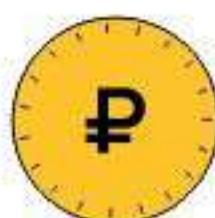
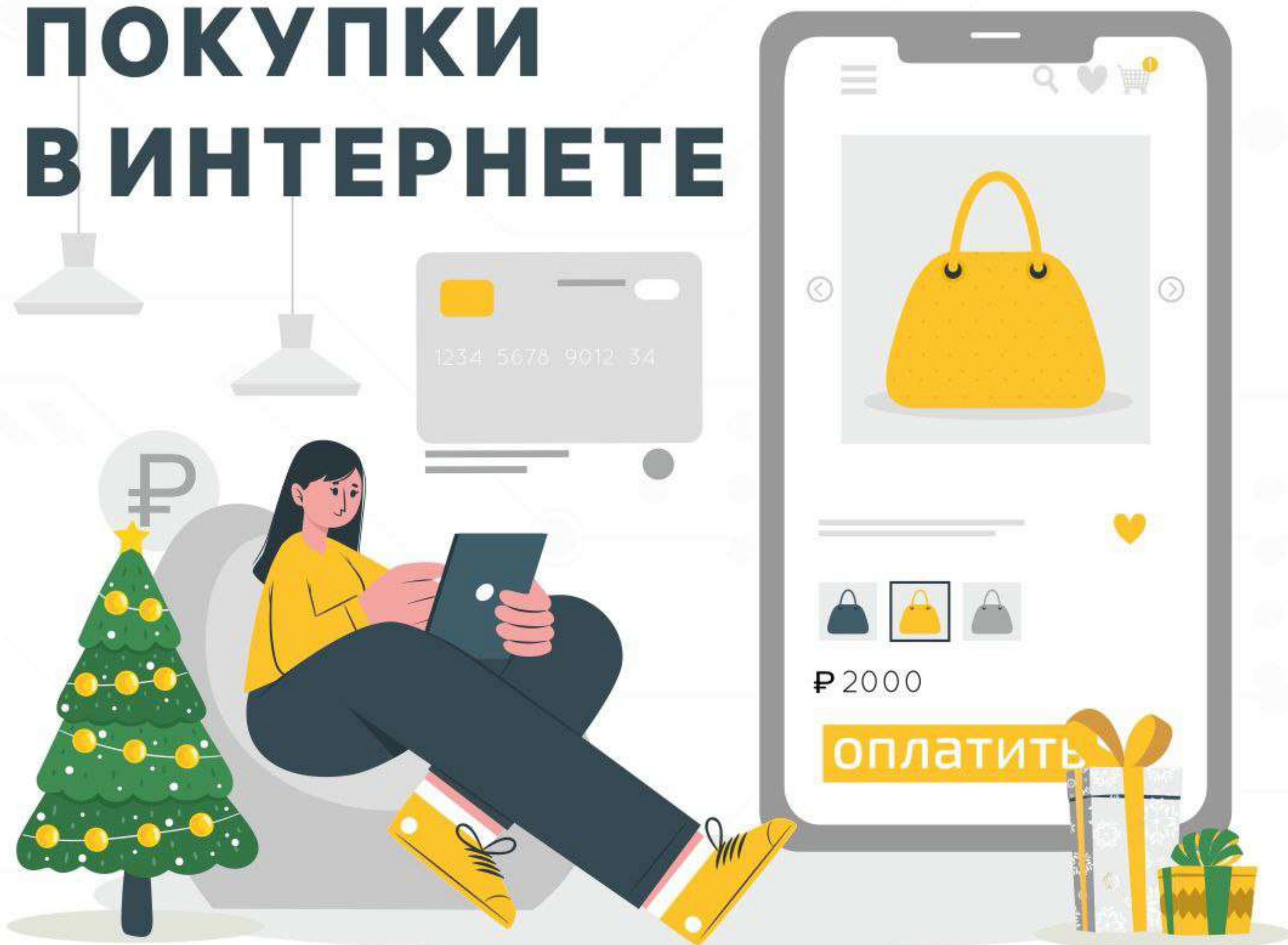


Безопасные покупки в интернете



Финансовая
культура

Не доверяйте обещаниям небывалых скидок!

Получили сообщение
о супервыгодной распродаже?

Ссылка может привести вас
на сайт, имитирующий
настоящий интернет-магазин

Если вы введёте на нём
данные своей банковской карты,
то они попадут к мошенникам



Проверяйте подлинность сайтов!

Признаки «клона» интернет-магазина:

- адрес (доменное имя) отличается на одну-две буквы или символ от привычного адреса

- нет префикса **https** (**s** означает secure, «безопасное соединение»)

- цены существенно ниже рыночных, это должно насторожить и заставить перепроверить подлинность сайта

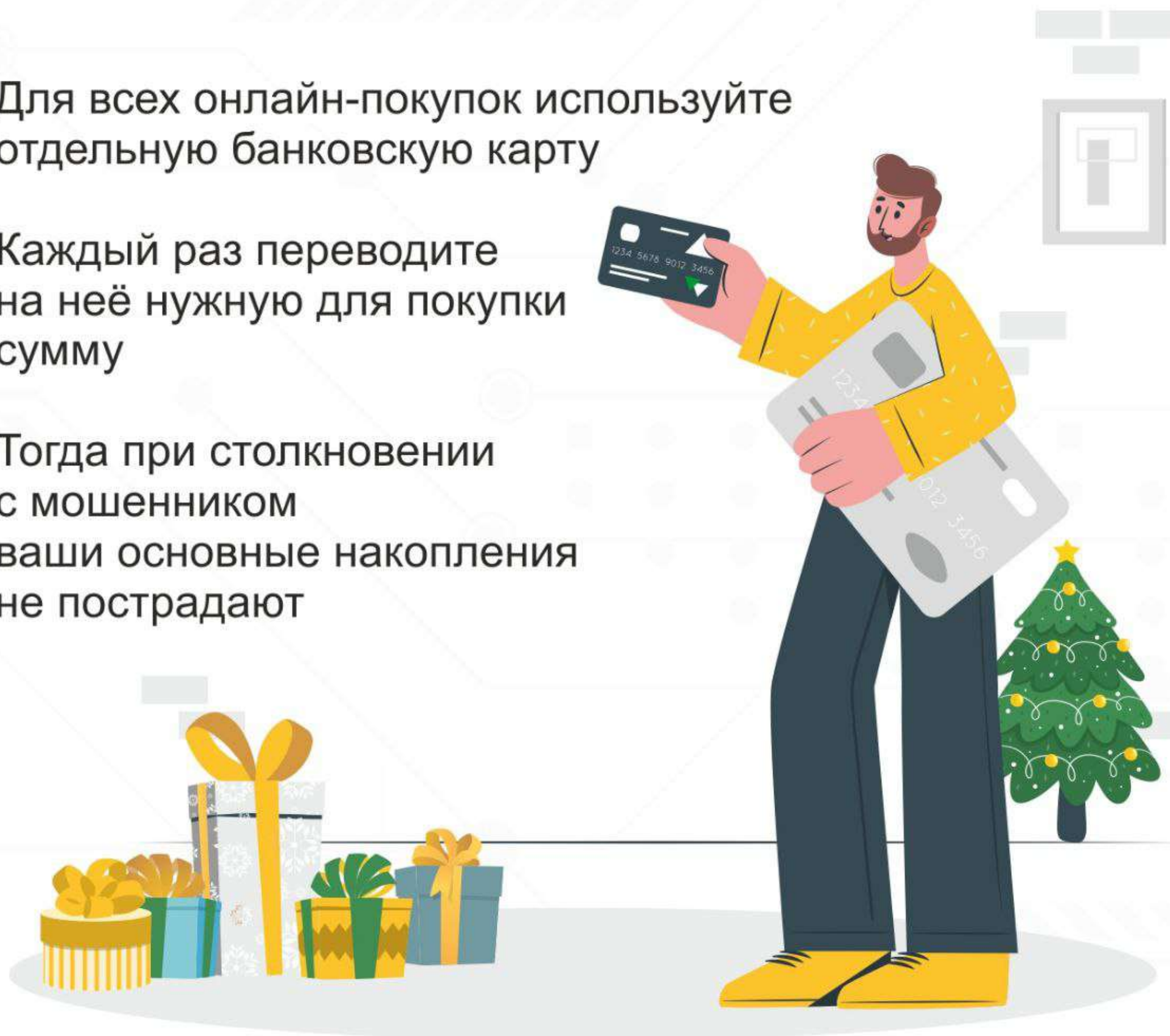


Берегите свою основную карту!

Для всех онлайн-покупок используйте отдельную банковскую карту

Каждый раз переводите на неё нужную для покупки сумму

Тогда при столкновении с мошенником ваши основные накопления не пострадают



Никому не сообщайте платежную информацию!

