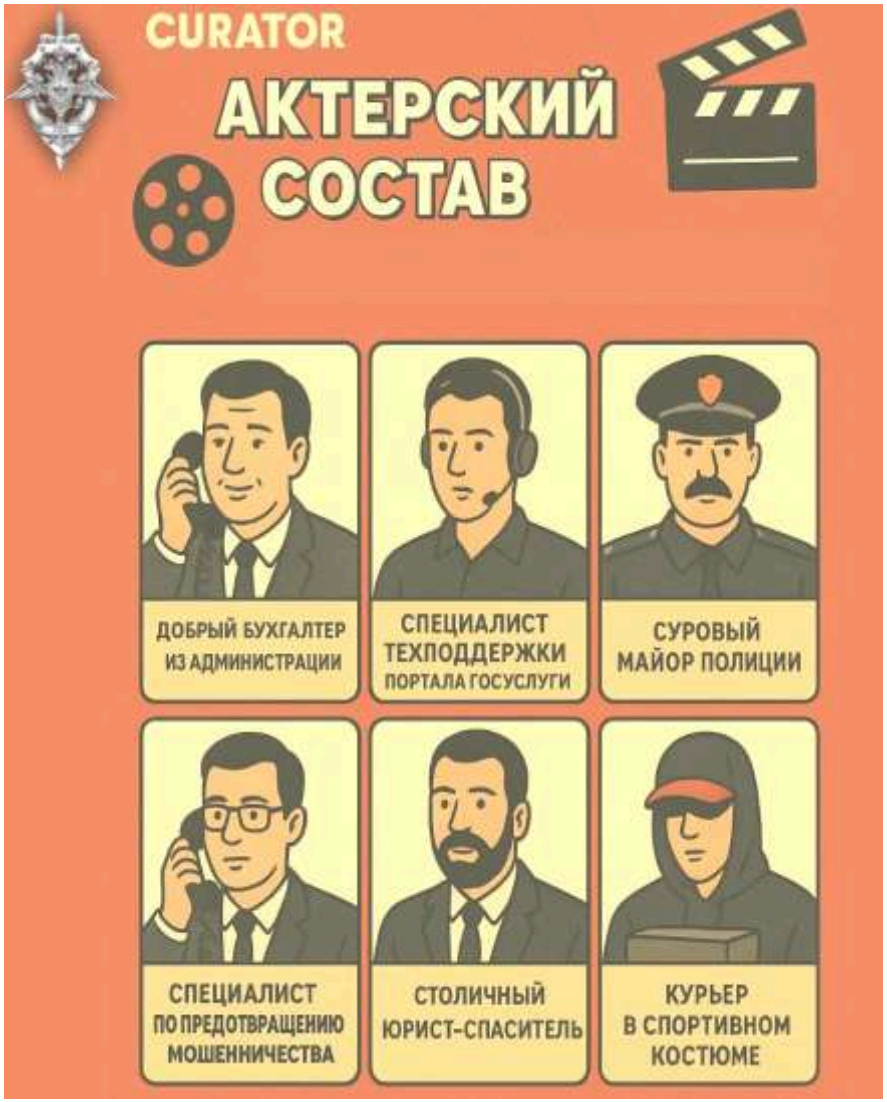


Актёрский состав одного телефонного звонка

Современная мошенническая схема часто напоминает сериал с низким бюджетом, где сценарий строго «по учебнику», а один и тот же актер играет сразу несколько ролей.

Ниже набор образов из одного эпизода
(к сожалению, не сериала, а уголовного дела):

«Добрый бухгалтер из администрации»
Первая сцена. Спокойный, вежливый голос сообщает о «выплате» или «проверке документов». Главная задача — первый контакт и выманивание кода авторизации.

«Специалист техподдержки портала Госуслуги»
«Технический специалист» сообщает о якобы взломе аккаунта, «подозрительных действиях» или «угрозе утечки данных». Именно эта роль создаёт первую тревожную сцену и формирует ощущение, что ситуация требует немедленных действий.

