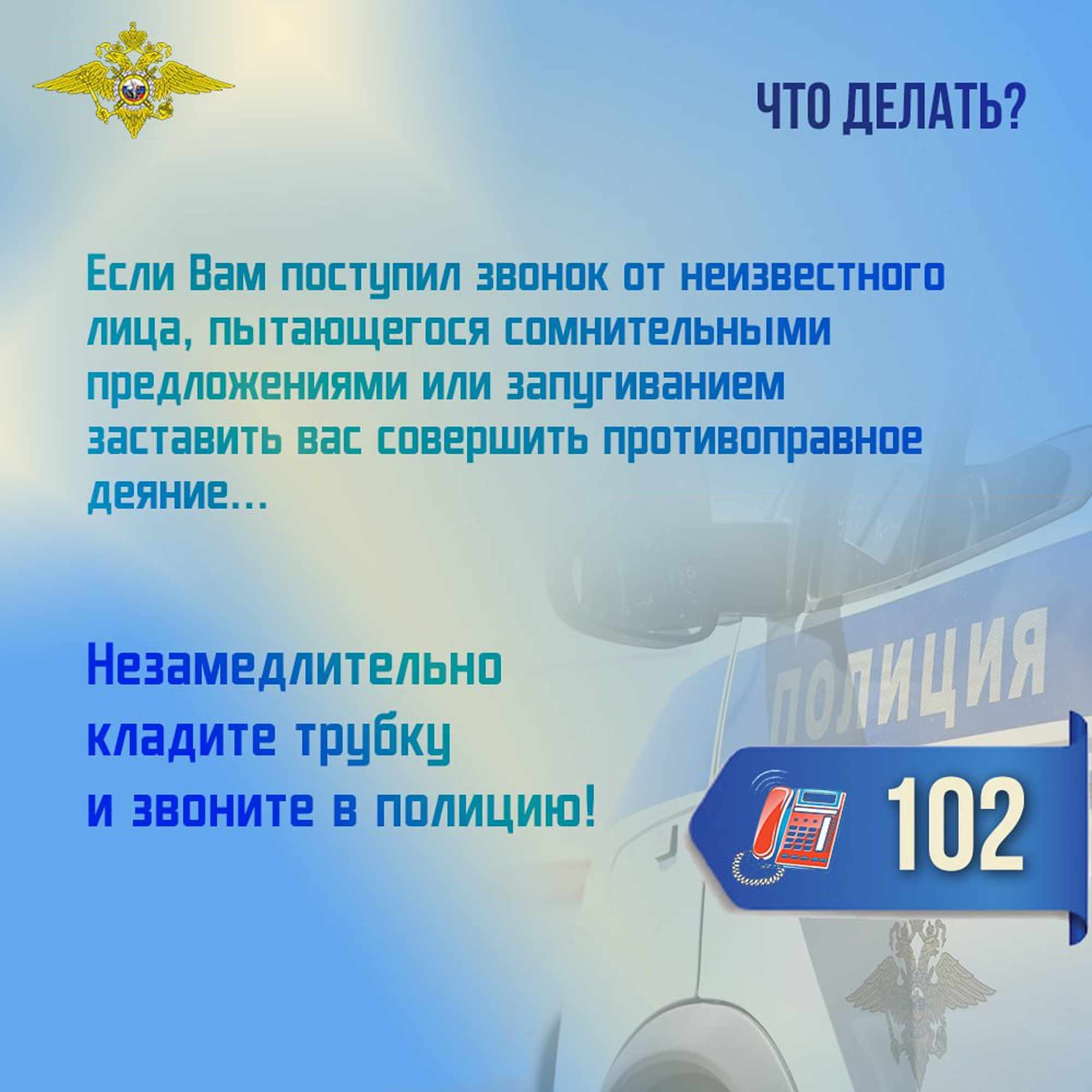
Помните, что атаки на военные и стратегически важные объекты действующим законодательством квалифицируются как диверсия или террористический акт.

Это - особо тяжкие преступления!

ЧТО ДЕЛАТЬ?

Если Вам поступил звонок от неизвестного лица, пытающегося сомнительными предложениями или запугиванием заставить вас совершить противоправное деяние...

Незамедлительно кладите трубку и звоните в полицию!



Фишинг и звонки от подставных сотрудников банков

Способы мошенничества достаточно общеизвестны. Это, во-первых, различные мошеннические схемы, связанные **с продажей товаров с созданием фейковых сайтов.** Сайт магазина либо бренда выглядит точно так же, как и настоящий, но в свои рекламные сообщения они **вставляют фишинговые ссылки,** и люди, переходя по ним, продукцию не получают, а деньги уходят мошенникам.

Еще одним распространенным способом являются **звонки от якобы служб безопасности различных банков** с предложением вывести деньги на безопасный счет.