Никогда не разглашайте:

- данные своей карты и ПИН-код
- цифры с оборотной стороны карты
- коды платежа из СМС
- логины и пароли своих аккаунтов

Подключите СМС-оповещения
об операциях по карте

Так вы сможете быстро
отреагировать на действия
мошенников и заблокировать
свою карту





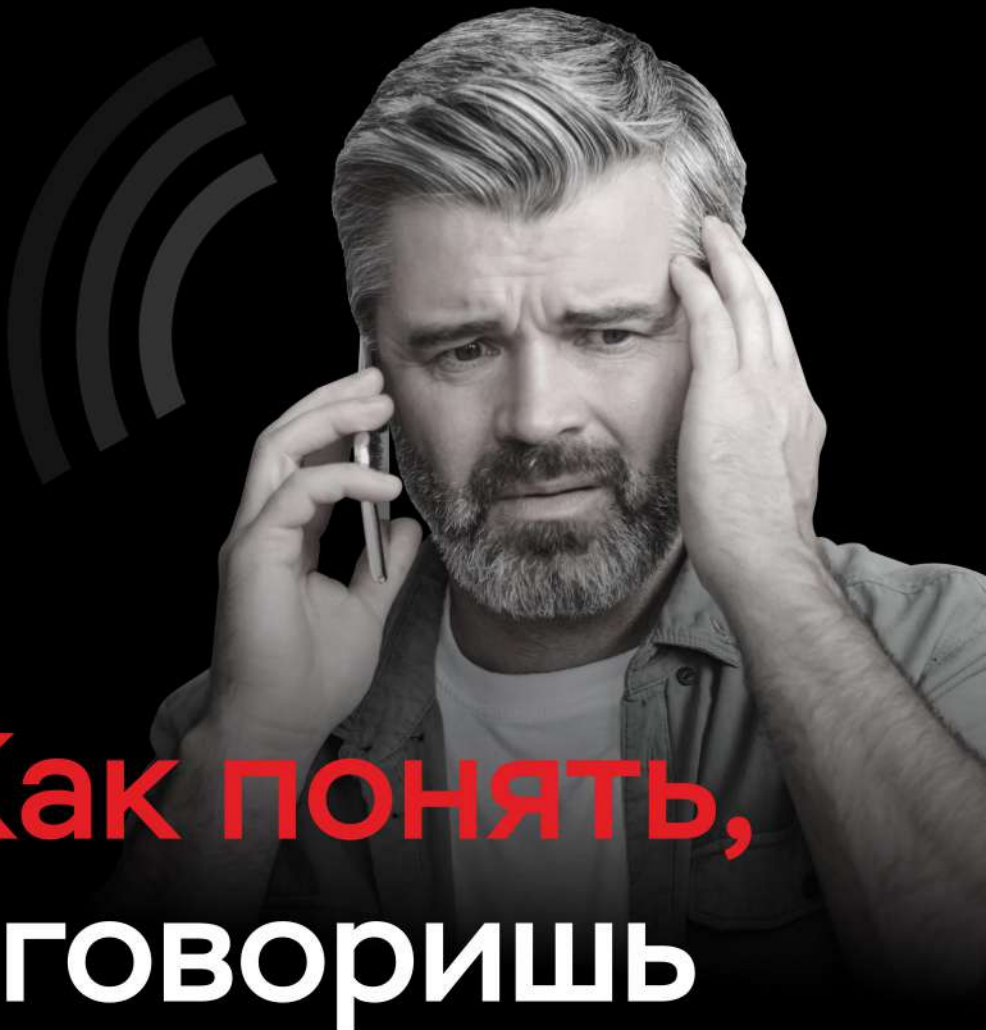
Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ



**Как понять,
что говоришь
с мошенником?**

Образ мошенника:

сотрудник вашего банка

- сообщает о попытке хищения денег
- предлагает перевести сбережения на «безопасный счет»





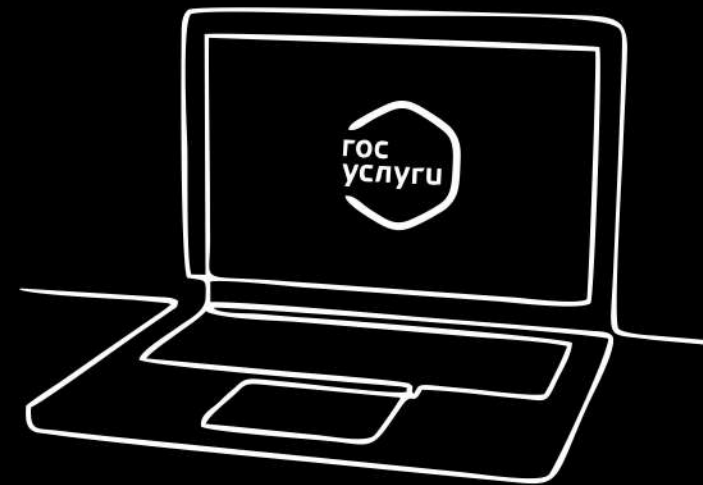
Образ мошенника:

сотрудник полиции

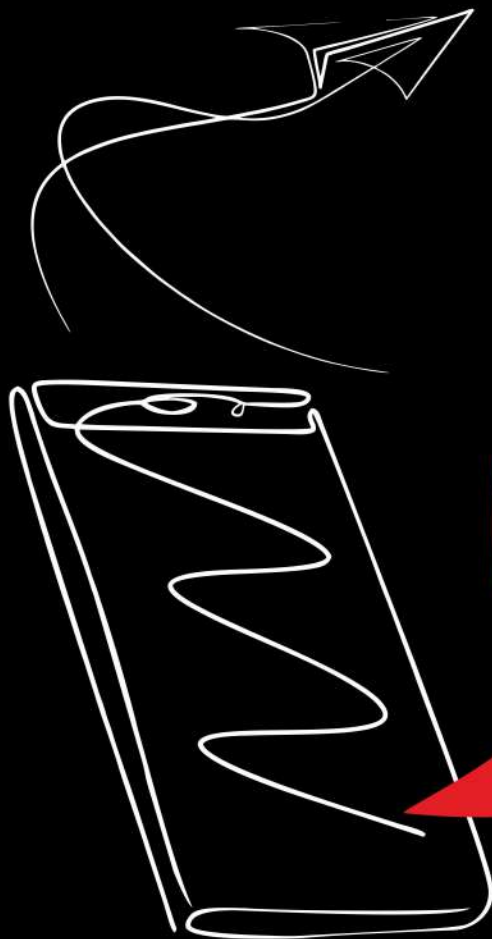
- ведет расследование об утечке персональных данных
- просит помощи в задержании аферистов
- обвиняет в госизмене

Образ мошенника:

служба безопасности Госуслуг



- пугает взломом личного кабинета
- сообщает о попытке оформить онлайн-кредит
- говорит об утечке персональных данных



Образ мошенника:

**оператор
мобильной
связи**

- сообщает о смене тарифного плана
- пугает отключением услуг
- предлагает переоформить договор

Образ мошенника:

“сотрудник
Соцфонда

- предлагает получить единовременную выплату
- настаивает на пересчете пенсии





Будь умней
телефонного
мошенника!



Клади
трудку



Без разговоров

КТО ТАКИЕ ДРОППЕРЫ?

Дроппер (или дроп) – человек, которого мошенники используют для вывода и обналичивания похищенных денег.

Как правило, человек сознательно помогает аферистам выводить деньги, но иногда становится их сообщником случайно.



КОГО МОШЕННИКИ ВОВЛЕКАЮТ В ДРОППЕРСТВО?

Подростки и студенты, как правило, нуждаются в деньгах и хотят быстро заработать.

Злоумышленники очень часто втягивают именно их в преступную деятельность.

По закону подростки вправе оформить банковскую карту уже с 14 лет и несут персональную ответственность за все операции по ней.



ЧТО ДЕЛАЕТ ДРОППЕР?

- как посредник передает чужие деньги от одного человека другому;
- переводит деньги на незнакомые счета и карты по указанию мошенников;
- снимает или вносит чужие наличные в банкоматах;
- оформляет на себя банковские карты и отдаёт их мошенникам, либо даёт доступ к своему онлайн-банку.

Мошенники предлагают вознаграждение, но сам дроппер становится соучастником мошеннической схемы: помогает запутать цепочку переводов.



ГДЕ МОШЕННИКИ ИЩУТ ПОТЕНЦИАЛЬНЫХ ДРОППЕРОВ?

Чаще всего — в интернете:

- социальные сети;
- мессенджеры;
- электронная почта.

Через знакомых рассказывают
о возможности якобы заработать легкие деньги.

В общественных местах расклеивают объявления.

