ПАМЯТКА: «ЗАЩИТИ СЕБЯ ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ»

Bonpoc: Вам позвонил незнакомец, представился сотрудником банка или госучреждения и просит срочно совершить действия с картой или деньгами. Что делать?

Ваш главный принцип: НИКАКОЙ ПАНИКИ И НИКАКОЙ ПОСПЕШНОСТИ. Мошенники всегда создают ощущение срочности и угрозы, чтобы вы отключили логику.

Порядок действий: «СТОП. ПРОВЕРЬ. НЕ ВЕРИШЬ — ПЕРЕЗВОНИ»

1. ШАГ: СТОП — НИЧЕГО НЕ ГОВОРИТЕ И НИЧЕГО НЕ ДЕЛАЙТЕ

НЕ НАЗЫВАЙТЕ ни при каких обстоятельствах:

- Номер карты
- Срок действия карты
- CVC/CVV-код (3 цифры на обороте)
- Пароли и коды из SMS (их нельзя никому сообщать, даже «сотруднику банка»).

НЕ ПЕРЕХОДИТЕ по ссылкам, присланным в SMS или мессенджерах.

НЕ УСТАНАВЛИВАЙТЕ никакие приложения по их просьбе (AnyDesk, TeamViewer и т.д.).

НЕ ПЕРЕВОДИТЕ деньги на «безопасные счета», «для проверки» или под любым другим предлогом.

2. ШАГ: ПРОВЕРЬ — ЗАДАЙТЕ КОНТРОЛЬНЫЕ ВОПРОСЫ

- «Из какого вы отделения банка? Назовите его точный адрес».
- «Назовите мои полные ФИО и номер договора/счета».
- «Какой госорган вы представляете? На каком основании запрашиваете информацию?»

Легитимные сотрудники всегда имеют на руках ваши данные. Мошенники — нет.

3. ШАГ: НЕ ВЕРИШЬ — ПЕРЕЗВОНИ САМ

НЕ ВЕРЬТЕ звонящему. Мошенники могут подделать номер (спуфинг), и на вашем телефоне будет светиться якобы настоящий номер банка.

ПОЛОЖИТЕ ТРУБКУ.

САМОСТОЯТЕЛЬНО найдите официальный телефон вашего банка (на обороте своей карты или на официальном сайте) и перезвоните туда.

Спросите у оператора: «В вашей организации работает такой-то сотрудник? Поступали ли ко мне предупреждения о подозрительных операциях?»

Для госучреждений — найдите их контактный телефон на официальном портале (например, gosuslugi.ru) и перезвоните.

Типичные уловки мошенников (чего НЕ БЫВАЕТ на самом деле):

«Блокировка карты из-за взлома». Банк никогда не звонит с предложением перевести деньги на «безопасный счет». Для блокировки карты достаточно позвонить в банк самому.

«Ошибочный перевод денег на вашу карту». Вас просят «вернуть» эти деньги, а на самом деле вы отправляете им свои собственные.

«Подозрительные покупки/займы». Цель — убедить вас установить программу для «безопасности», которая на самом деле дает мошенникам доступ к вашему телефону и банковским приложениям.

«Проблемы с соцвыплатами, налогами, штрафами». Настоящие госорганы рассылают уведомления почтой или через «Госуслуги», а не решают финансовые вопросы по телефону.

Краткая шпаргалка-напоминалка:

ЧТО ПРОСЯТ СДЕЛАТЬ	ВАШИ ПРАВИЛЬНЫЕ ДЕЙСТВИЯ	
Назвать данные карты	ВЕЖЛИВО ПОЛОЖИТЬ ТРУБКУ. Никогда и никому не сообщать эти данные.	
Продиктовать код из SMS	НЕ СООБЩАТЬ НИКОГДА. Это код для подтверждения операций, его знаете только вы и банк.	
Перейти по ссылке	НЕ ПЕРЕХОДИТЬ. Это фишинговая ссылка для кражи данных.	
Перевести деньги	НЕ ПЕРЕВОДИТЬ. Ни на какой «безопасный счет», «для проверки» или родственникам.	
Установить программу	ОТКАЗАТЬСЯ. Это программы для удаленного доступа к вашему устройству.	

