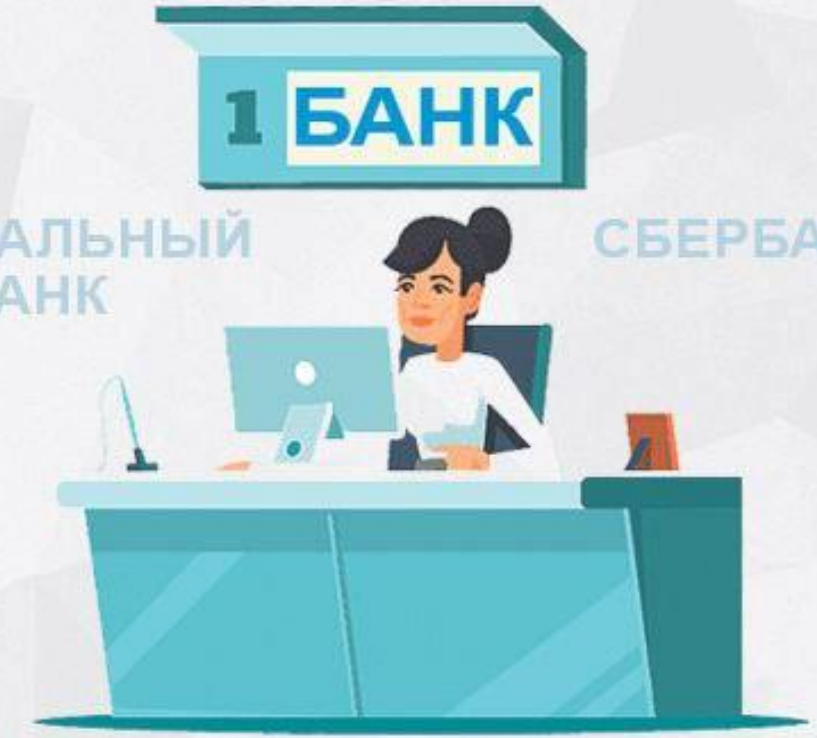
КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

УМВД России по Оренбургской области

Начальник Управления по борьбе с киберпреступлениями

Емельяненко Владимир Владимирович

КЕМ ПРЕДСТАВЛЯЮТСЯ МОШЕННИКИ



ЦЕНТРАЛЬНЫЙ БАНК

СБЕРБАНК

СОТРУДНИКАМИ БАНКА

МВД

ПРОКУРАТУРА

ФСБ

ФСИН

ПОЛИЦИЯ

СЛЕДСТВЕННЫЙ КОМИТЕТ

СОТРУДНИКАМИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

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**.

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.

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.

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**.

«Идут следственные действия, помогите задержать мошенников и не разглашайте информацию»

Работники правоохранительных органов не проводят процессуальные действия по телефону, не запрашивают финансовые данные и не предлагают поучаствовать в задержании мошенников.

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 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

ПРИ ЗВОНКЕ ОТ «СОТРУДНИКА БАНКА»:

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

(вас торопят? задумайтесь!!!)

3

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!

4

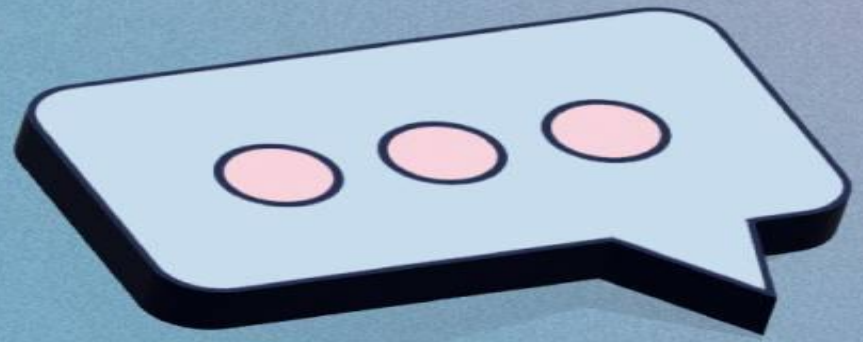
ВАЖНО ЗНАТЬ:

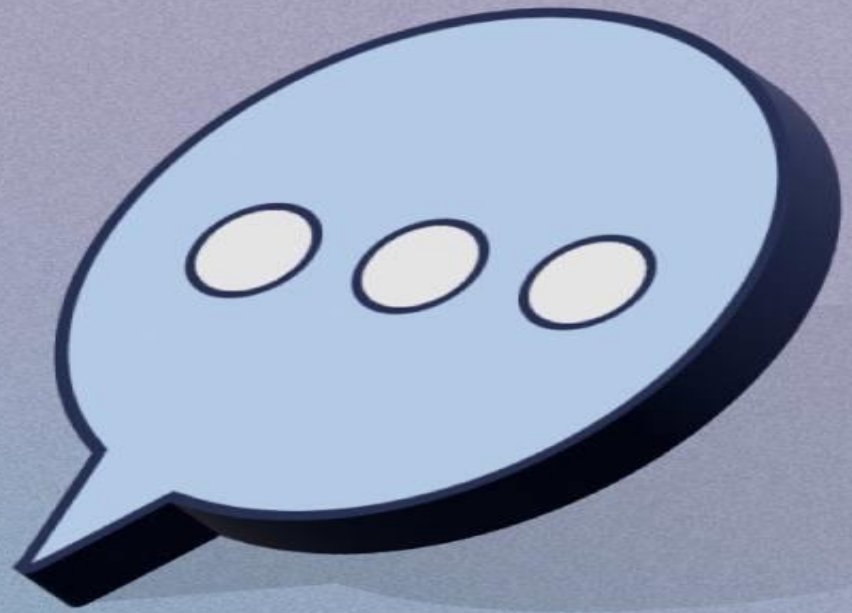
Настоящие сотрудники правоохранительных органов не привлекают граждан к содействию путем телефонных звонков или по видеосвязи.

3

Как распознать мошенника?

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





«Оформлена заявка на кредит»

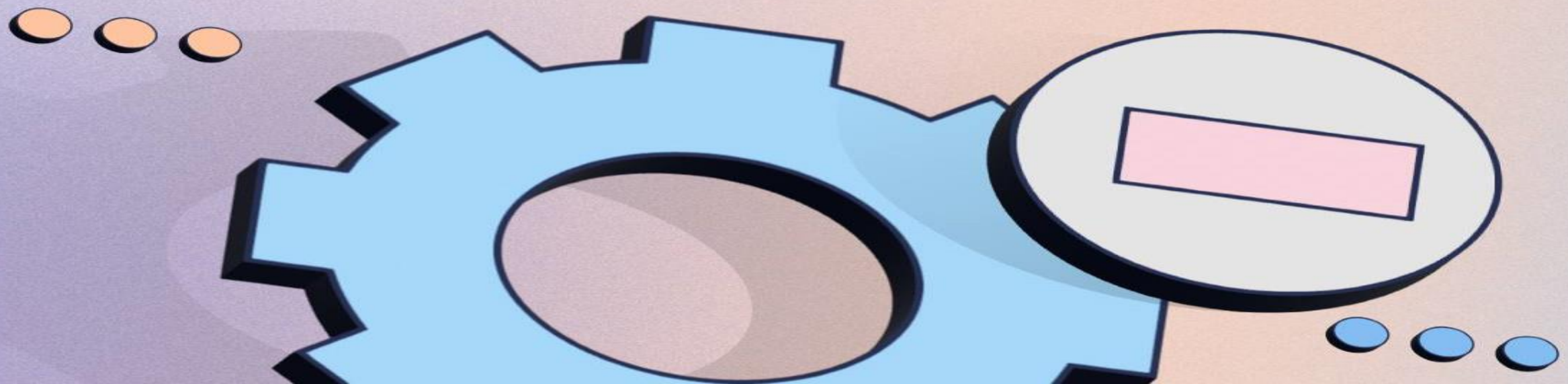
Если вы не оставляли заявку, а вам сообщают о предварительно одобренном кредите, то просто кладите трубку. Не продолжайте разговор – иначе, сказав лишнего, вы точно поможете мошенникам оформить на вас кредит и похитить деньги.

