

Простые правила информационной гигиены

Самое простое правило недавно озвучил наш Президент: если в телефонном разговоре речь заходит о деньгах и имуществе, нужно сразу класть трубку. Действительно, это один из самых эффективных способов защиты от современных мошенников, которые неустанно совершенствуют свои преступные схемы.

РОЦИТ совместно с Управлением по борьбе с киберпреступлениями МВД России подготовил для Вас памятку. Мы в доступной форме объясняем, как распознать обман в разговоре с незнакомцами. Надеюсь, что этот буклет станет практичным инструментом, который поможет не растеряться и принять верное решение.

Борьба с телефонным мошенничеством ведется и на государственном уровне. Первый антимошеннический пакет был принят в 2025 году, а его нормы начали действовать с лета прошлого года. Мошенникам стало сложнее оформить дистанционный кредит, получить подложную SIM-карту или выдавать себя за сотрудников банков.

Но преступники быстро адаптируются. Например, сейчас активно используются нейросети, которые позволяют за несколько секунд сгенерировать фразы по образцу голоса человека или даже его видеоизображение (дипфейки). Поэтому второй пакет мер усиливает ответственность за использование нейросетей в преступных целях.

При этом не стоит забывать, что ключевым фактором защиты граждан остается информированность. Ведь одно простое действие – вовремя положить трубку – поможет вам не стать жертвой мошенников.

С уважением,

*председатель правления РОЦИТ,
первый заместитель председателя комитета
Государственной Думы РФ
по информационной политике,
информационным технологиям и связи*

Антон Горелкин

Что делать, если вас обманули?

Помните: действовать нужно сразу!

Заставили перевести деньги

1. Позвоните в банк: сообщите о мошенничестве, попросите заблокировать перевод, подайте заявление на возврат средств.
2. Подайте заявление в ближайший отдел полиции.
3. Сохраните переписки, скриншоты, звонки или любые доказательства, подтверждающие факт мошенничества.

Заразили телефон вирусом

1. Отключите устройство от интернета, чтобы не допустить распространения вируса.
2. Обратитесь в отдел полиции по месту жительства.
3. Очистите устройство самостоятельно или обратитесь к техническому специалисту.

Взломали «Госуслуги»

1. Попробуйте восстановить доступ через ссылку «Забыли пароль?».
2. Если это не помогает, обратитесь в ближайший центр обслуживания. Это может быть МФЦ, отделение банка или почты.
3. После восстановления доступа убедитесь, что в истории операций нет подозрительных действий.

Звоните – вам помогут!

Телефон горячей линии «Госуслуг»

8-800-100-70-10

Телефон полиции

102



Кладите трубку!

Как не стать жертвой телефонных мошенников



Что говорят мошенники и почему нельзя им верить

Мошенники чаще всего звонят под видом сотрудников правоохранительных органов, банков, операторов связи, управляющих компаний, госслужащих, курьеров или даже ваших родственников.



Попал в аварию, нужны деньги на лечение

Вам сообщают, что близкий человек якобы попал в плен или аварию, задержан, нуждается в срочной операции, адвокате или деньгах на «решение вопроса». Главная задача мошенников — не дать времени на проверку и заставить перевести деньги в состоянии шока. В такой ситуации нужно сразу прекратить разговор и лично связаться с родственником или другими членами семьи.



Сейчас пришлю файл, его нужно открыть

Под видом договора, фото, перерасчета или иного важного документа вам могут прислать вредоносный файл. После его открытия на устройство установится программа, которая может получить доступ к SMS, звонкам, контактам, уведомлениям и банковским приложениям. Любые файлы, программы и «обновления», полученные в мессенджере или по почте от неизвестных лиц, открывать и устанавливать нельзя.



Нужно перевести деньги на безопасный счёт

Фразы про «взлом аккаунта», «оформленную доверенность» или «сговор сотрудников банка» используются, чтобы напугать вас и заставить перевести или передать деньги мошенникам своими руками. В действительности никаких «безопасных счетов» для перевода средств не существует. Если вам сообщают об угрозе деньгам, не выполняйте указаний по телефону и сразу проверяйте информацию через ваш банк.



На ваше имя оформлена доставка посылки

Неожиданные сообщения о посылке, заказном письме, призе или подарке рассчитаны на то, что вы растеряетесь и начнете действовать, не проверяя информацию. Дальше обычно просят назвать код, перейти по ссылке или «подтвердить получение». Настоящие организации не требуют срочно сообщать коды по телефону и переводить деньги ради получения письма, посылки или выигрыша.



Вам начислили дополнительный пенсионный стаж

Сообщения о «доначисленном стаже», «новой выплате», «наборе для льготников» или иной неожиданной льготе часто используются как предлог для выманивания персональных данных и кодов подтверждения. Вас постараются убедить, что деньги или помощь уже готовы, осталось только быстро «подтвердить личность». Любые выплаты и перерасчеты нужно проверять только через официальные органы и сервисы, а не по входящему звонку.



У вас заканчивается договор с оператором связи

Мошенники часто используют бытовые и привычные поводы: продление договора связи, замену домофона, обновление данных жильцов, переоформление SIM-карты или иных услуг. Их задача — заставить поверить, что без немедленных действий вы останетесь без связи, доступа в подъезд или другой важной услуги. Запомните: нельзя сообщать коды, переходить по ссылкам и устанавливать приложения по указанию звонящего.



Вам придет SMS-сообщение с цифрами, назовите их!

Коды из SMS, push-уведомлений, а также данные паспорта, СНИЛС и других документов нельзя сообщать по телефону незнакомым лицам. Чаще всего именно с этого начинается мошенническая атака. Если у вас что-то запрашивают в срочном порядке, разговор следует прекратить и самостоятельно связаться с организацией по официальному номеру.



Вы обязаны содействовать следствию

Мошенники нередко представляются сотрудниками полиции, ФСБ, СК, прокуратуры или других ведомств и заявляют, что вы должны «содействовать операции», «выявить преступников» или «сохранить тайну следствия». Правоохранительные органы никогда не требуют переводить средства, передавать ценности или скрывать разговор от родственников.



Это срочно, делайте прямо сейчас, как я скажу!

Фразы «срочно», «осталось пять минут», «хакеры уже в системе», «действуйте немедленно» нужны только для того, чтобы отключить критическое мышление. Когда вас торопят, вы меньше проверяете факты и чаще совершаете ошибки. Поэтому в любой тревожной ситуации главное правило — не принимать решений под давлением, прекратить разговор и проверить информацию самостоятельно в официальном источнике.



Про наш разговор никто не должен знать

Требование никому не рассказывать о разговоре — один из самых явных признаков мошенничества. Злоумышленники понимают, что при обсуждении с близкими их ложь быстро раскроется, поэтому запрещают класть трубку, советоваться с семьей, обращаться в банк или полицию.