Мошенники действуют из-за рубежа

Мошенники в подавляющем большинстве случаев находятся **за границей,** и максимальное их количество – **на Украине.** Все потому, что там есть русскоязычные граждане, которые **могут поддержать разговор, разыгрывая при этом различные спектакли.** Они могут представиться менеджером магазина, или сотрудником службы безопасности банка, или представителем полиции. Зачастую они включают определенные **психологические технологии, технику давления на человека.**

Простой способ себя обезопасить

К сожалению, достаточно много людей покупаются на эти схемы. Самый простой способ обезопасить себя от злоумышленников – **всегда положить трубку и перезвонить.**

Если вам звонят якобы из банка, значит, перезвоните в банк, если вам звонят из полиции, положите трубку и позвоните своим родственникам, которые якобы попали в ДТП, или позвоните в полицию. **Всегда есть возможность проверить информацию.**

Цифровая грамотность

Надо максимально скептически относиться ко всему, и после того как проверили, уже принимать решение. И уж точно не бежать в банк, не брать кредит и не переводить деньги на якобы безопасные счета.

И обязательно надо, чтобы об этом знало, как можно больше граждан, чтобы дети доводили эту информацию до своих пожилых родителей. **Обязательно надо повышать цифровую грамотность.**

РОСКОМНАДЗОР

Безопасно используем банковские

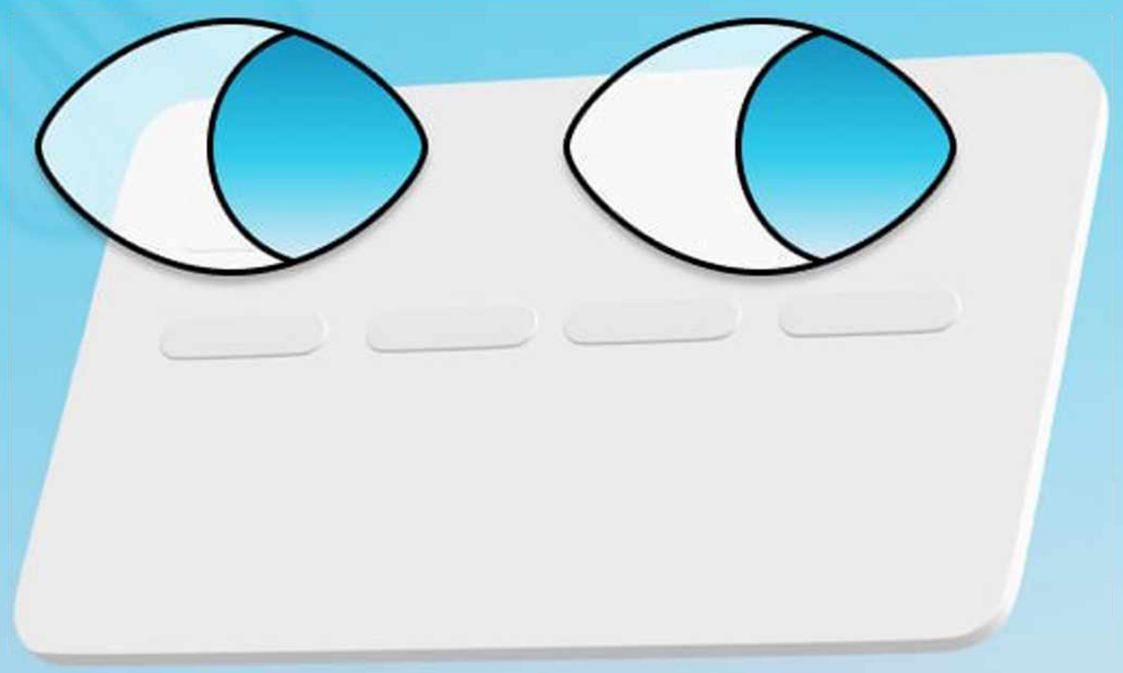
Банк России

и

е карты

Не оставляйте банковскую карту без присмотра

Любые операции по ней – только при вас.
Не разрешайте, например, официантам или кассирам уходить с вашей картой: просите принести терминал для оплаты.
Недобросовестные лица могут сфотографировать данные карты или переписать их.