«Сотрудник Центробанка»

Настоящие работники Банка России не звонят и не пишут гражданам для совершения каких-либо банковских операций. Так поступают лжесотрудники мегарегулятора.

«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.



«Истекает срок действия сим-карты»

Не сомневайтесь, вы разговариваете с мошенником: у сим-карты мобильного оператора нет срока годности и она не нуждается в замене по этой причине.

«Продиктуйте код из СМС-сообщения»

Код из СМС – это аналог вашей собственноручной подписи. Его никогда и никому нельзя сообщать или пересылать.

«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.

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!

НЕ СТАНЬ ЖЕРТВОЙ ОБМАНА!

Подписывайся чтобы быть в курсе
и не попасть на уловки мошенников

@CYBERPOLICE_RUS

Запомни:

1. **ТОЛЬКО** мошенники звонят в мессенджерах.
2. Центробанк **НЕ ЗВОНИТ** гражданам.
3. Позвонили из твоего банка? - перезвони туда сам по номеру, указанному **НА ПЛАСТИКОВОЙ КАРТЕ.**
4. Позвонили из полиции? - перезвони туда сам **ПО НОМЕРУ** 112.

Сомневаешься? - ПОВЕСЬ ТРУБКУ!!!

Не забывай об этом и передай другим!

МВД РОССИИ ПРЕДУПРЕЖДАЕТ!

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

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!

Кража аккаунтов мессенджеров WhatsApp и Telegram

Как это работает: **Взлом аккаунтов осуществляется посредством «веерной рассылки» сообщений с просьбой проголосовать в конкурсе и ссылкой для перехода на форму голосования. При переходе по ссылке происходит перенаправление на сайт, где размещается краткая информация о конкурсе. На данном интернет-ресурсе представлены кандидаты голосования и кнопка «Перейти к голосованию», которая ведёт на страницу, где предлагается ввести данные от аккаунта мессенджера.**

Кража аккаунтов мессенджеров WhatsApp и Telegram

Совет: **Не переходите по сомнительным ссылкам, а если задумались это сделать — сначала позвоните тому, кто Вас об этом попросил. Предупредите своих родных и близких о случае «взлома» Вашего аккаунта и необходимости перепроверять сомнительную информацию.**

Кража аккаунтов мессенджеров WhatsApp и Telegram

Последствия: **При введении необходимых данных Вы фактически предоставляете доступ к своему аккаунту, завладев которым злоумышленники смогут не только рассылать сообщения от Вашего имени, но и видеть переписки, вложения и другую информацию, что в некоторых случаях может обернуться шантажом и вымогательством.**

Кража аккаунтов мессенджеров WhatsApp и Telegram

Совет как себя обезопасить: **Подключите двухфакторную аутентификацию, требующую наличия двух независимых способов подтверждения легитимности пользователя.**

При этом желательно использовать для входа в аккаунт два или более факторов, которые должны быть независимыми друг от друга, что усиливает защиту учётной записи.

ПРЕДУПРЕЖДЁН - ЗНАЧИТ ВООРУЖЁН!

К ВАМ ОБРАТИЛСЯ ЧЕРЕЗ СОЦСЕТИ СТАРЫЙ ПРИЯТЕЛЬ С ПРОСЬБОЙ ОДОЛЖИТЬ ПАРУ ТЫСЯЧ?

ВПОЛНЕ ВЕРОЯТНО, ЧТО ЭТО МОШЕННИКИ !

ПРЕДУПРЕЖДЁН - ЗНАЧИТ ВООРУЖЁН!

Злоумышленник может получить доступ к странице вашего друга и от его имени попросить:

- одолжить денег
- предоставить реквизиты банковских карт
- перейти по сомнительной ссылке

*WhatsApp (принадлежит Meta, деятельность которой признана экстремистской и запрещена в России)

ПРЕДУПРЕЖДЁН - ЗНАЧИТ ВООРУЖЁН!