ПАМЯТКА: «ВАМ ЗВОНИТ "СОТРУДНИК" СИЛОВОГО ВЕДОМСТВА»

Вопрос: Позвонивший представился сотрудником полиции, ФСБ, Следственного комитета или прокуратуры. Он сообщил, что с Вашего счета кто-то переводит деньги гражданину недружественной страны. Что будете делать? Ваша первая и главная реакция: СОСРЕДОТОЧЬТЕСЬ И НЕ ПОДДАВАЙТЕСЬ ПАНИКЕ. Мошенники используют авторитет госорганов, чтобы запугать вас и полностью отключить критическое мышление.

Порядок действий: «ПАУЗА. НЕ ВЕРЮ. ПЕРЕЗВОНЮ»

ШАГ 1: ПАУЗА — ВЗДОХНИТЕ И ВЗЯТИЕ ПОД КОНТРОЛЬ

- Не подтверждайте никаких данных о себе (ФИО, номер паспорта, адрес).
- Не поддавайтесь на провокации. Вас могут обвинять в чем угодно «отмывании денег», «финансировании терроризма». Цель одна вызвать у вас чувство страха и вины.

Помните: Ни один настоящий следователь или оперативник не будет вести следственные действия по телефону, особенно связанные с переводами денег.

ШАГ 2: НЕ ВЕРЮ — ЗАДАЙТЕ ВОПРОСЫ ДЛЯ ПРОВЕРКИ

Сохраняя спокойный и вежливый тон, задайте уточняющие вопросы:

- 1. «Назовите, пожалуйста, ваше полное ФИО, должность, звание и название отделения, в котором вы работаете?»
- 2. «Под каким номером находится ваше дело/проверка? Я его запишу.»
- 3. «На каком основании вы проводите проверку по телефону, а не через официальный запрос?»
- 4. Мошенники часто теряются, начинают грубить или давить еще сильнее, требуя «не мешать работе».

ШАГ 3: ПЕРЕЗВОНЮ — ПРЕРВИТЕ КОНТАКТ И ПЕРЕЗВОНИТЕ САМИ

- 1. Вежливо положите трубку, не вступая в дальнейшие споры. Например: «Я не буду продолжать этот разговор по телефону. Все вопросы решим при личном визите в ваше учреждение».
- 2. НЕ ПЕРЕЗВАНИВАЙТЕ на номер, с которого вам звонили. Мошенники используют подмену номера (спуфинг).
- 3. **САМОСТОЯТЕЛЬНО** найдите официальный телефон окружного отдела полиции, управления ФСБ или прокуратуры в интернете (например, на сайте genproc.gov.ru для прокуратуры) и позвоните туда.
- 4. **Спросите:** «Я получил подозрительный звонок от человека, представившегося вашим сотрудником. Проверьте, пожалуйста, работает ли у вас такой человек и ведется ли такое дело?»
- 5. В 99,9% случаев вам ответят, что звонок был мошенническим.

Чего НИКОГДА не станут делать настоящие сотрудники:

- **Х Сообщать о подозрениях** в серьезных преступлениях по телефону.
- 🗙 Требовать срочно «обеспечить сохранность средств» путем перевода их на любой другой счет.
- 🗙 **Просить сообщить данные** банковских карт, пароли из SMS, коды доступа к банковским приложениям.
- **X Требовать установить на телефон** какие-либо приложения (например, для «безопасного соединения» или «слежки»).
- ★ Присылать такси или курьера для изъятия вашей банковской карты, наличных или ценных вещей «на экспертизу».

Финансовая цель мошенника: Убедить вас, что ваши деньги находятся под угрозой, и единственный способ их спасти — это перевести на «защищенный», «временный» или «специальный» счет в другом банке. На самом деле этот счет будет принадлежать мошенникам.

Краткая шпаргалка для экстренной ситуации:

ЧТО ГОВОРИТ МОШЕННИК	ЧТО ДЕЛАТЬ ВАМ
«Вы под следствием! Ваш счет используют преступники!»	Взять паузу, не поддаваться панике. Помните: это стандартный сценарий запугивания.
«Чтобы спасти деньги, переведите их на безопасный счет».	НИКОГДА И НИКУДА не переводить. Это конечная цель всего звонка.
«Сообщите данные карты и коды из SMS для проверки».	НЕ СООБЩАТЬ. Настоящий сотрудник никогда не попросит об этом. Положить трубку.
«Это государственная тайна. Никому не звоните и не говорите».	НАРУШИТЬ ЭТО ТРЕБОВАНИЕ. Обязательно посоветуйтесь с родными и перезвоните в ведомство по официальному номеру.
«К вам уже выехала группа для задержания».	НЕ ВЕРИТЬ. Это давление. Пока вы разговариваете с ними по телефону, никакая «группа» не приедет.