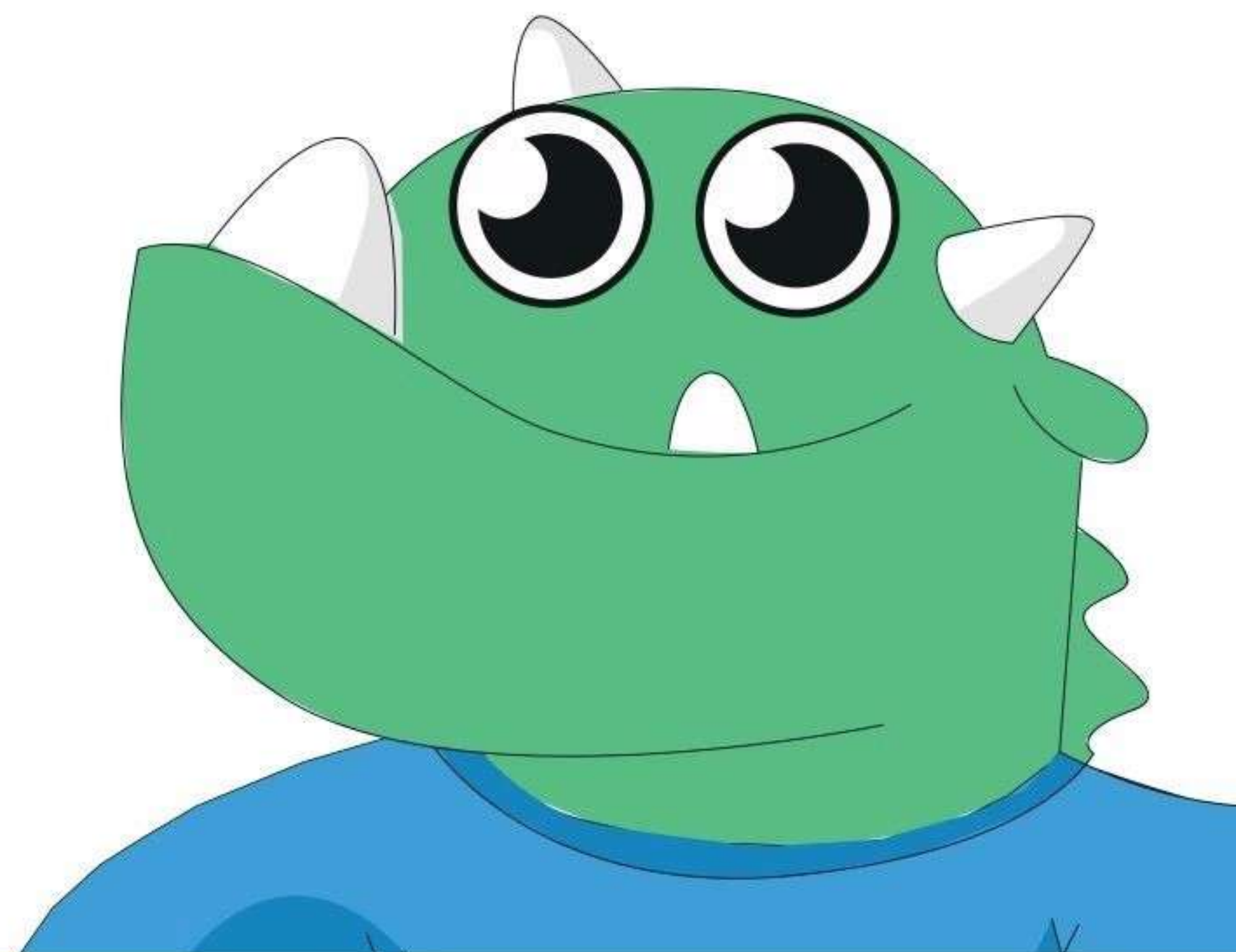


ЧЕМ МОШЕННИКИ ЗАВЛЕКАЮТ В ПРЕСТУПНУЮ СХЕМУ?

- предлагают «вакансию» без опыта работы, образования или специальных навыков;
- обещают лёгкую и быструю прибыль, но умалчивают, что дропперу придётся отвечать по всей строгости закона.



ЧЕМ ГРОЗИТ УЧАСТИЕ В ДРОППЕРСКОЙ СХЕМЕ?



Это уголовно наказуемое преступление.

Правоохранительные органы при расследовании мошеннических дел в первую очередь выходят на дропперов.

С «помощника» мошенников могут взыскать через суд всю сумму похищенных денег.

Кроме того, мошенники могут оформить кредиты на дропперов, которые им придётся выплачивать.

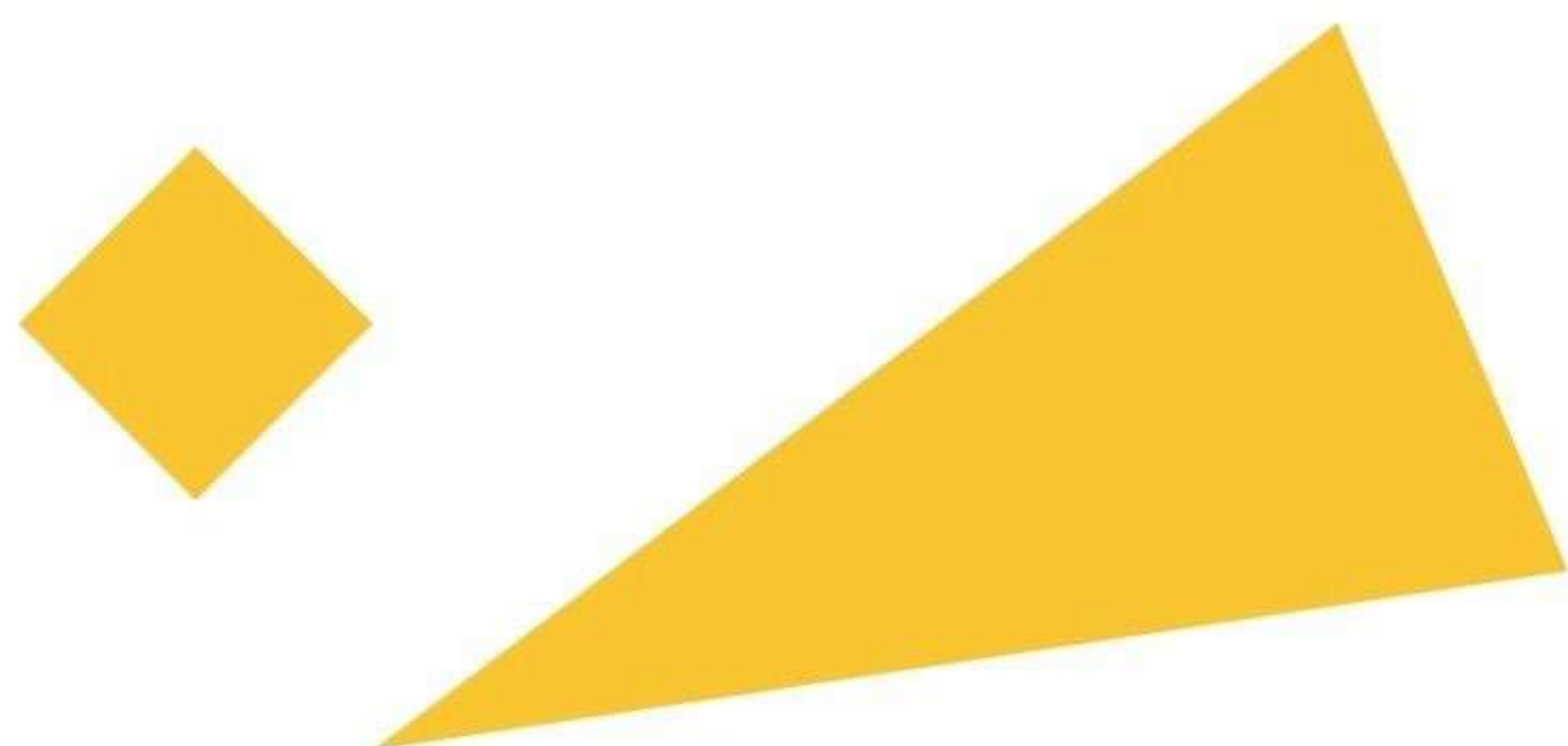
ВАРИАНТЫ ВЕРБОВКИ ДРОППЕРОВ

- **рассказы о «планах по продажам» в банках:**
«Оформи карту за вознаграждение»

- **вовлечение в сетевой маркетинг:**
«Приведи друга с картой — получи деньги»

- **предложение «трудоустройства»:**
«Стань администратором лотереи и отправляй выигрыш победителям»

- **сообщение якобы об ошибочной операции:**
«По ошибке отправил вам деньги — верните, но на другую карту или счёт»



С КАКИМИ ПРОБЛЕМАМИ СТАЛКИВАЮТСЯ ДРОППЕРЫ?

Банки ограничивают дропперам доступ к картам и онлайн-банку.

Сложности с получением
банковских услуг у дропперов
сохраняются вне зависимости
от того, сколько времени
прошло после участия
в преступной схеме.



”

Не передавайте свои банковские карты
и их реквизиты другим людям!

Не принимайте участие
в дропперской деятельности!

Подробнее читайте на сайте
Финкульт.инфо





ОСТОРОЖНО! МОШЕННИКИ!

**РОДСТВЕННИЦАМ УЧАСТНИКОВ СВО МОШЕННИКИ
СООБЩАЮТ О ГИБЕЛИ БЛИЗКИХ**

РАССКАЗЫВАЕМ, КАК С НИМИ РАЗГОВАРИВАТЬ!



Мошенники звонят, называют ФИО родственника и сообщают, что он погиб / находится в плену / ранен. Пока женщина отходит от шока, ее успевают попросить или потребовать перевести деньги. Так, например, могут легко попросить 10 миллионов за возможность вернуть из плена.



ОТКУДА БЕРУТ ИНФОРМАЦИЮ?