РОСКОМНАДЗОР | Банк России

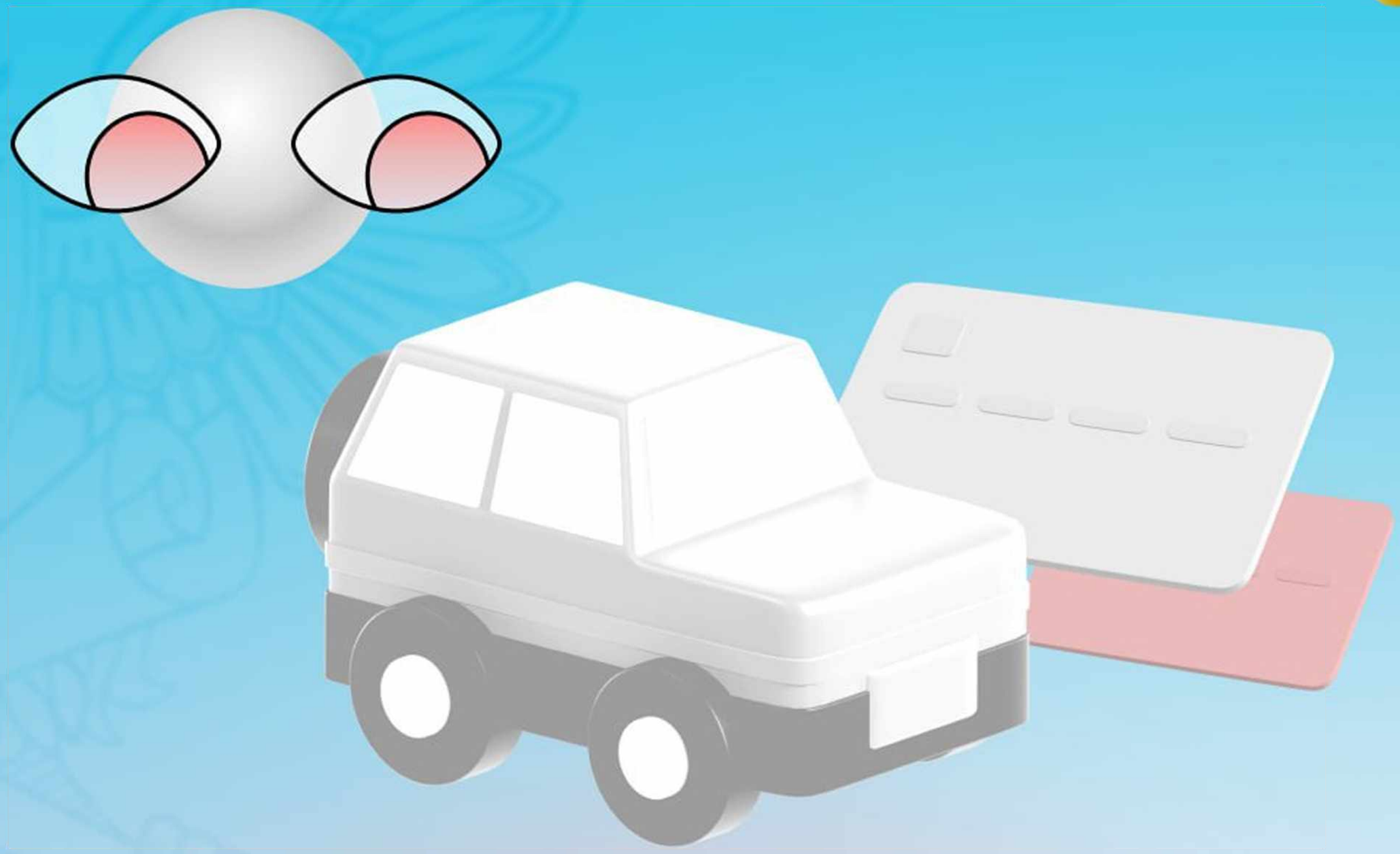
Не используйте зарплатную карту для онлайн-покупок