«Суровый майор»
После появления «специалиста» на сцену выходит представитель силового блока. Использует юридическую лексику, говорит о «подозрительных финансовых операциях», «угрозе ответственности» и давит на эмоции.

«Столичный юрист-спаситель»
Создаёт иллюзию легитимности. Предлагает «законную схему защиты» и называет адрес офиса для солидности.

«Сотрудник по контролю и надзору за финансовым мошенничеством»
Кульминация. Заявляет, что на имя гражданина открыты счета, идут переводы, а единственный способ «защитить средства» — выполнить ряд срочных указаний, включая выдачу наличных или перевод средств.

«Курьер в костюме»
Финальный исполнитель — человек, которому передаются деньги. Молча получает пакет, называет пароль и исчезает.

Мораль проста: *если вам по одному сценарию звонят пять разных людей — вы не в сериале «Клан Сопрано», вы в эпицентре мошеннической схемы.*

? *Зависят ли схемы мошенников от возраста потенциальной жертвы?*

И да, и нет. *Базовые приёмы, такие как давление, ложные авторитеты, и способы вывода денег - универсальны. Но поводы для контакта и стиль общения преступники подстраивают под возраст, интересы и жизненный опыт человека.*

⬇*Ниже — самые характерные сценарии.*

9–17 лет

Основные риски — онлайн-игры и соцсети. Мошенники выдают себя за стримеров или администраторов проектов, предлагают «призы» или «прокачку» и требуют данные карт родителей, коды из СМС или доступ к телефону. Используют и запугивание: придумывают «уголовные дела» или «угрозы семье». Распространены и псевдоподработки (лайки, комментарии, «помощь в продаже»), которые часто оказываются вовлечением в незаконные операции.

18–25 лет

Главные приманки — вакансии, подработки и инвестиции. Требуют «активационный платёж», оплату обучения или покупку товара «для старта». Часто встречаются фейки про «взлом Госуслуг» и «оформление кредита». На сайтах знакомств выманивание денег маскируется под просьбы оплатить билеты, подарки или доставку.