Из тематических чатов по поиску без вести пропавших, могут «пробить» родственников в социальных сетях, а могут услышать от вас же - уже обычное дело, когда звонят на телефон супруга, жена по наивности сходу сообщает, что телефон дома, а он на СВО и потом начинается череда звонков уже по новому поводу.



КАК РАЗГОВАРИВАТЬ С МОШЕННИКАМИ?

Как только услышали, что речь идет о вашем близком, который сейчас на СВО, лучше разговор закончить. После перезвонить, если есть возможность, супругу, либо в воинскую часть, либо на горячую линию Министерства обороны и узнать, все ли в порядке.



Если близкий действительно пропал без вести, то удержаться и положить трубку сложно. В таком случае, выслушайте внимательно информацию, которую вам говорят. Ни в коем случае не переводите деньги, не говорите номер карты, и вообще прекращайте разговор, как только речь заходит о деньгах. Если вас заинтересовала информация, запишите ее на бумагу и отправляйтесь в полицию, разберетесь уже вместе с сотрудниками правоохранительных органов.



Если вам сообщили о смерти или ранении - не паникуйте. Помните, что мошенники так часто делают. Попросите представиться и оставить телефон. Скажите, что отойдете от шока и перезвоните, не продолжайте этот разговор в состоянии паники. Потом выясните, где муж. Если ситуация неоднозначная - идите в полицию.



**Столкнулись с мошенниками?
Звоните по телефону: 102**



**УПРАВЛЕНИЕ ПО РАБОТЕ С ОБРАЩЕНИЯМИ ГРАЖДАН
МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
(ОБЩЕСТВЕННАЯ ПРИЕМНАЯ МИНИСТРА ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ) С 9.00 ДО 18.00 ПО
МОСКОВСКОМУ ВРЕМЕНИ ПО ТЕЛЕФОННЫМ
НОМЕРАМ:**

8-(800)-444-01-10 (МНОГОКАНАЛЬНЫЙ),

+7-(495)-696-71-32,

+7-(495)-696-71-36 ИЛИ

НА ОФИЦИАЛЬНЫЙ САЙТ

МИНИСТРА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ:

[HTTPS://LETTERS.MIL.RU/ELECTRONIC_RECEPTION/REQUEST/NATURAL.HTM](https://letters.mil.ru/electronic_reception/request/natural.htm).

**В ЮГРЕ РАБОТАЮТ ТЕЛЕФОНЫ «ГОРЯЧЕЙ ЛИНИИ»
ВОЕННОГО КОМИССАРИАТА.**

**ПО ТЕЛЕФОНУ ПРИНИМАЮТ ОБРАЩЕНИЯ ОТ
ЧЛЕНОВ СЕМЕЙ МОБИЛИЗОВАННЫХ.**

**С ПОНЕДЕЛЬНИКА ПО ПЯТНИЦУ С 8:30 ДО 12:30 И С
14:00 ДО 17:00 МОЖНО ЗВОНИТЬ ПО НОМЕРУ
+7(3467)39-72-10, 39-72-06.**

**ЕЖЕДНЕВНО С 8:00 ДО 2:00 ЗВОНКИ ПРИНИМАЮТ
ПО ТЕЛЕФОНУ +7(3467)39-72-05.**

**ТЕЛЕФОН «ГОРЯЧЕЙ ЛИНИИ» УПОЛНОМОЧЕННОГО ПО
ПРАВАМ ЧЕЛОВЕКА В ЮГРЕ.
8-952-710-90-95**



ОСТОРОЖНО! МОШЕННИКИ!

Как мошенники убеждают граждан оформить
«Зеркальный кредит»

ПОМНИ!

**Мошенники — хорошие психологи.
Утром думаешь, что тебя это не коснется,
а вечером пишешь заявление в полицию!**

Позвонил сотрудник банка?

- ✓ Прервите звонок и обратитесь в офис банка
- ✓ Никогда не сообщайте данные карты:
 - срок действия
 - CCV-код
 - пароль из sms-сообщения



ПРЕДУПРЕЖДАЕМ!

**Сотрудники службы безопасности банков
никогда не звонят клиентам для
предупреждения об имеющихся проблемах
со счетами, картами.**



Не следуйте инструкциям звонивших и
не отвечайте на задаваемые вопросы.
Положите трубку!



ОСТОРОЖНО! МОШЕННИКИ!

Как мошенники убеждают граждан оформить «Зеркальный кредит»

1

Вам звонит человек и представляется сотрудником службы безопасности банка

Уважаемый клиент! От вашего имени поступила заявка на оформление кредита на 500 тысяч рублей. Вы можете это подтвердить?

Нет. Я не оформлял кредит. Что мне делать?



2

Подставной специалист уверяет, что необходимо принять срочные меры и защитить свои данные



Я предлагаю вам оформить зеркальную заявку на этот займ. Так мы опередим мошенников. После этого я сразу отменю заявку.

Я согласен.

3

Желая спасти свои денежные средства, клиент следует указанием лжеспециалиста

Отлично, кредит оформлен. Теперь необходимо перевести всю сумму на безопасную ячейку. Записывайте номер.

Я выполнил все ваши указания.



4

Только когда деньги переведены на счета мошенников, граждане понимают, что их обманули, а кредит действительно одобрили

Абонент временно недоступен...



**Столкнулись с мошенниками?
Звоните по телефону 112**

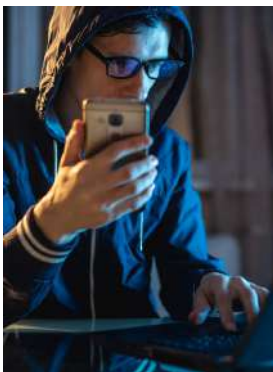


УМВД России по Югре, Прокуратура Югры,
Департамент региональной безопасности Югры
предупреждают

ОСТОРОЖНО! МОШЕННИКИ!

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

Если вам позвонили и, называя себя сотрудником банка, правоохранительных органов, руководителем органа власти, учреждения либо организации, представителем финансовой компании либо сайта «Госуслуги», специалистом известных телекоммуникационных компаний или интернет-магазинов, близким человеком,



► рекомендуют под предлогом пресечения противоправных действий, несанкционированного оформления кредита либо хищения денежных средств оформить встречный кредит и направить кредитные средства и личные сбережения на «безопасный банковский счет»;

► предлагают «быстрый, легальный и высокодоходный» заработок путем инвестиционных вложений;

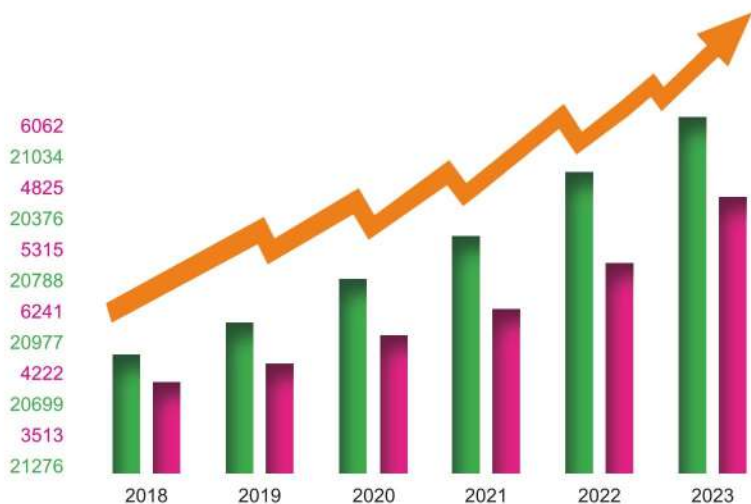
► сообщают о необходимости продлить договор на оказание услуг, обещая дополнительные бонусы и скидки, приглашают принять участие в оценке качества работы интернет-магазинов, предлагая при этом передать реквизиты банковской карты, коды из SMS-сообщений либо скачать «нужное» приложение;

► просят оказать срочную финансовую помощь, направляя сообщения или осуществляя звонки с известных вам номеров в мессенджерах «WhatsApp», «Viber», «Telegram»

Помните, что это может быть преступник, преследующий единственную цель – с помощью уговоров, давления, угроз и запугивания склонить вас к действиям с финансовыми средствами или к совершению противоправного деяния!

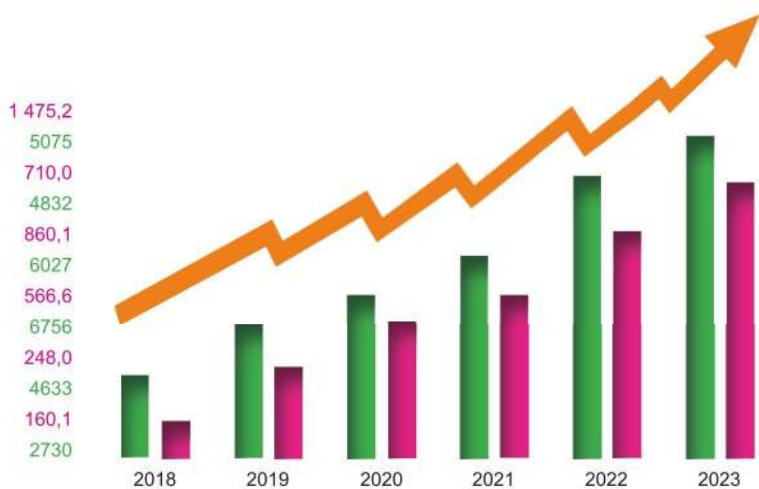
Незамедлительно кладите трубку! Не пытайтесь самостоятельно разбираться в ситуации, обратитесь за помощью к правоохранительным органам либо в кредитную организацию, где у вас открыты счета!