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

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

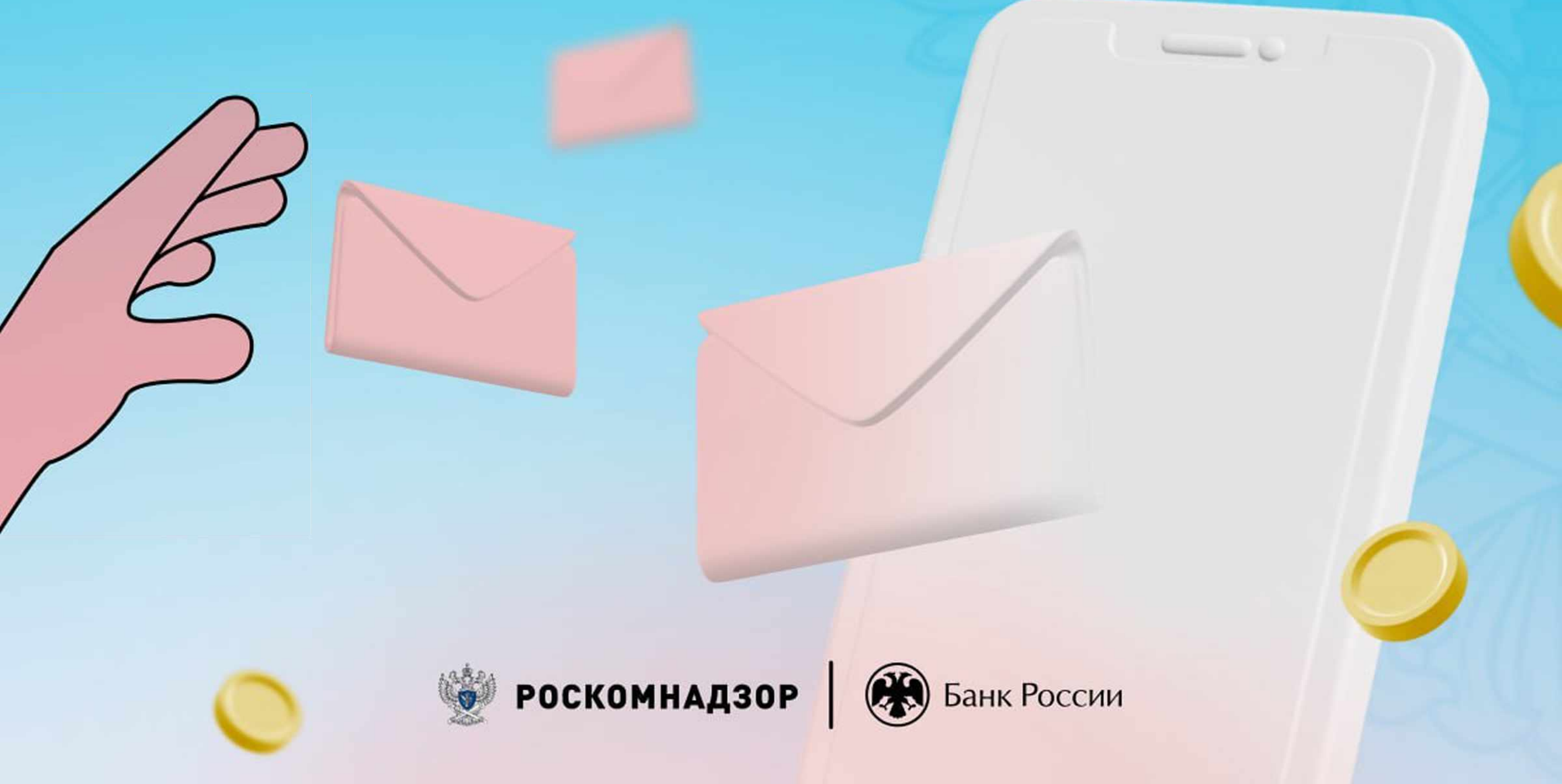
Не храните пин-код вместе с банковской картой и не записывайте его на «пластик»

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 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

Как себя обезопасить

Подключите смс- или пуш-уведомления. Так вы оперативно узнаете об операциях, которые не совершали, и сможете быстро заблокировать банковскую карту.

Пуш-уведомления обычно бесплатны и доступны для смартфона с приложением банка. Владельцам кнопочных телефонов подойдут смс-уведомления