ПАМЯТКА: «ПОКУПКА НА "АВИТО" У ИНОГОРОДНЕГО ПРОДАВЦА»

Bonpoc: Вы собираетесь купить подержанную вещь на «Авито» у иногороднего продавца. Он предлагает отправить товар транспортной компанией, но предварительно Вам нужно его оплатить. Также продавец просит перевести коммуникацию в WhatsApp. Вы согласитесь?

Короткий ответ: НЕТ, НЕ СОГЛАШАЙТЕСЬ. Это классическая схема мошенничества.

Почему это ловушка? Разберем по пунктам:

- «Предоплата перед отправкой» это главный признак обмана.
- Мошенник создает иллюзию выгодной сделки и доверия, но как только вы переведете деньги (даже часть), он просто исчезнет.
- Вы не получите ни товар, ни деньги назад.
- Просьба уйти в WhatsApp/Telegram/другой мессенджер это способ вывести вас из-под защиты «Авито».
- В мессенджерах нет истории сделки, и администрация «Авито» не сможет помочь вам в случае конфликта и принять мошенника к ответственству.
- Мошеннику так проще вас запутать и оказать психологическое давление.
- Использование имени известной транспортной компании (СДЭК, Boxberry и др.) это элемент легенды.
- Мошенник может прислать вам поддельные квитанции, ссылки на фейковые сайты или даже сказать, что «курьер уже ждет оплаты, чтобы выдать товар». Это неправда.

Правильный план действий: «ТРИ ПРАВИЛА БЕЗОПАСНОСТИ»

ПРАВИЛО 1: Никаких предоплат незнакомым людям!

- Все расчеты должны проводиться только через официальные способы оплаты на «Авито» (например, «Авито.Доставка»)
- Либо используйте наложенный платеж при получении в отделении транспортной компании. Вы платите за товар только тогда, когда увидели его и проверили.

ПРАВИЛО 2: Вся коммуникация — только в чате «Авито»!

- Весь диалог с продавцом, обсуждение условий, фото и видео товара должны оставаться в переписке на площадке.
- Если продавец настаивает на переходе в другой мессенджер это почти стопроцентный признак мошенничества. Вежливо откажитесь и прекратите общение.

ПРАВИЛО 3: Проверяйте продавца!

- Посмотрите отзывы. У добросовестного продавца, особенно из другого города, обычно есть история и положительные отзывы от других покупателей.
- Насторожитесь, если профиль создан недавно, на нем нет фото, товаров или отзывов.
- Попросите продавца сделать фото товара с сегодняшней датой и его именем на листке бумаги. Мошенники часто используют чужие фото, и они не смогут этого выполнить.

Краткая шпаргалка: «МОЖНО vs НЕЛЬЗЯ»

√ МОЖНО и НУЖНО ДЕЛАТЬ (Безопасно)	🗙 НЕЛЬЗЯ ДЕЛАТЬ (Опасно!)
Общаться с продавцом только в чате на «Авито».	Переходить для обсуждения сделки в WhatsApp, Telegram или
	Viber.
Оформлять заказ через официальную доставку «Авито».	Переводить предоплату на карту, по номеру телефона или через
	онлайн-кошелек.
Просить у продавца дополнительные фото/видео	Верить обещаниям и поддаваться на давление и
товара через чат.	спешку («Другие покупатели уже ждут»).
Внимательно читать отзывы о продавце.	Соглашаться на «особые условия», которых нет в официальных
	правилах «Авито».
Оплачивать товар только при получении и	Переводить деньги за «страховку», «бронь» или иные
проверке (наложенный платеж).	выдуманные сборы.

Вывод: Если продавец нарушает эти правила и настаивает на предоплате и уходе из чата — просто прекратите общение и заблокируйте его. В 99% случаев вас пытаются обмануть.