Ваш звонок может защитить вас!



■ Общее количество преступлений

■ Количество хищений, совершенных с использованием информационно-телекоммуникационных технологий



■ Количество потерпевших от хищений, совершенных с использованием информационно-телекоммуникационных технологий

■ Ущерб от хищений, совершенных с использованием информационно-телекоммуникационных технологий, млн руб.



ОСТОРОЖНО, ОБМАН!

МОШЕННИКИ:



ЛОЖЬ!

Добрый день, Мария Ивановна!
Я сотрудник банка...

ЛОЖЬ!

Здравствуйте! Я сотрудник полиции. Вы приобрели некачественные препараты, за них вам положена компенсация. Мы поможем вернуть деньги.



**ПОВЕСЬТЕ
ТРУБКУ!**

СОВЕТ:

Убедитесь, что вам звонили из банка,
перезвонив по номеру, указанному на
оборотной стороне карты





ОСТОРОЖНО, ОБМАН!

ЕСЛИ ВАМ СООБЩАЮТ, ЧТО ВАШ РОДСТВЕННИК:

1

Попал в ДТП, травмирован и ему нужна материальная помощь



2

Стал виновником ДТП, пострадавшему нужны деньги на операцию



3

Стал фигурантом уголовного дела и ему грозит тюремный срок



НЕМЕДЛЕННО ПРЕКРАТИТЕ РАЗГОВОР!



Позвоните родным и знакомым

1



Свяжитесь с родственником,
Который якобы попал в аварию

2



Обратитесь в полицию
или позвоните 112

3



ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО



Звонят из банка. Говорят об угрозе вашим деньгам на счете и попросят перевести деньги на другой счет. Спрашивают данные карты.

- что делать?



СРАЗУ ПОЛОЖИТЕ ТРУБКУ – ЭТО МОШЕННИКИ!

Позвоните по телефону, который указан на вашей банковской карте, сотрудник банка прояснит ситуацию.



Звонят и сообщают о выигрышах, выплатах, компенсациях и т.д.

- что делать?



НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ КАРТЫ!

если во время разговора вас просят совершить платеж - это мошенники. Положите трубку и, чтобы не сомневаться, уточните информацию на официальном сайте организации, от имени которой звонят.



Звонят и сообщают, что близкий человек попал в беду, просят перевести деньги.

- что делать?



ПРОЯСНИТЕ СИТУАЦИЮ!

Спросите фамилию звонящего и название организации, которую он представляет. Прекратите разговор и позвоните близкому человеку. Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.



ИНТЕРНЕТ



Предлагают вложить деньги на очень выгодных условиях.

- что делать?



**ОТКРОЙТЕ САЙТ
WWW.CBR.RU/FINORG**

Обо всех финансовых организациях, у которых есть лицензия Банка России, можно узнать на его официальном сайте.



На сайтах с объявлениями ("Авито", "Юла" и т.д.) предлагают товары и услуги по заниженным ценам.

- что делать?



НЕ ВНОСИТЕ ПРЕДОПЛАТУ!

Во время общения с продавцом не сообщайте данные банковской карты, не переходите по ссылкам. Пользуйтесь услугой "Безопасная сделка", которая доступна на сайте с объявлениями.



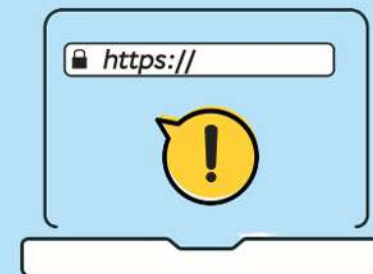
Нужно перевести или купить билеты. На одном из сайтов условия намного выгоднее, чем на знакомых ресурсах.

- что делать?



ПОЛЬЗУЙТЕСЬ ТОЛЬКО ПРОВЕРЕННЫМИ САЙТАМИ!

Безопасный сайт должен иметь надпись `https://` и "замочек" в адресной строке браузера.



ОСНОВЫ БЕЗОПАСНОЙ ЖИЗНИ ДЛЯ ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА



Департамент социального развития
Ханты-Мансийского автономного округа – Югры

Бюджетное учреждение
Ханты-Мансийского автономного округа – Югры
«Ресурсный центр развития социального обслуживания»

ОСНОВЫ БЕЗОПАСНОЙ ЖИЗНИ ДЛЯ ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА

ЭЛЕКТРОННОЕ МЕТОДИЧЕСКОЕ ПОСОБИЕ

Бюджетное учреждение
Ханты-Мансийского автономного округа – Югры
«Ресурсный центр развития социального обслуживания»
Сургут, 2024

Дорогие граждане!

Представляем Вашему вниманию электронное методическое пособие, адресованное людям старшего возраста с большим жизненным опытом.

На первый взгляд кажется, что они знают о жизни все и сами могут научить кого угодно. Но в реальности именно представители старшего поколения чаще всего становятся жертвами мошенников. Наверное, каждый может вспомнить случаи, когда вам или вашим близким предлагали «волшебные таблетки», сковородки и кастрюли «в подарок», обещали большие скидки на товары и услуги и т. д. Так действуют мошенники, цель которых – получить ваши деньги любой ценой. Для этого они используют любые средства: от уговоров и обещаний до запугивания.

Как показывает практика, наказать виновных, добиться справедливости и вернуть утраченные средства практически невозможно. Лучше предотвратить угрозу: предупрежден – значит вооружен.

КОРОТКО О МОШЕННИЧЕСТВЕ

*Граждане пожилого возраста –
самые уязвимые жертвы мошенников*

Жертвой мошенников может стать кто угодно, но самые уязвимые – пожилые люди. Им не хватает общения, они не всегда владеют современными технологиями и не могут сразу попросить о помощи. А еще они доверчивы и открыты к посторонним – этим мошенники и пользуются. Есть целая категория аферистов, которые специализируются на пенсионерах.

Мошенничество при личном контакте. Такие преступники подстерегают в торговых центрах и уговаривают бесплатно обследоваться, а потом навязывают дорогое лечение. Или ходят по квартирам и предлагают отрегулировать окна, вывести тараканов, «улучшить карму» и купить чудодейственный аппарат для снижения давления. При этом деньги пенсионер отдает наличными. Уголовный кодекс называет такое мошенничество классическим (ст. 159 УК РФ).

Классические аферисты очень убедительны: носят поддельные бумаги с гербовыми печатями, документы и удостоверения. А иногда и договоры на оказание услуг с несуществующими организациями. Они никогда не повышают голос, относятся с уважением, готовы к долгой и обстоятельной беседе. А еще они всегда знают, в чем проблема, и «готовы помочь». Таким сложно не поверить.

Дистанционные мошенники используют для своих махинаций телефон, интернет, страницы в соцсетях и недобросовестную рекламу. А деньги получают на электронные кошельки и банковские карты, оформленные на подставных лиц. Особые шпионские программы им не нужны: это дорого и сложно, а пожилые люди сами называют данные для перевода денег.

Чаще всего пенсионеров обманывают с помощью электронных платежей или используют их персональные данные.

Мошенничество с электронными платежами: человек теряет деньги через банковские карты, виртуальные кошельки. Например, если ему звонят якобы из банка, спрашивают данные карты и воруют деньги со счета (ст. 159.3 УК РФ).

Мошенничество с персональными данными: персональные данные похищают или изменяют, чтобы получить права на имущество. Например, оформляют за пенсионера электронную подпись и сами подписывают договор купли-продажи его квартиры (ст. 159.6 УК РФ).

В настоящее время можно легко и без особых проблем установить «запрет на действия с недвижимостью без личного участия» собственника, обратившись в АУ «Многофункциональный центр Югры» (филиал по месту жительства).

ПАМЯТКА ДЛЯ ПОЖИЛЫХ ЛЮДЕЙ



- Если вам предлагают купить чудодейственное средство от всех болезней
- Приобрести медицинские препараты с большой скидкой
- Пройти бесплатное обследование в медцентре
- Купить или переустановить счетчики, фильтры, дымоуловители
- Сообщают, что вы выиграли ценный приз, бесплатную путевку
- Незнакомцы требуют деньги за помощь вашим родным

БУДЬТЕ БДИТЕЛЬНЫ, ЭТО МОШЕННИКИ!