26–40 лет

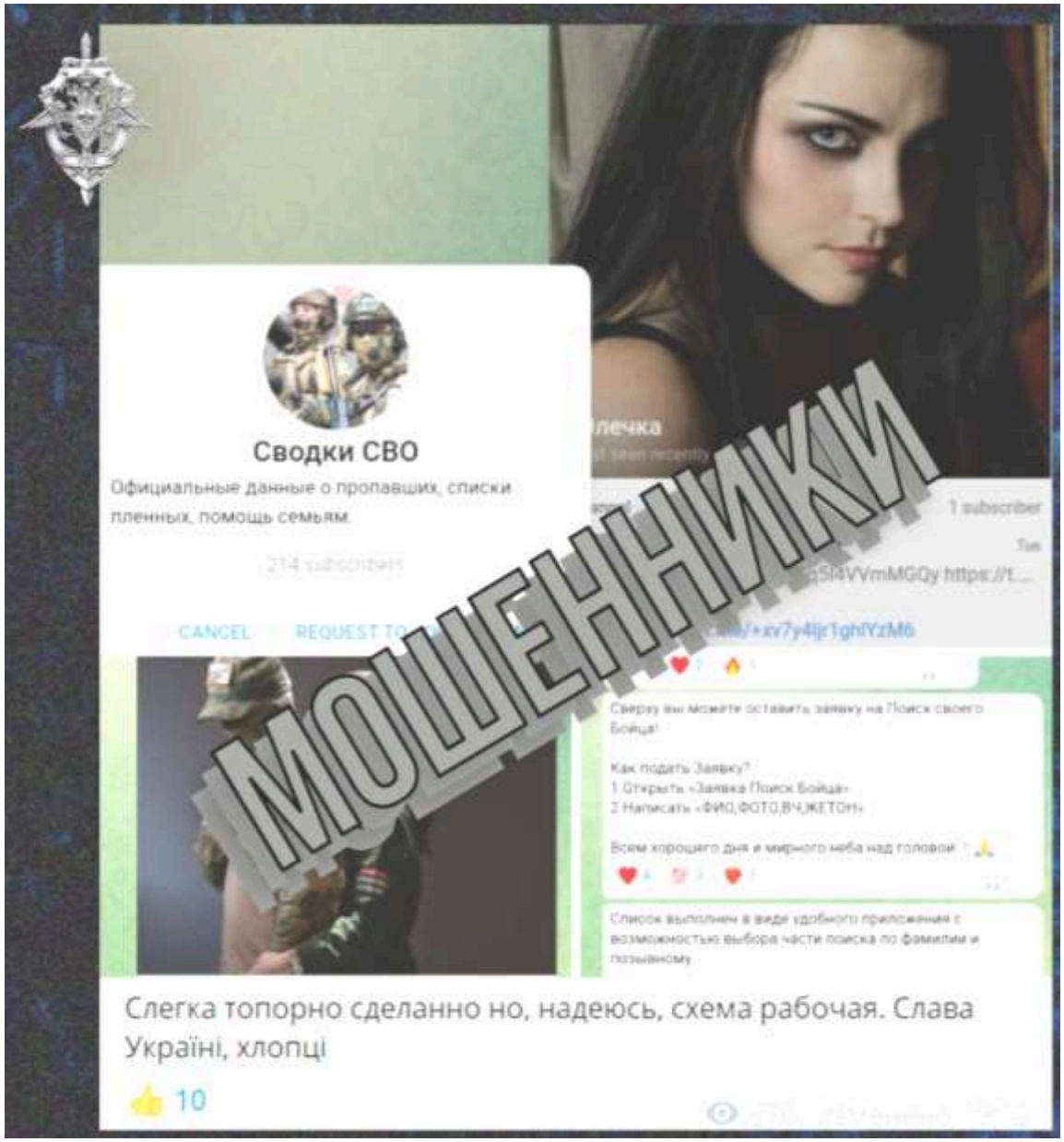
На фоне интереса к заработку предлагают «инвестиции с гарантией», высокооплачиваемый фриланс и торговые платформы. Часто применяются звонки от «ЦБ» или «Росфинмониторинга»: сообщают о подозрительных операциях и убеждают перевести деньги «на резервный счёт». Много обманов связано с маркетплейсами и вредоносными ссылками под видом доставки или акций.

45–60 лет

Преступники чаще всего представляются сотрудниками госорганов или финансовых структур. Сообщают о «финансировании терроризма», «блокировке счетов» и добиваются переводов или передачи средств курьерам. Звонки от «ЖКХ», «налоговой» или «оператора» используются для получения кодов и доступа к аккаунтам.

61+

Основная угроза — многоходовые схемы с имитацией взлома сервисов и последующим звонком «из банка/ЦБ/ФСБ».
По-прежнему актуальна схема «родственник в беде». Опасны и «проверки» от якобы сотрудников ЖЭКа или почты: коды, подписи, доступ в квартиру. Нередко пожилых людей вовлекают в роль курьеров.



Отсутствие связи с военнослужащим — это всегда тяжелое испытание для семьи. Однако в этой тревожной ситуации крайне важно сохранять бдительность.