ПАМЯТКА ДЛЯ ПРОДАВЦА: «ВАМ ПРЕДЛАГАЮТ ВНЕСТИ ПРЕДОПЛАТУ ЗА ТОВАР»

Bonpoc: Вы продаёте смартфон через сайт объявлений. Сразу после размещения вам звонит «покупатель». Чтобы «гарантированно» получить смартфон, он предлагает внести предоплату, но для этого нужен номер вашей карты. Согласитесь?

Короткий ответ: НЕТ, НЕ СОГЛАШАЙТЕСЬ. Это развод!

Почему это ловушка? (Схема мошенничества)

Мошенник притворяется очень заинтересованным покупателем, который действует по стандартной схеме:

- 1. **«Я готов внести предоплату прямо сейчас!»** Он создает иллюзию выгодной и быстрой сделки, чтобы вы расслабились и потеряли бдительность.
- 2. **«Мне нужен номер вашей карты, чтобы перевести деньги»** Это кажется логичным, но это первый шаг к обману.
- 3. Далее следует фраза: «Мне пришло смс от банка, нужно подтверждение. Я вам сейчас сброшу код, вы его продиктуйте» ЭТО ГЛАВНАЯ ЦЕЛЬ!

На самом деле он инициирует операцию не по переводу денег, а по взносу наличных через ваш счет или привязке вашего номера телефона к своему мобильному банку.

Код из SMS, который он просит, — это **подтверждающий пароль для списания денег с ВАШЕГО ЖЕ СЧЕТА**. Вы сами дадите ему разрешение на это.

Результат: Вместо получения предоплаты вы мгновенно теряете собственные деньги со своей же карты. Мошенник исчезает.

Правильный план действий для продавца: «ТОЛЬКО НАЛИЧНЫЕ, ТОЛЬКО ПРИ ВСТРЕЧЕ»

ПРАВИЛО 1: Никаких данных карты и кодов из SMS

- **НИКОМУ И НИКОГДА** не сообщайте номер своей банковской карты, срок действия, СVC-код и, самое главное, **коды из SMS**.
- Помните: настоящий покупатель не будет просить у вас эти данные для перевода предоплаты.

ПРАВИЛО 2: Расчет — только при личной встрече

- Самый безопасный способ это встреча в людном месте (например, у станции метро, в торговом центре), где покупатель осматривает и проверяет товар, а вы получаете оплату наличными.
- Если покупатель из другого города и настаивает на пересылке, используйте только официальные способы с наложенным платежом (например, «СДЭК» или «Почта России»). В этом случае деньги вам переведет сама транспортная компания после того, как покупатель оплатит заказ при получении.

ПРАВИЛО 3: Проверяйте «покупателя»

- Звонок сразу после размещения объявления, спешка и готовность внести предоплату без лишних вопросов это классические признаки мошенника.
- Честный покупатель всегда будет задавать вопросы о состоянии товара, торговаться и адекватно реагировать на предложение о встрече.

Краткая шпаргалка для продавца:

∜ ПРАВИЛЬНО (Безопасно)	🗙 НЕПРАВИЛЬНО (Опасно!)
Продавать товар при личной встрече с оплатой	Сообщать номер своей банковской карты, срок
наличными.	действия или CVC-код.
Для иногородних покупателей использовать	Диктовать коды из SMS-сообщений, которые
наложенный платеж через проверенные транспортные	приходят вам на телефон. Это всегда обман.
компании.	
Встречаться в людном, безопасном месте.	Верить в срочность и соглашаться на «особые
	условия» оплаты.
Требовать оплату на свой счет только через безопасные	Передавать товар курьеру, которого прислал
сервисы (например, «Авито.Доставка»).	«покупатель», до поступления денег на ваш счет.

Вывод: ваш главный принцип как продавца— «Сначала деньги, потом товар». А под «деньгами» подразумеваются только наличные в ваших руках при встрече или гарантированный перевод через официальные и защищенные сервисы. Любая просьба о ваших карточных данных или кодах из SMS— это попытка вас ограбить.