Некоторые граждане осуществляют необдуманные финансовые операции и переводят деньги на указанные им номера и счета, в результате чего становятся жертвами мошенников

ПРЕДУПРЕЖДЁН - ЗНАЧИТ ВООРУЖЁН!

Не поленитесь!
Перепроверьте информацию,
позвонив дорогому вам человеку,
чтобы убедиться
в необходимости осуществления
финансовой операции

Заодно узнаете, как у него дела!

НЕ СТАНЬ ЖЕРТВОЙ ОБМАНА!

Запомни!

1. **ТОЛЬКО** мошенники рассылают в мессенджерах просьбы проголосовать **В КОНКУРСАХ!**
2. **НЕ ПЕРЕХОДИ** по неизвестным ссылкам! Не дай "угнать" свой аккаунт!
3. Пришло сообщение от родственника или знакомого, что ему надо перевести деньги? **ПЕРЕЗВОНИ ЕМУ И УБЕДИСЬ В ЭТОМ!**
4. Сомневаешься? – **ПОЗВОНИ 112.**

Сообщи родителям об этих простых вещах!

Не забывай об этом и передай другим!

@CYBERPOLICE_RUS

КАК ЗАЩИТИТЬ СВОИ ГАДЖЕТЫ ОТ ВИРУСОВ

ВИРУСЫ:

- открывают удаленный доступ к вашему устройству
- крадут логины и пароли от онлайн- и мобильного банка
- перехватывают секретные коды из сообщений

Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов

КАК ПОНЯТЬ, ЧТО УСТРОЙСТВО ЗАРАЖЕНО?

- Зависает, перезагружается или отключается
- Само завершает работу приложений
- Показывает всплывающие окна
- Теряет объем памяти

ЧТО ДЕЛАТЬ, ЕСЛИ НА УСТРОЙСТВЕ ВИРУС?

- **Позвоните в банк** и попросите заблокировать доступ к онлайн- и мобильному банку и все карты, которые использовали на устройстве
- **Обратитесь в сервисный центр**, чтобы вылечить гаджет
- **Перевыпустите карты, смените логин и пароль** от онлайн-банка и заново установите банковское приложение

КАК ЗАЩИТИТЬ УСТРОЙСТВО ОТ ВИРУСОВ?

- **Используйте антивирус** и регулярно его обновляйте
- **Не переходите по ссылкам** от незнакомцев, не устанавливайте программы по их просьбе и не используйте чужие флешки
- Скачивайте приложения **только из проверенных источников**
- **Обновляйте** операционную систему устройства
- **Избегайте** общедоступных Wi-Fi-сетей

Все мы в душе немного «шопоголики»:
кто-то выбирает новые туфельки, кто-то запчасти для любимого автотранспорта, кто-то вкусненькое или что-нибудь ещё...

… а кто-то выбирает доверчивых «шопоголиков» и забирает у них персональные данные и денежные средства!

Однако и в этой ситуации можно принять самые простые меры, которые помогут Вам не стать тем самым «выбором» злоумышленников!

1. Для покупок в сети «Интернет» заведите себе отдельную карту, на которую можете переводить необходимое количество денежных средств.

Такую карту можно как выпустить в банке в «пластиковом» виде, так и оформить виртуально (сведения о ней будут находиться в Вашем личном кабинете мобильного-банка).

Особо продвинутые пользователи могут оформить себе «электронный кошелёк» - его то Вы уж точно не сможете потерять.

2. По возможности используйте двухфакторную систему аутентификации. Она позволит Вам осуществлять контроль за входом на сайт или в приложение.

3. Всё большую популярность приобретают такие виды оплат, как: по «Qr-коду», через «Систему быстрых платежей» и посредством «Мобильного ID», однако их использование целесообразно только с соблюдением общих правил и принципов поведения в цифровой среде.

4. Если Вы решили совершить «онлайн шоппинг», в том числе дорогостоящих вещей — сделайте это по надёжному каналу связи, используя мобильный-интернет Вашего оператора связи или домашний «Wi-Fi».