В мессенджерах и социальных сетях активно создаются фиктивные чаты и группы «по поиску пропавших». *Их настоящая цель — не помощь, а хищение денег и получение данных, посредством распространения среди родственников участников СВО вредоносного программного обеспечения.*

! Не доверяйте личную информацию сомнительным каналам*. Единственно верный путь — обращаться в официальные инстанции!*

Под видом «антирадаров» распространяются вредоносные приложения

! *В ряде регионов зафиксированы случаи, когда граждане скачивали якобы бесплатные сервисы для просмотра расположения дорожных камер, после чего с их счетов происходили списания денежных средств.*

Злоумышленники распространяют вредоносное программное обеспечение (ВПО) ***в анонимных каналах и через "пиратские" сайты*** *под видом APK-файлов:*

– DPS_RADAR (1).apk
– GDEDPS.apk
– Антирадар.apk
– Антирадар_камеры.apk
– PDS-Radar.apk

Сценарий почти всегда одинаков: человек видит рекламу «полезного приложения», скачивает APK из непроверенного источника. После установки программный модуль получает доступ к банковским приложениям или SMS, что позволяет совершать несанкционированные списания.

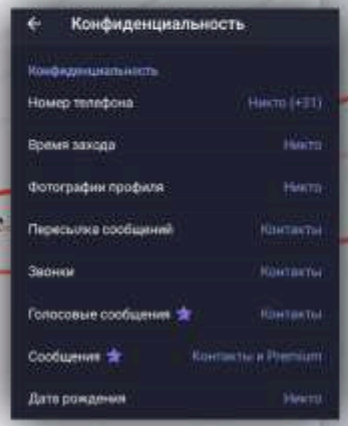
Методические рекомендации для проведения профилактических мероприятий

ЗАЩИТИТЕ СЕБЯ В МЕССЕНДЖЕРАХ

Telegram:

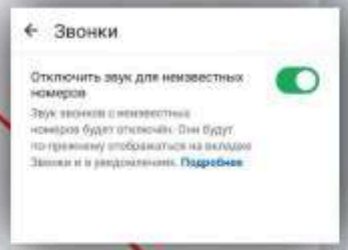
Настройки →
Конфиденциальность →
Звонки →
Мои контакты.

Так мошенник не сможет вам позвонить.



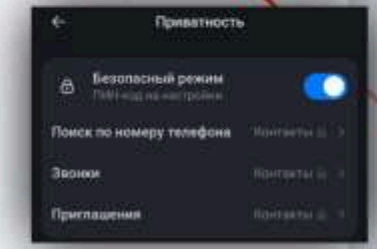
WhatsApp:

Настройки →
Конфиденциальность →
Звонки →
Отключить звук для неизвестных номеров.



MAX:

Настройки →
Приватность →
Безопасный режим.



ПРИ МАЛЕЙШИХ ПОДОЗРЕНИЯХ, ЧТО С ВАМИ ГОВОРИТ МОШЕННИК - ЗВОНИТЕ С МОБИЛЬНОГО 102

ЗА БЕСПЛАТНОЙ ПРАВОВОЙ ПОМОЩЬЮ МОЖНО ОБРАТИТЬСЯ

+7 (499) 550-80-03

Центр правовой помощи гражданам в цифровой среде

ХОТИТЕ ЗНАТЬ БОЛЬШЕ? ПОДПИШИТЕСЬ НА КИБЕРПОЛИЦИЮ РОССИИ

@CYBERPOLICE_RUS

КИБЕРПОЛИЦИЯ РЕКОМЕНДУЕТ

ПРОСТЫЕ НАСТРОЙКИ – МАКСИМУМ ЗАЩИТЫ

В этом буклете мы обобщили простые советы, которые значительно усложнят жизнь мошенникам.

Потратьте немного времени сейчас – сэкономьте нервы и средства в будущем.

В текущем году в компьютерных играх зафиксировано порядка 1000 фактов мошенничества.
В нашем антирейтинге и в глобальном рейтинге мобильных игр по загрузкам лидирует Roblox.