ПАМЯТКА: «ВАМ ЗВОНЯТ ИЗ "МОБИЛЬНОГО ОПЕРАТОРА"»

Bonpoc: Вам звонит человек, который представляется сотрудником мобильного оператора, и произносит фразу: «Срок действия вашей SIM-карты истек. Если хотите его продлить, назовите код из SMS, который сейчас придет». Как вы поступите?

Короткий ответ: НЕМЕДЛЕННО ПРЕРВИТЕ РАЗГОВОР. Это 100% мошенничество.

Почему это ловушка?

Срок действия SIM-карт не истекает. Это главный маркер обмана. Если ваша карта активна и на счету есть деньги, она будет работать годами.

Код из SMS — это доступ к вашему мобильному банку. Мошеннику нужен не продление SIM-карты, а одноразовый пароль для входа в приложение банка, подтверждения платежа или сброса паролей. Сообщив код, вы сами отдадите ему доступ к своим деньгам.

Цель — опустошить ваш банковский счет. Получив код, мошенник может за несколько минут привязать ваш номер к своему устройству, войти в интернет-банк и перевести все ваши сбережения.

Правильный план действий: «ПОВЕСИЛ ТРУБКУ — ПЕРЕЗВОНИЛ»

ШАГ 1: НИЧЕГО НЕ ГОВОРИТЕ, НЕ ПОДТВЕРЖДАЙТЕ, НЕ НАЗЫВАЙТЕ

- **НЕ ГОВОРИТЕ** «Да» или «Алло». Мошенники могут записать ваш голос для подтверждения операций в голосовых меню некоторых банков.
- **НЕ СООБЩАЙТЕ** никаких данных: ни кода из SMS, ни паспортных данных, ни паролей.
- Если вам уже пришел код НИ В КОЕМ СЛУЧАЕ НЕ ОЗВУЧИВАЙТЕ ЕГО.

ШАГ 2: НЕМЕДЛЕННО ПОЛОЖИТЕ ТРУБКУ

- Не вступайте в дискуссии, не пытайтесь уличить мошенника. Чем дольше вы разговариваете, тем больше у них возможностей вас запутать и уговорить.
- Просто положите трубку.

ШАГ 3: ПЕРЕЗВОНИТЕ ОПЕРАТОРУ САМОСТОЯТЕЛЬНО

- НЕ ПЕРЕЗВАНИВАЙТЕ на номер, с которого вам звонили.
- Наберите короткий официальный номер вашего оператора:

МТС: 0890 или 8-800-250-08-90 Билайн: 0611 или 8-800-700-06-11 МегаФон: 0500 или 8-800-550-05-00 Теле2: 611 или 8-800-555-06-11

• Спросите у оператора: «Мне только что звонили от вашего имени и просили сообщить код из SMS. Это вы?». Вам подтвердят, что это мошенники.

Что делать, если код из SMS вы уже назвали?

- 1. ДЕЙСТВУЙТЕ ОЧЕНЬ БЫСТРО!
- 2. НЕМЕДЛЕННО позвоните в свой банк по номеру с обратной стороны карты и заблокируйте карту.
- 3. СРАЗУ ЖЕ позвоните оператору (номера выше) и сообщите о мошенничестве. Попросите заблокировать SIM-карту, чтобы мошенник не мог получать коды.
- 4. Напишите заявление в полицию.

Краткая шпаргалка для экстренной ситуации:

√ ПРАВИЛЬНЫЕ ДЕЙСТВИЯ (Безопасно)	🗙 НЕПРАВИЛЬНЫЕ ДЕЙСТВИЯ (Опасно!)
Немедленно положить трубку, не вступая в диалог.	Сообщать коды из SMS, пароли или персональные данные.
Перезвонить оператору по официальному короткому	Подтверждать голосом любую информацию («Да»,
номеру.	«Согласен»).
Помнить: срок действия SIM-карты не истекает.	Верить в необходимость «продления» сим-карты.
Сообщить о звонке официальному оператору.	Перезванивать на номер, с которого поступил звонок.

Вывод: любой звонок, в котором у вас просят код из SMS, — это мошенничество. Ваш код — это ключ от вашего кошелька. Никогда и никому его не передавайте.

ПАМЯТКА: «ВАМ ЗВОНЯТ ИЗ "МФЦ" ПО ПОВОДУ ПОЛИСА»

Вопрос: Вам позвонил вежливый человек, который представился сотрудником МФЦ. Он сообщил, что из-за массового сбоя была нарушена привязка Вашего полиса к поликлинике. Для того, чтобы исправить ситуацию, надо перейти по ссылке, которую Вам выслали в SMS. Что вы будете делать?