Если же необходимо что-то срочно приобрести, то постарайтесь не использовать бесплатную общедоступную сеть «Wi-Fi» и VPN-сервис. Указанные каналы связи зачастую используются злоумышленниками для получения Ваших персональных данных и денежных средств.

5. Не переходите на сторонние ссылки, не скачивайте никаких новых и дополнительных приложений, а также не договаривайтесь о переходе для дальнейшего общения на сторонние ресурсы (в мессенджеры) все действия по покупке товара должны осуществляться на одном ресурсе. Если вам предлагают совершить вышеуказанные действия, то стоит задуматься об истинных намерениях «продавца».

6. При совершении покупок обязательно обращайте внимание на название «магазина» и правильность его написания в адресной строке браузера.

Зачастую злоумышленники намеренно допускают ошибку в написании (другая буква или знак препинания/пробел), которую невнимательный пользователь обязательно пропустит.

Вас обязательно должен насторожить адрес состоящий из хаотичного набора символов и знаков — вероятнее всего это «фишинговый» ресурс.

Кроме того, обращайте внимание на оформление сайта: отсутствие разделов, наличие различных ошибок, неактуальная информация и иные моменты, которые должны насторожить Вас.

ЛОВУШКИ ВИРТУАЛЬНОГО МИРА

ЛЁГКИЙ ЗАРАБОТОК

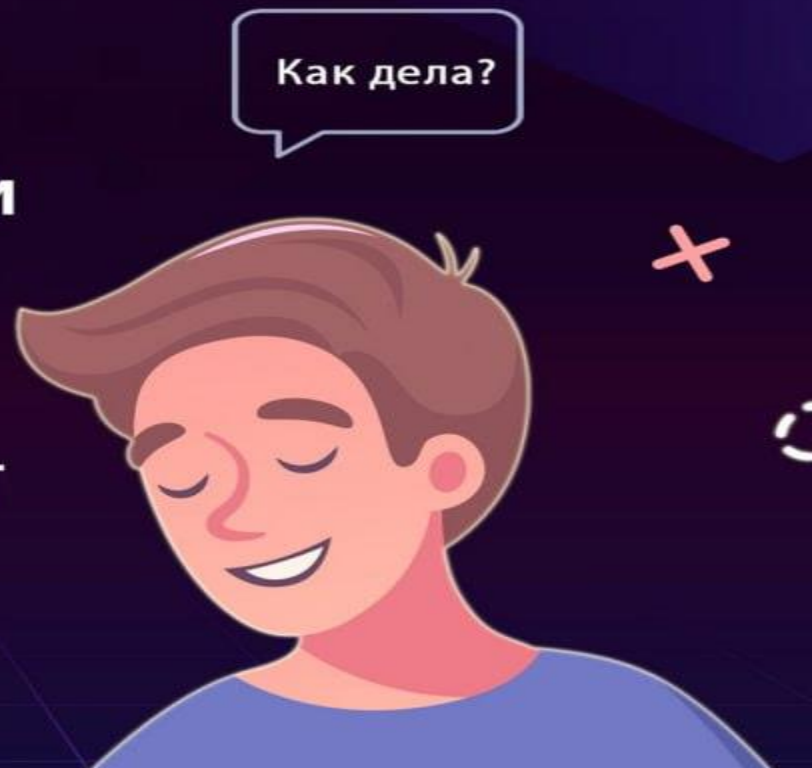
Незнакомец связывается с ребёнком в любом из мессенджеров и предлагает заработать путем **просмотра видеороликов** известных блогеров. Далее злоумышленник **отправляет ссылку и просит ввести банковские данные** одного из родителей, а также код из смс-уведомления, пояснив, что в дальнейшем по этим реквизитам будет переводить деньги

ДОПОЛНЕНИЯ ДЛЯ ОНЛАЙН-ИГР

Мошенники заманивают несовершеннолетних пользователей онлайн-игр **низкими ценами и «уникальными акциями» на различные девайсы для своего виртуального мира,** чтобы быть наравне с лидирующими игроками. Для покупки усовершенствующих дополнений отправляют ссылку, перейдя по которой просят ввести данные банковской карты