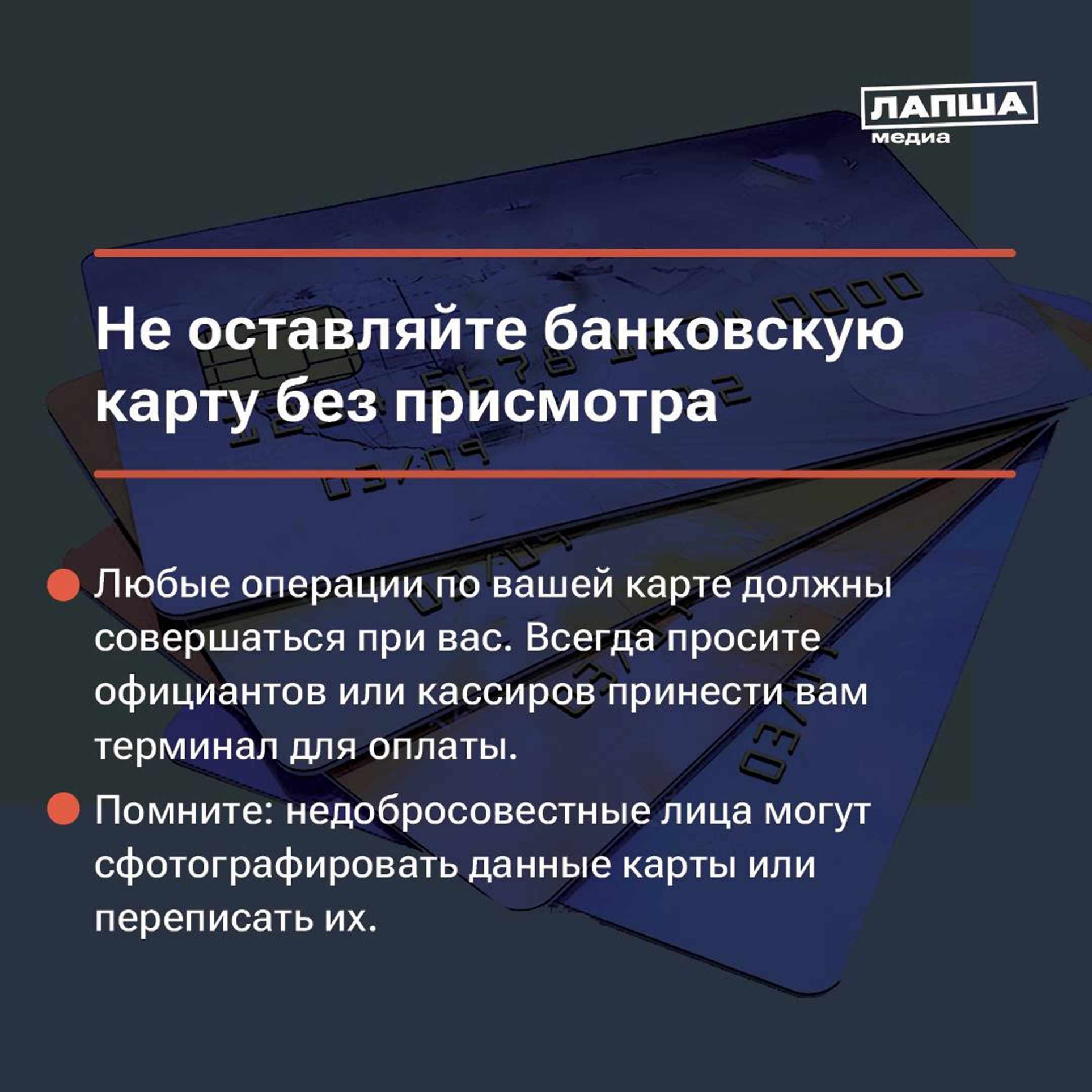
РОСКОМНАДЗОР | Банк России

Как себя обезопасить

Для безопасности на смартфоне лучше отключить отображение уведомлений при заблокированном экране устройства. Тогда при утере или краже мобильного мошенники не увидят содержимое оповещений от банка.