Запишите имена и телефоны злоумышленников и сообщите в полицию

ЕСЛИ ВЫ ОТКАЗАЛИСЬ В БЕДЕ И ВАМ НУЖНА ПОМОЩЬ, ЗВОНИТЕ 102 И 112

© ИА «Тюменская линия»

ВИДЫ МОШЕННИЧЕСТВА



ОСНОВНЫЕ ПРИЕМЫ МОШЕННИКОВ

**ПРОСЯТ ДЕРЖАТЬ
ВСЕ В ТАЙНЕ**

**НЕРЕАЛЬНЫЕ
ОБЕЩАНИЯ
(ЛЕКАРСТВО
ОТ ВСЕХ БОЛЕЗНЕЙ...)**

**НЕ ДАЮТ ВРЕМЕНИ
НА ОБДУМЫВАНИЕ**

НЕОЖИДАННОСТЬ

**НЕ ДАЮТ
ВОЗМОЖНОСТИ
ПОСОВЕТОВАТЬСЯ
С БЛИЗКИМИ**

ИМИТАЦИЯ ЗАБОТЫ

**ЭМОЦИОНАЛЬНОЕ
ДАВЛЕНИЕ, НАПОР**

ЗАПУГИВАНИЕ

ВЫ В ЗОНЕ РИСКА, если:

верите в чудеса

слишком доверчивые

испытываете одиночество

желаете вернуть былое здоровье

испытываете чувство тревожности

оказались в сложной жизненной ситуации

находитесь в тяжелом материальном положении

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

- ! БУДЬТЕ БДИТЕЛЬНЫ
- ! СОВЕТУЙТЕСЬ С БЛИЗКИМИ
- ! ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ
- ! НЕ СТЕСНЯЙТЕСЬ ОБРАЩАТЬСЯ ЗА ПОМОЩЬЮ И ИНФОРМАЦИЕЙ В ПОЛИЦИЮ, АДМИНИСТРАЦИЮ И ДРУГИЕ СЛУЖБЫ
- ! НЕ ОТКРЫВАЙТЕ ДВЕРЬ НЕЗНАКОМЫМ, НЕ РАССКАЗЫВАЙТЕ О СЕБЕ ПОСТОРОННИМ ЛЮДЯМ
- ! НЕ РАЗГОВАРИВАЙТЕ С НЕЗНАКОМЫМИ ЛЮДЬМИ ПО ТЕЛЕФОНУ
- ! НЕ ДАВАЙТЕ ПОСТОРОННИМ СВОИ Ф.И.О., АДРЕС, ДАННЫЕ ПАСПОРТА И БАНКОВСКИХ КАРТ
- ! НЕ ЗАНИМАЙТЕСЬ САМОЛЕЧЕНИЕМ, ВСЕ ЛЕКАРСТВЕННЫЕ ПРЕПАРАТЫ И МЕДИЦИНСКИЕ ПРИБОРЫ ПРИОБРЕТАЙТЕ В АПТЕКЕ ПО НАЗНАЧЕНИЮ ВРАЧА
- ! НЕ ПОКУПАЙТЕ ТОВАРЫ С РУК, НЕ ВЕРЬТЕ РЕКЛАМЕ И ОБЕЩАНИЯМ
- ! НЕ ОФОРМЛЯЙТЕ НА СВОЕ ИМЯ НИКАКИЕ БАНКОВСКИЕ КАРТЫ, КРОМЕ ПЕНСИОННОЙ
- ! НЕ БЕРИТЕ КРЕДИТЫ И МИКРОЗАЙМЫ
- ! НЕ ПОДПИСЫВАЙТЕ НИКАКИХ ДОКУМЕНТОВ, ПРЕДВАРИТЕЛЬНО НЕ ПРОЧИТАВ ИХ И НЕ ПОСОВЕТОВАВШИСЬ С БЛИЗКИМИ
- ! НИКОМУ НЕ СООБЩАЙТЕ ПИН-КОД, CVV-КОД И ДРУГИЕ ДАННЫЕ СВОЕЙ БАНКОВСКОЙ КАРТЫ
- ! НЕ ПРИНИМАЙТЕ ПОСПЕШНЫХ РЕШЕНИЙ

КАК ПРЕДОТВРАТИТЬ МОШЕННИЧЕСТВО

ПО СМС

Примеры сообщений:

«Вам по ошибке перечислили деньги – верните их через СМС-банк»

«Вы выиграли в лотерею – следуйте инструкциям и получите выигрыш»

«Вам положена компенсация. Чтобы ее получить, отправьте СМС...»

«Ваша карта заблокирована, для разблокировки отправьте в ответ ...»

Что нужно мошенникам: чтобы гражданин отправил деньги или данные карты через СМС.

Что не нужно делать: блокировать входящие СМС, отключать исходящие и мобильный банк. Опасны не сами СМС, а то, что пожилой человек переведет аферистам деньги. К тому же в СМС бывает что-то полезное: напоминания о записи к врачу, уведомления о зачислении пенсии и списаниях по карте.

Что делать: когда гражданин пожилого возраста оформляет в банке карту, можно привязать ее к отдельному номеру телефона. Можно настроить смартфон так, чтобы он принимал СМС на обе карты, а отвечать можно было с одной – не привязанной к счету, или купить для нее отдельный телефон. Пенсионер не будет проверять его постоянно, а у кодов подтверждения короткий срок действия.

Пример из жизни. Бабушка 76 лет получила СМС от банка: «Код для регистрации в онлайн-банке – 7735». Следом пришла СМС с незнакомого номера: «Извините, ошибся в одной цифре, и мой пароль пришел вам. Перешлите его, пожалуйста». Бабушка хотела помочь незнакомцу, но дома была внучка и отговорила ее. А если бы карта была привязана к номеру, где невозможно отправить СМС, бабушка и без внучки не попала бы на развод.

НЕ ГОВОРИ

НИКОГДА И НИКОМУ

- коды из СМС
- трехзначный код на оборотной стороне карты (CVV/CVC)
- PIN-код
- пароли/логины к банковскому приложению и онлайн-банку
- кодовое слово
- персональные данные



Банк России



Финансовая
культура

КАК БЫСТРО РАСПОЗНАТЬ МОШЕННИКА?

5 ПРИЗНАКОВ ОБМАНА

1 НА ВАС ВЫХОДЯТ САМИ

Аферисты могут представиться службой безопасности банка, налоговой, прокуратурой

Любой неожиданный звонок, СМС или письмо — повод насторожиться

2 РАДУЮТ ВНЕЗАПНОЙ ВЫГОДОЙ ИЛИ ПУГАЮТ

Сильные эмоции притупляют бдительность

3 НА ВАС ДАВЯТ

Аферисты всегда торопят, чтобы у вас не было времени все обдумать

4 ГОВОРЯТ О ДЕНЬГАХ

Предлагают спасти сбережения, получить компенсацию или вложиться в инвестиционный проект

5 ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Злоумышленников интересуют реквизиты карты, пароли и коды из банковских уведомлений



ВАЖНО

Сотрудники банков и полиции НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы с вашей карты



КАК ЗАЩИТИТЬ СВОИ ФИНАНСЫ



Узнай больше на
fincult.info

ПО ТЕЛЕФОНУ

Что говорят:

«Мама/папа/бабушка/дедушка, я попал в беду! Нужны деньги на лечение/взятку/компенсацию пострадавшему»

«Это служба безопасности банка, по вашей карте обнаружена подозрительная активность, давайте отменим операцию. Продиктуйте номер карты, срок действия и пин-код»

«Мы из полиции: ваш внук сбил человека, нужны деньги для пострадавшего»

«Вам положены компенсации/выплаты/надбавки/перечисления из бюджета. Нужно только оплатить комиссию»

«Это из поликлиники. У вас плохой диагноз – нужны лекарства и «волшебные» медицинские приборы, у нас они в наличии»

«Поучаствуйте в беспроигрышной лотерее»

«Вчера к вам приезжал курьер с доставкой, у нас строгая отчетность, и для нее необходимо продиктовать цифры из СМС-сообщения»

Что нужно мошенникам: данные карты для перевода денег (номер, срок действия и CVV – трехзначный код на обратной стороне карты). Граждане сами диктуют информацию по телефону.

Что не нужно делать: отказываться от банковских карт. Деньги в банке защищены лучше, чем наличные под матрасом.

Что делать: стереть с обратной стороны карты трехзначный код. Картой можно будет платить в магазинах, снимать с нее деньги и пополнять счет. Но без кода человек не переведет аферистам деньги, ничего не купит в сомнительном телемагазине и не сделает ставку в онлайн-лотерее. Для этого придется найти, где он записан,

или позвонить тому, у кого из родственников он сохранен, и спросить код. А родственник как раз и спросит, зачем он нужен.

Некоторые мошенники звонят и убеждают принести деньги наличными. Лучше отказаться от наличных в повседневной жизни, а снятие с карты ограничить несколькими тысячами рублей. Это можно сделать в мобильном приложении или в отделении банка, если прийти туда с пожилым родственником. Когда пенсионер не сможет снять большую сумму, он запаникует и позвонит кому-то из близких.

Также не нужно принимать доставки, которые вы не заказывали (цветы, пицца и т. д.).

Пример из жизни. Дедушке 74 лет позвонили и сказали, что его сын сбил человека. Пострадавший якобы в порядке, но за молчание просит 20 000 руб. Дедушка пошел к банкомату, но тот не работал. Тогда он позвонил внучке и спросил, где еще есть банкомат, – она и распознала обман. Если бы банкомат работал, дедушка лишился бы денег. Еще в этом случае помогло бы ограничение на снятие крупных сумм.