SMS ОТ ДРУГА

Киберпреступники взламывают аккаунт друга в соцсетях, а затем от его имени присылают сообщение. Начинают разговор с банального «как дела?» и практически сразу переходят к просьбе о помощи и просят в долг. Или со словами «Лови фотки со дня рождения!» вместо ссылки на фотографии присылают вредоносный вирус, который крадет с гаджета персональные данные, логины и пароли



ВЫИГРЫШ В КОНКУРСЕ

Аферисты рассылают сообщения в социальных сетях или отмечают в комментариях под постом с розыгрышем, где **сообщают о неожиданном выигрыше.** Но затем за доставку «приза» или какие-то другие дополнительные услуги школьника **просят оплатить небольшую комиссию**

ВАЖНО!

- Не переходите по неизвестным ссылкам и не сообщайте незнакомцам данные банковских карт и коды-подтверждения из смс-сообщений

- Прежде чем выполнить всё, о чем просит «приятель» в соцсетях, перезвоните ему и уточните, действительно ли нужна помощь

- Когда для получения приза организаторы конкурса просят что-либо оплатить, это повод насторожиться. Убедитесь, что это не мошенники: почитайте отзывы в Интернете, новости (вдруг они уже были замечены в обманах)

- **Если у ребёнка имеется собственная банковская карта,** то не стоит переводить на неё огромные деньги. Кроме того, можно ограничить суммы списаний или количество операций по карте в день, чтобы мошенникам не удалось украсть с нее все сбережения разом

- **Подключите СМС или push-оповещения** ко всем банковским картам, так вы сразу заметите подозрительные покупки


ДЕТЕЙ
УЧАТ
НЕ ОТКРЫВАТЬ
НЕИЗВЕСТНЫМ!
ВЗРОСЛЫХ
НУЖНО
УЧИТЬ
НЕ РАЗГОВАРИВАТЬ
ПО ТЕЛЕФОНУ
С НЕИЗВЕСТНЫМИ!

НАПИСАЛ ТЕБЕ ЗНАКОМЫЙ,
ПОПРОСИЛ ЗАНЯТЬ ДЕНЬЖАТ?
ПОЗВОНИ ЕМУ СНАЧАЛА,
ИЛИ БУДЕШЬ ТЫ НЕ РАД!
ТАК КАК ВСЕ ТВОИ ФИНАНСЫ,
УЛЕТЯТ ВО ВРАЖЬИ МАССЫ!

ПОЗВОНИЛИ С СОТОВОЙ КОМПАНИИ, СКАЗАЛИ ЗАКОНЧИЛСЯ ДОГОВОР? СБРОСЬ! ЭТО МОШЕННИКИ!

ТОВАРИЩ, ПОМНИ!

Твои финансы
целы,
пока ты сам
не предоставил
к ним доступ!

Любой, звонивший
с номера,
не записанного
в телефонной книге –
потенциальный
мошенник