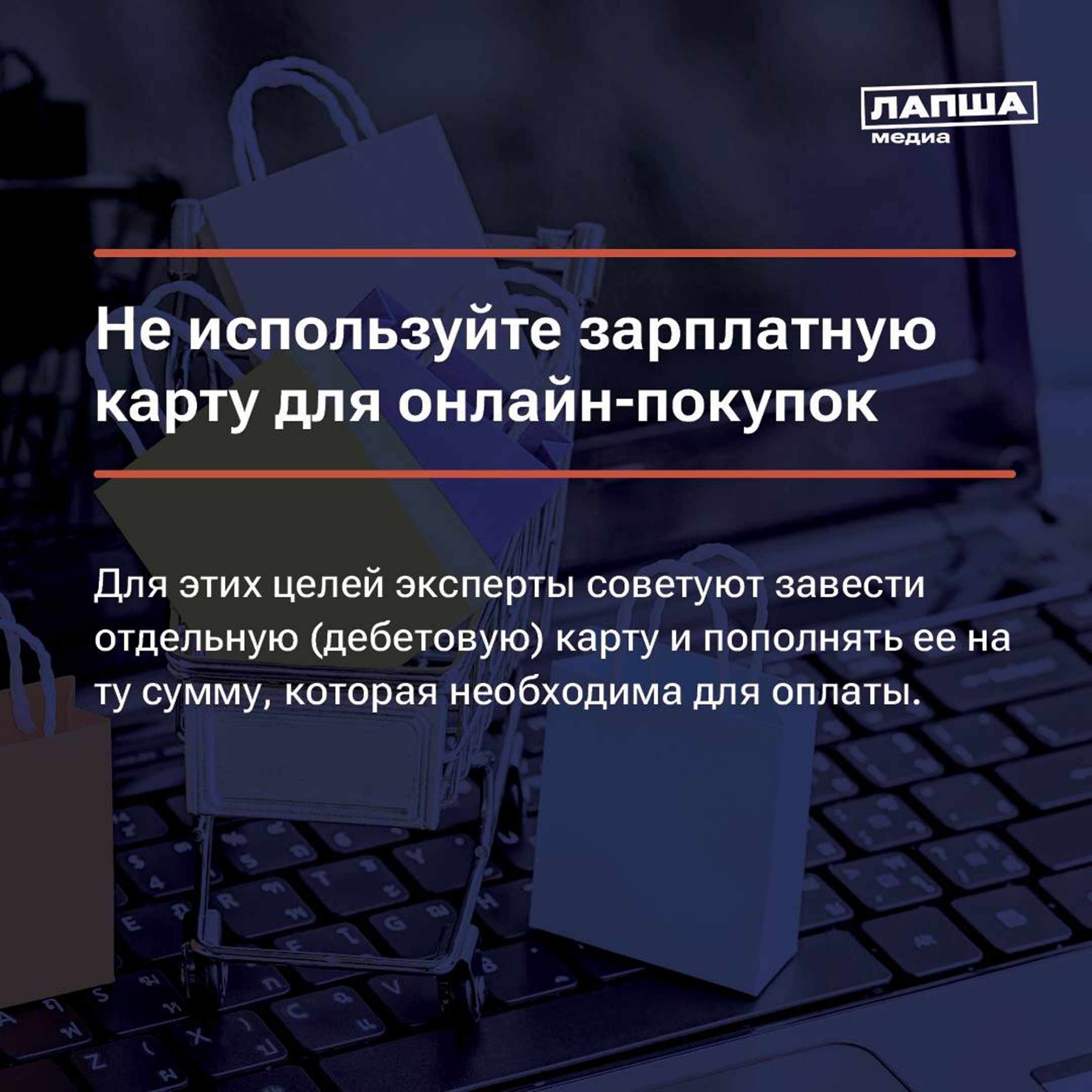
РОСКОМНАДЗОР | Банк России

ЛАПША медиа



Не оставляйте банковскую карту без присмотра

- Любые операции по вашей карте должны совершаться при вас. Всегда просите официантов или кассиров принести вам терминал для оплаты.
- Помните: недобросовестные лица могут сфотографировать данные карты или переписать их.



ЛАПША медиа

Не используйте зарплатную карту для онлайн-покупок

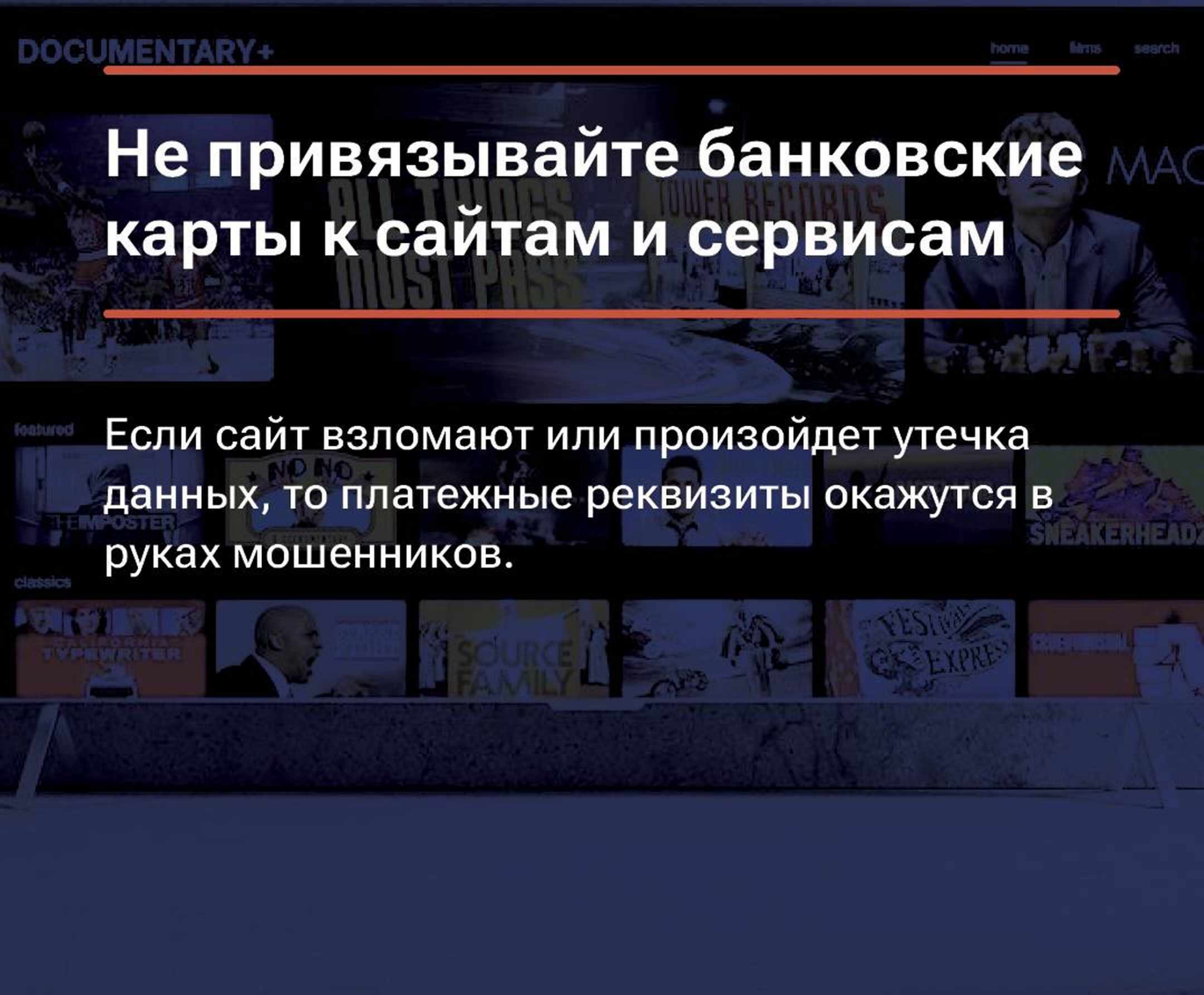
Для этих целей эксперты советуют завести отдельную (дебетовую) карту и пополнять ее на ту сумму, которая необходима для оплаты.