Как распознать мошенника?



Просят данные банковской карты, пароли и коды из СМС



Представляются якобы сотрудниками банка или полиции



Предлагают перевести деньги на «безопасный счет»



Пугают взломом Госуслуг



Гарантируют супердоход от инвестиций

**Клади
тфуцки**

Без разговоров.
Это мошенники!



Банк России



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ



ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

В КВАРТИРАХ

Что говорят:

«Мы из социальной службы, вам положена консультация»

«Мы из ЖЭУ, нужно осуществить поверку/проверку счетчиков»

«Мы из оконной фирмы, давайтеотрегулируем окна»

«В доме тараканы и клопы, требуется санобработка»

«Для пенсионеров у нас техника/лекарства/посуда со скидкой»

«Вам положено бесплатное медицинское обследование на дому»

«Подпишите петицию за справедливость. Надпись «кредитный договор» – это просто форма такая...»

Что нужно мошенникам: вынудить подписать кредитный договор, навязать втридорога бесполезный товар или обманом выманить наличные.

Что делать: для начала – осложнить мошенникам поиск жертвы. Они не обходят все квартиры в доме, а заранее выясняют, где живет пенсионер. Чтобы никто не догадался, что в квартире живет бабушка/дедушка, приведите в порядок почтовый ящик и входную дверь, переведите пенсию на карту и уберите лишнее с балкона. Еще можно приклеить на дверь наклейку, что объект охраняется.

В старых домах почтовые ящики часто без замков, и из них легко достать содержимое. Из платежных извещений мошенники узнают данные пенсионера, а потом называют его по имени и отчеству. Там же смотрят, сколько в квартире прописано человек: если один, то, возможно, это одинокий человек. Еще в документах бывает информация о льготах. Выход – установить замок на почтовый ящик и следить, чтобы там не скапливалась корреспонденция.

Еще два возможных признака, что в квартире живет пожилой человек: много вещей на балконе и обшарпанная дверь. Убедите родных не хранить на балконе «старье» и не сушить там половики. И попросите родных поставить хотя бы недорогую железную дверь. Внешне она не будет сильно отличаться от дорогих.

Почтальон, который разносит пенсии в определенный день, – тоже знак, что в квартире живет бабушка или дедушка. Причем банковских карт у них нет, зато есть наличные. У таких почтальонов мошенники тоже часто выуживают информацию. Например, представляются участковыми и спрашивают, кто в подъезде всегда дома и мог быть свидетелем преступления. Почтальоны не только называют таких пенсионеров, но и дают им характеристики. Лучше отказаться от доставки пенсии наличными и оформить начисление на банковскую карту (это бесплатно).

Мошенники не любят места, где есть камеры и в любой момент может появиться полиция. Можно купить муляжи камер и наклейки с надписью «ведется видеонаблюдение». Они яркие и бросаются в глаза («охраняется полицией», «ведется видеонаблюдение»). Также можно повесить в подъезде плакат с телефоном участкового и графиком приема.

Пример из жизни. Бабушка 83 лет шла по улице, а рядом женщина упала на землю. Бабушка подошла к ней, а та сказала: «Я ясновидящая. Мне было видение, что с вашим самым дорогим человеком случится беда. От этого мне стало плохо. Покажите мне фото, и я сниму порчу». Бабушка пригласила ее в квартиру и дала фото своей дочери. Мошенница сказала, что ей нужны все бабушкины деньги, чтобы снять сглаз. Но у пенсионерки была только карта. Аферистка дала номер своей карты и попросила перевести все, что есть, но никому об этом не рассказывать, а то процедура не подействует. Мошенница ушла, а бабушка не удержалась и позвонила дочери – сообщить про порчу. Денег мошенница не дождалась. Если бы мошенница увидела в подъезде наклейки о видеонаблюдении, возможно, у нее нашлись бы другие дела. Смотреть в полиции видеозаписи своих подвигов преступники не любят.

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

1

ПРОВЕРЬТЕ СРОК ПОВЕРКИ СЧЕТЧИКОВ:

- В ВЕРХНЕЙ ЧАСТИ ЕПД
- В ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ ПРИБОРА
- ПРИ ЛИЧНОМ ПОСЕЩЕНИИ ЦЕНТРА ГОСУСЛУГ «МОИ ДОКУМЕНТЫ»



Если срок поверки не наступил, то проверять и заменять счетчик нет необходимости. Если вас уверяют в обратном – скорее всего, это мошенники.



Если подошел срок поверки, выберите аккредитованную организацию или управляющую компанию с соответствующим разрешением, или обратитесь в организацию, которая установила вам счетчики.

2

УТОЧНИТЕ У ЗВОНЯЩЕГО НАЗВАНИЕ ОРГАНИЗАЦИИ, ОБЯЗАТЕЛЬНО ЗАПИШИТЕ ЕГО И СВЕРЬТЕ ДАННЫЕ С «ЧЕРНЫМ СПИСКОМ» НЕДОБОРОСОВЕСТНЫХ ПОСТАВЩИКОВ УСЛУГ НА САЙТЕ ФАС fas.gov.ru



3

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ, ОБРАТИТЕСЬ В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ



В МЕДИЦИНСКИХ И ТОРГОВЫХ ЦЕНТРАХ

Что говорят:

«Для вас есть заем на выгодных условиях. Внукам не говорите – купите им подарки и сделаете сюрприз»

«В нашем медцентре для вас бесплатная диагностика по госпрограмме. Заболевание у вас тяжелое, а лечение нужно дорогое... Но в соседнем кабинете можно оформить кредит на выгодных условиях»

«Для пенсионеров мы проводим бесплатный курс по торговле на бирже. Сейчас подскажем, какие акции купить, чтобы и вам на безбедную старость хватило, и внукам на подарки»

Что нужно мошенникам: вынудить подписать кабальный договор купли-продажи, кредитный договор или «развести» на большие траты.

Что делать. От такого мошенничества труднее всего защититься. Фирмы аферистов часто официально зарегистрированы и даже платят налоги. Почти всегда они подписывают с пенсионером договор, а при его наличии нет оснований для возбуждения уголовного дела. В этом случае полиция отправляет человека в суд. Привлечь виновных к ответственности и вернуть деньги почти невозможно. Наоборот, если пенсионер не платит по кредиту, мошенник может подать на него в суд.

Гарантированных способов борьбы с этим пока нет. Главное – не носить с собой паспорт: без него невозможно заключать договоры. Можно просто положить его подальше, рядом с документами на квартиру, например.

Пример из жизни. В торговом центре женщине предложили полежать на ортопедическом чудо-матрасе. Он стоил 30 000 руб., и ее убедили купить его в кредит. Оказалось, ставка – 10% ежемесячно. Женщина уже год ходит по судам, чтобы расторгнуть кабальный договор. Если бы у нее не было с собой паспорта, она бы не оформила кредит. Паспортные данные пенсионеры редко помнят.



ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

**МОШЕННИКИ
ПРЕДЛАГАЮТ
КОМПЕНСАЦИИ
ЗА ЛЕКАРСТВА
И БАДЫ**

Как не стать жертвой мошенников, снимая деньги в банкомате?



Пользуйтесь банкоматами
в фойе банков, крупных
ТРЦ



Проверяйте, нет ли у банкомата
подозрительных деталей



Прикрывайте клавиатуру
рукой, когда набираете
PIN-код



Сохраняйте чеки,
чтобы свериться с историей
платежей на Kaspi.kz



Никогда никому не
сообщайте PIN-код, CVV2
и срок действия карты



Сделайте
репост, расскажите
друзьям!

Схема мошенничества с банковской картой в кафе, барах, магазинах



Клиент отдает карту
для оплаты в руки
официанту (бармену,
продавцу)



Работник-мошенник
уносит карту
и фотографирует
ее реквизиты



Спустя время он совершает
онлайн-покупки, а с карты
клиента списываются
суммы

Как предотвратить:



Не передавать карту
третьим лицам (в том
числе фото карты)



Не показывать
CVV-код



Попросить принести
POS-терминал или пройти
к кассе для оплаты



Держать закрытым
доступ для покупок
в интернете



Не игнорировать
сообщения от банка
о списании
денег



Сделайте
репост, поделитесь
с друзьями!

ПАМЯТКА ДЛЯ РОДСТВЕННИКОВ ПОЖИЛЫХ ЛЮДЕЙ

КАК ЗАЩИТИТЬ ПОЖИЛОГО РОДСТВЕННИКА ОТ МОШЕННИКОВ

1. Почаще звоните, приходите в гости к пожилым родственникам и спрашивайте, как у них дела. *(Тогда они скорее послушают вас, чем попадутся на уловки аферистов.)*

2. Рассказы о мошенниках помогают плохо: новые схемы появляются каждый день и бабушки/дедушки не всегда их распознают. *(Но не стоит и запираť пожилого человека дома: он не заключенный.)*

3. Почистите бабушкин/дедушкин почтовый ящик и установите на него замок. Уберите лишние вещи с балкона и поставьте новую входную дверь. *(Так аферисты не догадаются, что в квартире живет одинокий пожилой человек.)*

4. Убедите пожилого родственника получать пенсию на банковскую карту, а не наличными у почтальона.