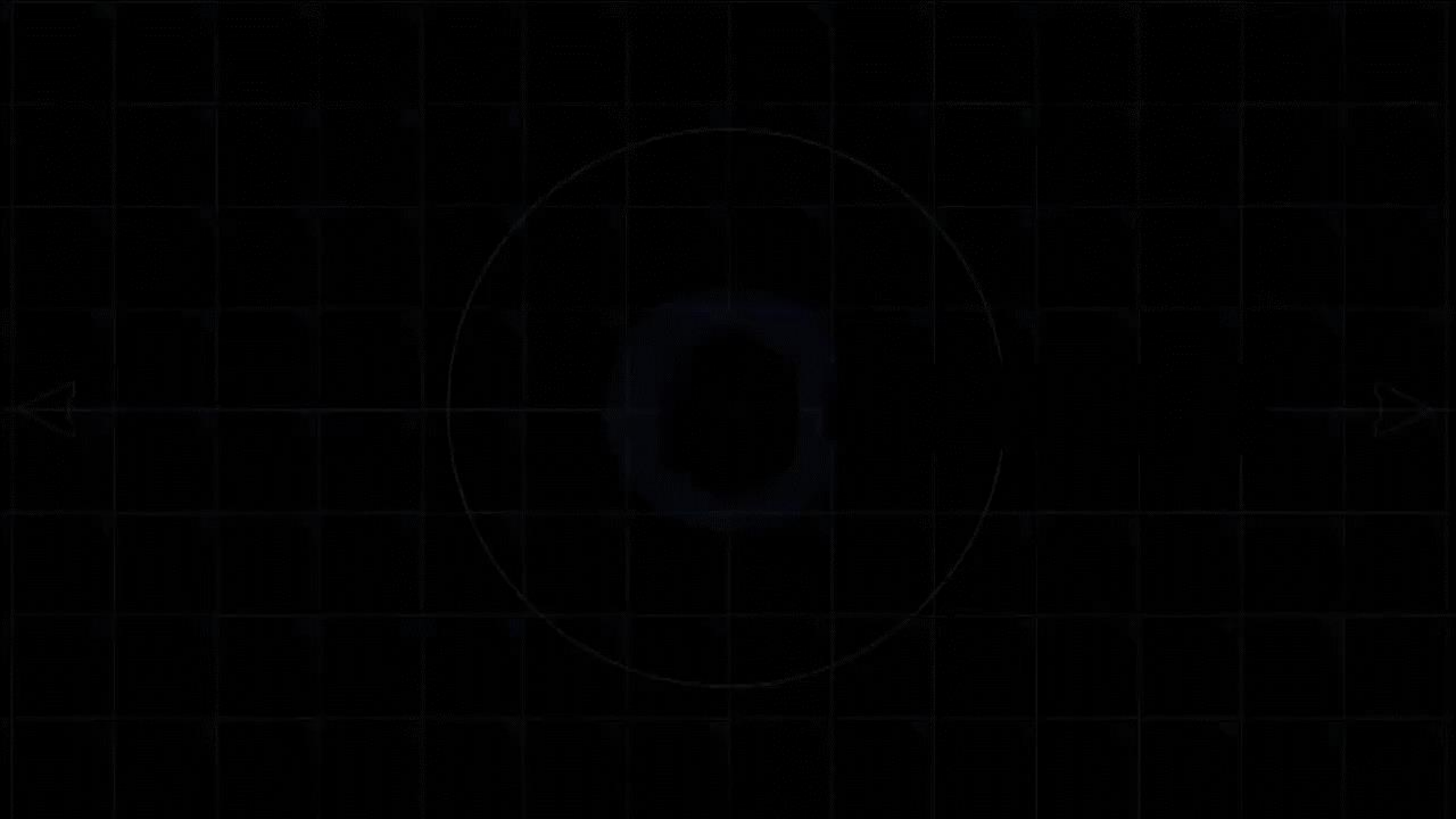
ХОЧЕШЬ ЛУЧШИМ ИНВЕСТОРОМ СТАТЬ?
НЕ НУЖНО НИКОМУ СВОИ ДЕНЬГИ ДОВЕРЯТЬ!
ЛУЧШИЙ ИНВЕСТОР – СБЕРЕГАТЕЛЬНОЙ СЧЁТ,

ВСЁ ОСТАЛЬНОЕ ОБМАН
И ТЫ БАНКРОТ!

Прежде чем товар оплатить – убедись в его наличии, соответствии и качестве!