ЛАПША медиа

Не храните банковские карты в машине

На наличие в авто карт и ценных документов преступники обращают внимание в первую очередь.

ЛАПША
медиа



Не привязывайте банковские карты к сайтам и сервисам

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

ЛАПША медиа

Не храните пин-код вместе с банковской картой

Если у вас несколько банковских карт, для каждой установите свой сложный пин-код.

ЛАПША медиа

Почему работники могут стать жертвами мошенников?

Авторитет начальника и доверие знакомому человеку. Большинство уже выработало иммунитет к просьбам «полицейских» или «следователей». В схеме с «начальником» все иначе — к жертве обращается якобы знакомый и влиятельный человек.

Переадресация на внешних исполнителей. В примитивных вариантах схем «начальник» отдает распоряжение сам, но чаще он просит обсудить детали с сотрудником «ФСБ», «полиции» или «налоговой».

Большая срочность. Это важно, чтобы у жертвы не было времени подумать и разобрать ситуацию.

Абсолютная секретность. Чтобы никто не мог вмешаться в разыгрываемую сцену, «босс» предупреждает жертву, что обсуждать происшествие ни с кем нельзя.

ЛАПША медиа

Каковы цели атаки?

- Если жертва уполномочена проводить в фирме финансовые транзакции, ее будут убеждать провести срочный «секретный платеж» или перевести деньги на «безопасный» счет.
- Для сотрудников, не связанных с финансами, целью атаки будут либо данные компании — например, пароли к внутренним системам, — либо их собственные средства.
- Для большей убедительности мошенники могут пообещать компенсировать все расходы и труды жертвы — потом.

ЛАПША медиа

Важны ли детали?

- Благодаря многочисленным утечкам данных и публикациям в соцсетях, мошенникам стало проще проводить персонализированные атаки.
- Они могут заранее уточнить полное имя жертвы, ее руководителя, директора фирмы, узнать имена реальных сотрудников.
- Если на кону стоят серьезные суммы, мошенники могут провести длительную подготовку, чтобы разыгранная ими схема была предельно убедительна.

ЛАПША медиа

Технические аспекты

- Сложные мошеннические схемы почти всегда включают в себя общение со злоумышленниками по телефону.
- Первичное сообщение «от босса» может поступать разными способами — в рабочей электронной почте, мессенджере или опять же по телефону.
- Что касается телефонных звонков, то злоумышленники часто используют специальные сервисы, позволяющие подменять номер, или нелегально получают дубликат сим-карты.
- Во время звонков злоумышленники могут пользоваться инструментами автоматической замены голоса.

ЛАПША медиа

Как защититься от мошенников?

Не торопитесь и не паникуйте. Задача мошенников — вывести вас из равновесия. Сохраняйте спокойствие и перепроверьте все факты.

Обращайте внимание на адрес, телефон и аккаунт отправителя. Если вы обычно переписываетесь с начальником по почте, а тут он вдруг отправляет вам сообщение в мессенджере с незнакомого номера — время насторожиться.

Следите за нюансами. Странные просьбы, необычные формулировки и речевые обороты, грамматические ошибки и нетипичное оформление документов — проанализируйте все эти «красные флаги».

Насторожитесь при необычных требованиях. Если начальник или коллега требует срочно сделать что-то нестандартное, да еще сохраняя это в тайне, то это почти всегда признак мошенничества.

Уточните информацию у других коллег и обратитесь в правоохранительные органы или в службу безопасности компании.