5. Привяжите банковскую карту пожилого родственника к отдельному номеру и заблокируйте на нем исходящие СМС.

6. Запомните (запишите) и сотрите трехзначный код на обороте банковской карты пожилого родственника. Установите лимит на снятие наличных.

7. Убедите пожилого родственника держать паспорт подальше (если есть возможность – уберите в сейф в его квартире). Когда документ понадобится, пусть он позвонит вам и спросит, где находится его паспорт или код от сейфа.

8. Контролируйте звонки и расходы пожилого родственника через приложения банков и мобильных операторов.

9. Установите в квартире пожилого родственника видеоглазок или сигнализацию. Сигнализации бывают с веб-камерами, датчиками движения и брелоками с тревожной кнопкой. Если что-то случится, вам поступит звонок.

Как телефонные мошенники используют для обмана WhatsApp

Входящий вызов
+7 99* * ** ***

1

Мошенник звонит
с иностранного
номера



2

Я из
техподдержки

Представляется
сотрудником банка



3

Предлагает
перейти в WhatsApp
«для безопасности»



4

Отправляет фото
поддельных
удостоверений



5

Запугивает, что
у жертвы пытаются
похитить средства



6

Убеждает перевести
их на «безопасный
счет» и исчезает

Обратите внимание



Сделайте
репост, поделитесь
с друзьями!

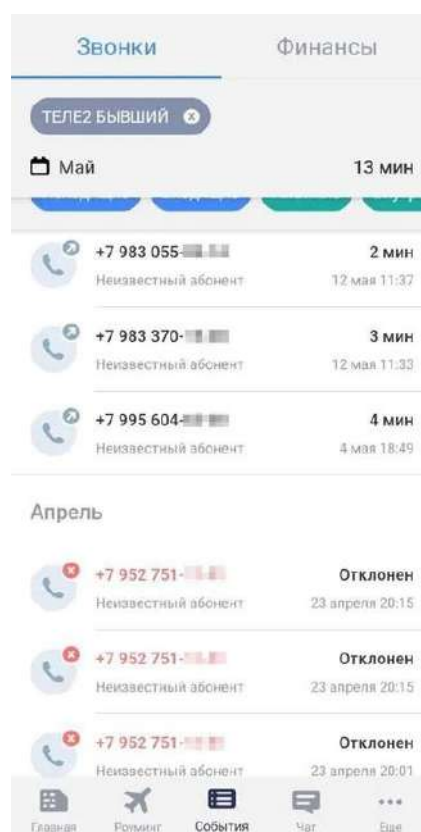
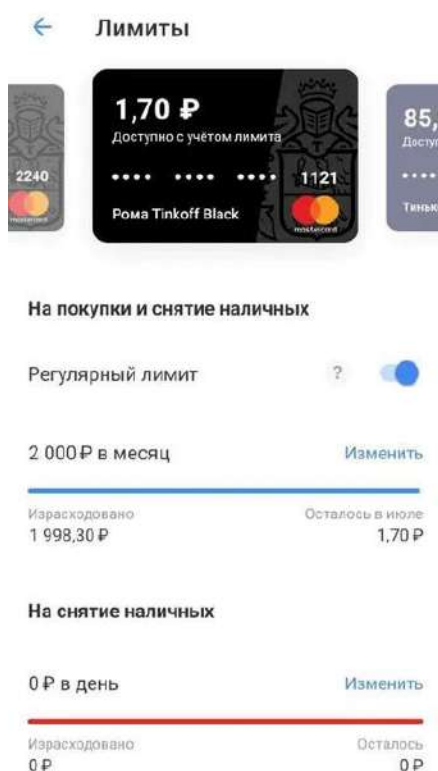
Техподдержка
банков не общается
через WhatsApp

Банки Казахстана
не звонят с номеров
других стран

ПРОГРАММЫ И ТЕХНИКА ДЛЯ ЗАЩИТЫ

Специальные технические средства и программы помогают защитить пожилых людей. Самое эффективное средство – обычный мобильный телефон. Средство, при помощи которого совершают мошенничество, можно использовать и для защиты от него. Чем чаще вы звоните родственникам и чем больше знаете о них, тем меньше вероятность, что они попадут в беду. Но есть еще удобные мобильные приложения, сигнализации и видеоглазки.

Приложения банков и мобильных операторов можно установить на свой смартфон (например, приложение «Т-Мобайл» от Т-Банка). Так вы будете контролировать траты пожилого родственника и фиксировать звонки с незнакомых номеров. Если пожилая бабушка звонила только подругам и родственникам, а потом стала часто набирать номера телефонов неизвестных людей, стоит насторожиться.



В приложениях многих банков можно установить лимит на платежи в течение месяца. Если понадобится, его легко можно увеличить в любой момент

Автономную GSM-сигнализацию можно установить и настроить самостоятельно. В комплекте идут датчики открытия

двери, веб-камера или брелок с тревожной кнопкой. В сигнализацию ставят сим-карту и задают номера родственников. Когда срабатывает датчик или кнопка, по этим номерам идет звонок.

Датчики будут срабатывать каждый раз, когда пожилой человек откроет дверь. Убедиться, что к бабушке просто пришла подруга, поможет веб-камера с передачей звука. Если увидите мошенников, позвоните бабушке и вызовите полицию.

Еще одно полезное устройство – брелок с тревожной кнопкой. Пожилой родственник сможет нажимать его каждый раз, когда к нему стучатся посторонние. Он подействует, даже если человек находится в подъезде или на улице, в 10-15 метрах от квартиры. И поможет, если ему станет плохо: проще нажать одну кнопку на брелоке, чем звонить вам по мобильному.

Видеоглазок фотографирует посетителей или снимает их на видео. Он выполняет также функции дверного звонка, а фотографию посетителя может отправлять вам на телефон (если подключен к Интернету через Wi-Fi).

В ЗАВЕРШЕНИЕ...



Если Вам звонят с неизвестного номера, и Вы понимаете, что это не Ваши близкие, – **КЛАДИТЕ ТРУБКУ!**



Если Вам предлагают продиктовать данные банковской карты, пароли, коды из СМС, перевести деньги на «безопасный счет», представляются сотрудниками банка, полиции, ФСБ, пугают взломом Госуслуг – **КЛАДИТЕ ТРУБКУ!**



Если Вас уговаривают заключить «подозрительный» договор в торговом центре, приглашают пройти обследование прямо сейчас быстро и недорого, предлагают огромные скидки и акции – **ЗАКАНЧИВАЙТЕ РАЗГОВОР И УХОДИТЕ!**



Не принимайте поспешных решений, не делайте ничего, не посоветовавшись с близкими!

ПОЛЕЗНЫЕ ССЫЛКИ

1. Интернет-ресурс Департамента региональной безопасности ХМАО – Югры: <https://deprb.admhmao.ru/profilaktika-moshennichestva/>

2. Интернет-ресурсы Банка России, Минцифры России, МВД России, финансово-кредитных учреждений, операторов связи и компаний, осуществляющих деятельность в сфере информационной безопасности, содержащих информационно-разъяснительные материалы по профилактике дистанционных преступлений:

МВД России:

https://мвд.рф/Videoarhiv/Socialnaja_reklama

<https://мвд.рф/mvd/structure1/Upravlenija/убк>

https://t.me/cyberpolice_rus

Банк России:

https://cbr.ru/protection_rights/finprosvet

Банк России г. Тюмень

https://disk.yandex.ru/d/aE-X_tMBixtXLg

<https://disk.yandex.ru/d/Xn5YAs2ItvY5sw>

Минцифры России:

<https://www.gosuslugi.ru/cybersecurity>

<https://киберзож.рф/>

<https://выучисвоюроль.рф>

<https://готовкцифре.рф>

3. Интернет-ресурсы финансово-кредитных учреждений, операторов связи и компаний, осуществляющих деятельность в сфере информационной безопасности:

<https://www.sberbank.ru/ru/person/kibrary>

<https://kaspersky.ru/resource-center>

<https://kids.kaspersky.ru/>

<https://rocit.ru>

4. Памятки по профилактике мошенничества <https://clck.ru/3ErjQC> (ссылку необходимо копировать и вставить в поисковую строку браузера)

5. Благотворительный фонд помощи пожилым людям и инвалидам «Старость в радость» https://starikam.org/news/gor_liniya/

ВАЖНЫЕ ТЕЛЕФОНЫ

Общий телефон МЧС

112

Социальная защита

Поликлиника

Управляющая компания/ЖЭК

Пенсионный фонд

Участковый (полиция)

Районная газовая служба

Аварийная служба

Банк

Телефон горячей линии
помощи пожилым людям

+7 (985) 862-95-02

с 10 до 18 по рабочим дням
(звонок платный, по тарифу вашего оператора, поэтому достаточно
набрать номер, услышать гудок и положить трубку - координатор
перезвонит вам и разговор будет бесплатным)



Распечатайте и запишите сюда все необходимые номера, а также внесите их в список контактов мобильного телефона!

Примечание: указанный номер принадлежит благотворительному фонду «Старость в радость», который помогает одиноким, малоимущим гражданам пожилого возраста и инвалидам по всей России <https://starikam.org/>.