Рассказываем о самых распространенных схемах мошенничества на этой площадке:

► *Злоумышленники чаще всего действуют через яркие видео, «ограниченные» предложения или фейковые раздачи, в игровых чатах, Discord-серверах, соцсетях или пишут ребёнку прямо в игре — под видом «подарка», «конкурса» или «выгодной сделки».*

«Одноразовый» Game Pass
Мошенники продают Game Pass, обещая особые функции или преимущества. На деле такие пропуска либо не дают ничего сверх обычного, либо работают только до перезапуска игры — после выхода из сессии они исчезают, и за них приходится платить снова.

«Невидимая» одежда
Рекламируются и продаются скины, которые якобы делают персонажа невидимым. В реальности это просто прозрачные предметы, которые выглядят как белая рубашка или пустота — никакой спецэффект не работает.

Мини-игры-ловушки
Например, появляется окно с надписью: «Сколько раз ты можешь кликнуть за минуту?». После активного нажатия игроку предлагают купить дорогой предмет, Game Pass или подписку — якобы за «рекорд». На самом деле это просто способ навязать покупку.

Поддельные «испытания на Robux»
В таких локациях ребёнка окружают боты или фейковые игроки, которые кричат: «Получил Robux!», «Это работает!», «Пройди испытание!». В конце просят ввести логин и пароль от аккаунта. Никогда не передавайте эти данные — это приведёт к краже аккаунта и, возможно, привязанных платёжных средств.

Фишинговые ссылки
Мошенники отправлять ссылки «для получения бесплатных Robux». Такие сайты имитируют Roblox, просят логин и пароль или данные карты, а затем блокируют аккаунт и списывают деньги.

Покупка Robux вне официального магазина
Предлагают «выгодно» купить валюту по заниженной цене — но только за пределами платформы. Чтобы «оплатить», просят данные родительской карты. Деньги списывают, а Robux не появляются. В худшем случае — получают доступ к карте и продолжают списания.

«Ты выиграл! Получи приз»
Ребёнку сообщают, что он выиграл Robux в «конкурсе», но для получения нужно ввести данные аккаунта. После этого мошенник меняет пароль и получает полный контроль над профилем — включая историю покупок и привязанные платёжные методы.

Очередная мошенническая схема, направленная на пенсионеров.

! *Пожилым гражданам по телефону или через мессенджеры предлагают перевести пенсионные накопления или личные сбережения в «программу долгосрочных сбережений» или «программу государственного софинансирования пенсий». При этом злоумышленники обещают мгновенное удвоение средств, быстрые выплаты или иные выгодные условия.*

Важно понимать:

▶ Программа государственного софинансирования пенсий ***больше не принимает новых участников.*** *Приём завершился 31 декабря 2014 года. Участвовать в ней могли только те, кто подал заявление в период с 1 октября 2008 года по 31 декабря 2014 года и внёс первый взнос до 31 января 2015 года.*

▶ Программа долгосрочных сбережений действительно ***существует****, но работает только через лицензированные негосударственные пенсионные фонды (НПФ). Заключить договор можно исключительно на официальном сайте или в офисе НПФ. Любые предложения оформить её по телефону, в мессенджере или на стороннем сайте — признак мошенничества.*

! *Государственные органы не звонят гражданам с предложениями участвовать в финансовых программах и не запрашивают паспортные, СНИЛС или иные личные данные дистанционно.*

✓Если вам поступило подозрительное предложение — не сообщайте свои данные, не переходите по ссылкам и свяжитесь с правоохранительными органами или близкими для проверки информации.

Виды дистанционных хищений:

1. Продление договора с оператором мобильной связи.

Если вам звонят от имени мобильного оператора, чтобы продлить действие симкарты, — скорее всего, это мошенники.

Звонящий утверждает, что вот буквально завтра заканчивается ваш контракт на мобильную связь. Если его не продлить, вы не сможете звонить, отправлять смс и пользоваться мобильным интернетом. Номер у вас отберут и передадут другому человеку. Мошенник предлагает продлить договор без посещению офиса. Достаточно продиктовать код из смс.