МИФ

ЛАПША медиа

Я пользуюсь антивирусом — этого достаточно

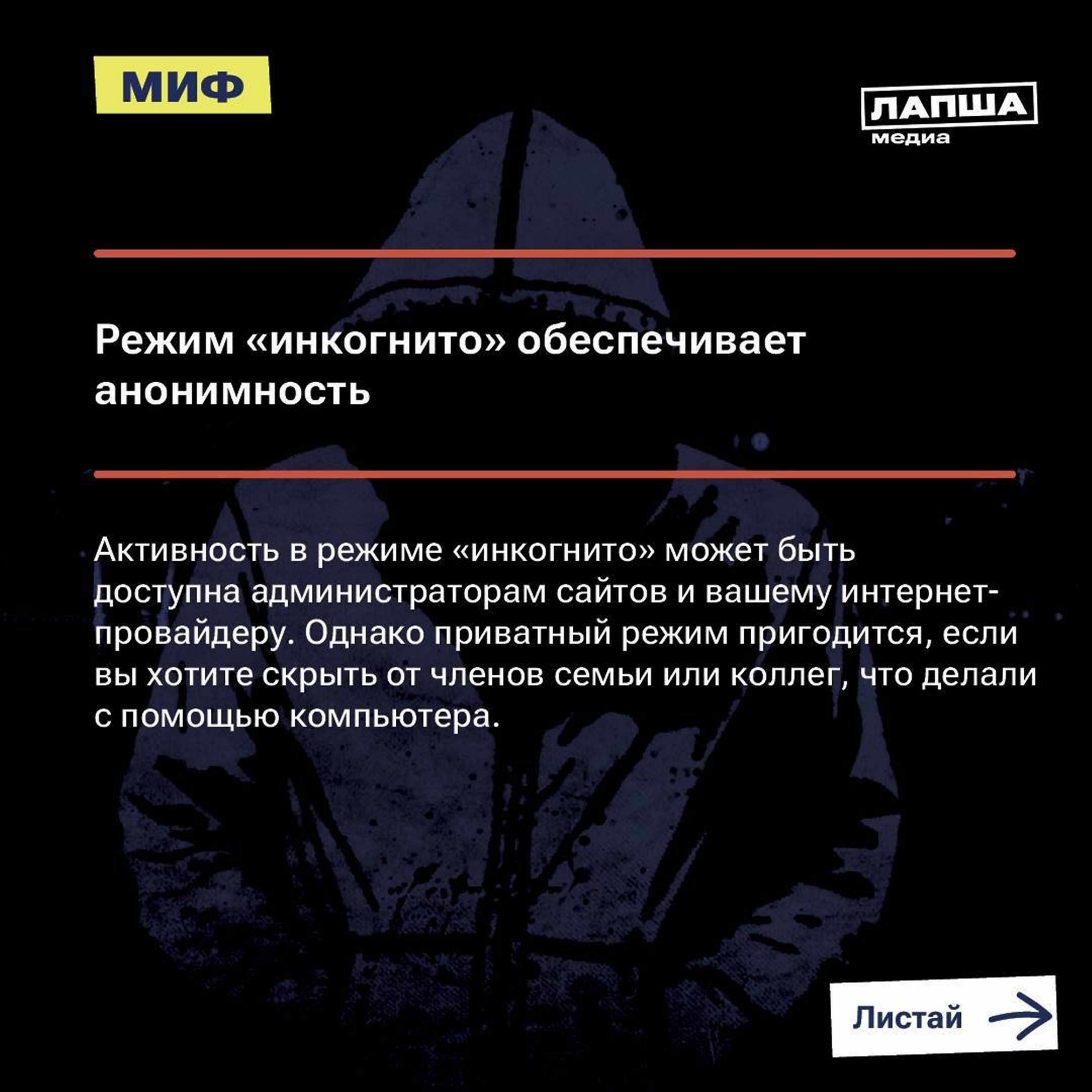
Серверы поставщиков антивирусного программного обеспечения могут быть уязвимы и подвергаться хакерским атакам. Поэтому всегда важно выбирать надежных разработчиков с именем и репутацией. Не экономьте на безопасности: лучше один раз оформить платную подписку, чем переплатить в будущем за новый софт.

Листай


МИФ
ЛАПША
медиа
В моих данных нет ничего ценного
Почти любые персональные данные могут быть использованы для совершения преступлений, например, краж или подделки документов. Любая информация в наше время представляет ценность.
Листай

МИФ

ЛАПША медиа



Режим «инкогнито» обеспечивает анонимность

Активность в режиме «инкогнито» может быть доступна администраторам сайтов и вашему интернет-провайдеру. Однако приватный режим пригодится, если вы хотите скрыть от членов семьи или коллег, что делали с помощью компьютера.

Листай

МИФ

ЛАПША медиа

Посещать известные сайты — безопасно

Все сайты используют файлы cookie для отслеживания интернет-активности пользователей. Обычно складывается ощущение, что все безопасно, но владельцы сайтов собирают и хранят ваши данные на серверах. Если сервер будет взломан, то хранящиеся на нем данные утекут в сеть.

Листай

Мошенничество в сети легко распознать

Это не всегда так. Фишинговые схемы становятся все более изощренными и убедительными: поддельные сайты для покупки билетов, сообщения в мессенджерах якобы от банков или ведомств, письма с напоминаниями сбросить пароль. Таким образом аферисты зарабатывают или рассылают вредоносный контент.

Письма мошенников: как понять обман

Мошенники часто присылают письма и сообщения, в которых под разными предлогами вынуждают перевести деньги им на счет.

Что должно насторожить в сообщениях, рассказываем в следующих слайдах.

Запрашивают информацию, которую нельзя передавать

- логины и пароли от учетных записей;
- данные счетов и карт;
- ФИО, адрес, телефон, номера документов;
- ответы на секретные вопросы для восстановления пароля;
- доступы к рабочим сетям и ресурсам.

Пишут подозрительные предложения и просьбы

- получить подарочные карты, купоны или скидки;
- забрать выигрыш в лотерею;
- срочно ответить на уведомление банка;
- получить прибыль по инвестициям с высокой доходностью;
- изменить пароль или подтвердить учетные данные;
- предоставить доступ к аккаунту.