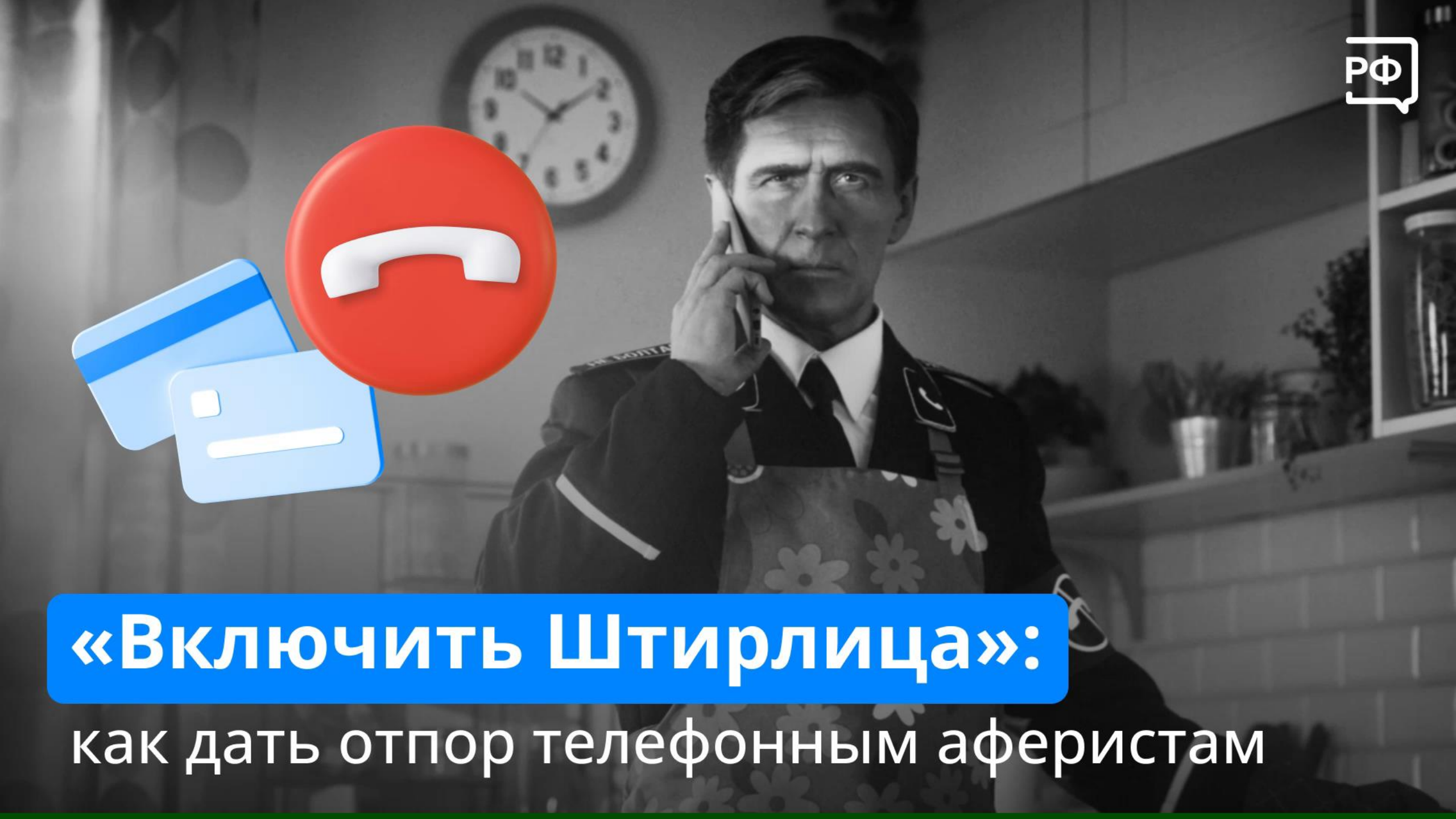
ПОКУПАЙТЕ ТОВАРЫ ТОЛЬКО У ПРОВЕРЕННОГО ПРОДАВЦА!


ВАМ ЗВОНЯТ С НЕЗНАКОМОГО НОМЕРА?



#ПРЕДУПРЕЖДЕНЗНАЧИТВООРУЖЁН

КАК УБЕРЕЧЬ ОТ МОШЕННИКОВ СВОИ ДЕНЬГИ НА БАНКОВСКОЙ КАРТЕ



«Включить Штирлица»:

как дать отпор телефонным аферистам

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

СПАСИБО ЗА ВНИМАНИЕ!

Начальник Управления по борьбе с киберпреступлениями

Емельяненко Владимир Владимирович