Короткий ответ: НЕМЕДЛЕННО ПРЕКРАТИТЕ РАЗГОВОР. Это фишинговая атака с целью кражи ваших данных и денег.

Почему это ловушка?

- 1. МФЦ не звонит с такими уведомлениями. МФЦ (Многофункциональный центр) работает с документами и заявлениями, которые вы подаете лично. Они не занимаются массовыми звонками по поводу сбоев в привязке полисов ОМС. Этим занимаются страховые медицинские компании и территориальные фонды ОМС.
- 2. «Массовый сбой» это любимая легенда мошенников. Она создает ажиотаж и ощущение срочности, чтобы вы перестали критически мыслить.
- 3. Ссылка в SMS ведет на фишинговый сайт. Перейдя по ней, вы попадете на поддельный сайт, который выглядит как официальный портал «Госуслуги», МФЦ или страховой компании. Вам предложат «восстановить привязку», введя данные:
- Паспортные данные
- Номер полиса ОМС
- Номер СНИЛС
- Данные банковской карты («для верификации» или «компенсации»)
- Логин и пароль от «Госуслуг»

Итог: Мошенники соберут ваши персональные данные, чтобы взять кредиты на ваше имя, получить доступ к вашим счетам или продать информацию.

Правильный план действий: «ПОВЕСИЛ ТРУБКУ — ПРОВЕРИЛ САМ»

ШАГ 1: НИЧЕГО НЕ ДЕЛАЙТЕ И НЕ ПЕРЕХОДИТЕ ПО ССЫЛКЕ

НЕ ПЕРЕХОДИТЕ по ссылке в SMS.

НЕ НАЗЫВАЙТЕ звонящему никаких данных и не подтверждайте их.

НЕ УСТАНАВЛИВАЙТЕ любые приложения, которые вам могут предложить «для удаленного доступа».

ШАГ 2: НЕМЕДЛЕННО ПОЛОЖИТЕ ТРУБКУ

Не ведите диалог. Мошенники используют психологическое давление и могут казаться очень убедительными. Просто положите трубку.

ШАГ 3: ПРОВЕРЬТЕ ИНФОРМАЦИЮ САМОСТОЯТЕЛЬНО

Способ 1 (основной): Лично позвоните в вашу страховую медицинскую компацию (ее номер указан на вашем полисе ОМС). Уточните у них информацию о состоянии вашего полиса и прикреплении к поликлинике.

Способ 2: Лично обратитесь в вашу поликлинику в регистратуру или к страховому представителю и уточните, не было ли сбоев.

Способ 3: Проверьте статус прикрепления к поликлинике через официальный портал «Госуслуги» (не по присланной ссылке, а через приложение или введя адрес gosuslugi.ru вручную!).

Что делать, если вы все же перешли по ссылке и ввели данные?

- Если вы вводили данные банковской карты: Немедленно позвоните в банк по номеру с обратной стороны карты и заблокируйте ее.
- Если вы вводили пароль от «Госуслуг»: Немедленно зайдите на настоящий сайт «Госуслуги» и смените пароль. Включите двухфакторную аутентификацию.
- Если вы вводили паспортные данные и СНИЛС: Будьте предельно внимательны к звонкам и письмам. Мошенники могут попытаться оформить на вас кредит. Вы можете подать заявление в правоохранительные органы.

Краткая шпаргалка для экстренной ситуации:

√ ПРАВИЛЬНЫЕ ДЕЙСТВИЯ (Безопасно)	🗙 НЕПРАВИЛЬНЫЕ ДЕЙСТВИЯ (Опасно!)
Немедленно положить трубку.	Переходить по ссылке из SMS или сообщения в мессенджере.
Самостоятельно перезвонить в страховую компанию (номер с полиса).	Сообщать какие-либо персональные данные незнакомому человеку по телефону.
Проверить информацию через официальный портал «Госуслуги».	Устанавливать какие-либо приложения по просьбе звонящего.
Уточнить информацию в поликлинике лично.	Верить в «массовые сбои», о которых сообщают по телефону.