Конечно, коды из смс никогда и никому говорить нельзя, и многие это знают. Если отказаться, мошенник не будет упорствовать и повесит трубку: его ждет следующий из списка обзвона. Но если почувствует ваши сомнения, постарается дожать: мол, речь о деньгах не идет и вы ничем не рискуете. Вам же хотят сэкономить время. Этот код нужен мошенникам, чтобы получить доступ в личный кабинет жертвы на сайте оператора. Там преступники устанавливают переадресацию звонков сообщений на свой номер. Так они будут узнавать все секретные коды, в том числе от банков. В результате аферисты смогут получить доступ к банковским кабинетам, снять деньги со счетов и даже попытаться оформить кредиты.

2. Продление договора связи стационарного телефона

В разных регионах России фиксируются мошеннические звонки на домашние телефоны. Злоумышленники представляются сотрудником Ростелекома и под предлогом «продления договора связи», просят сообщить КОД авторизации, пришедший в SMS на мобильный телефон жертвы. Получив код, злоумышленники получают доступ к важным аккаунтам, позднее следует новый звонок — уже от имени правоохранительных органов или Росфинмониторинга. Аферисты заявляют, что с аккаунтом жертвы или ее счетами «проводятся незаконные операции», и под видом «защиты» или «проверки» требуют передать деньги курьеру.

3. «Медицинские схемы»

Это один из самых распространенных и опасных для пенсионеров вариантов. В его случае жертву могут «записать на флюорографию», попросив продиктовать номер медицинского полиса или СНИЛСа, попросить помочь в обновлении данных для базы медучреждения, предупредить о необходимости смены медицинского полиса.

Телефонные аферисты начали представляться якобы сотрудниками единой медицинской системы и под предлогом изменения данных о пациенте в системе уговаривают установить программы и похищают денежные средства.

4. Замена кодов или ключей для домофона

В Казани женщина перевела мошенникам почти 500 тыс. руб. после звонка о замене кодов домофона. Злоумышленники представились сотрудниками различных ведомств и убедили женщину перевести деньги на «безопасный счет». Днем пенсионерке позвонил неизвестный, представившийся сотрудником организации по смене кодов домофонов. Он попросил продиктовать временные коды, которые поступят на телефон женщины. Она назвала нужную комбинацию цифр. Затем с

пенсионеркой связались люди, представившиеся сотрудниками Роскомнадзора и Росфинмониторинга. Они запугали женщину возможными несанкционированными переводами и убедили перевести полмиллиона рублнй на «безопасный счет». Мошенники вызвали пострадавшей такси до ближайшего банкомата и запретили общаться с сотрудниками банка и родственниками. Вечером женщина рассказала о произошедшем дочери, которая объяснила, что мать стала жертвой мошенников.

5. Перерасчет пенсии или трудового стажа

Потенциальная жертва получает в мессенджере звонок якобы от Социального фонда. Собеседнику предлагают записаться на «перерасчет пенсии» и просят код из СМС. Затем поступает следующий звонок от аферистов. В этот раз они представляются службой поддержки портала и сообщают, что кто-то пытается украсть данные пользователя. Параллельно человек получает поддельные СМС о входе в личный кабинет в разных микрофинансовых организациях, якобы оповещения о переводе кредитных денег в разные банки. После этого с жертвой связывается «полиция» или «банк», для «защиты» средств они предлагают перевести накопления на «безопасный счет».

«Телефонные мошенники обманывают пенсионеров под предлогом перерасчета трудового стажа и похищают деньги, угрожая уголовным делом за оказания помощи Украине.

Так, неизвестные звонят пожилым людям, представляются работниками Пенсионного фонда и просят продиктовать им паспортные данные якобы для перерасчета трудового стажа.

На этом разговор заканчивается. Затем с потенциальной жертвой связывается псевдоправоохранитель, который сообщает о том, что по паспортным данным человека осуществлен денежный перевод на Украину, в связи с чем в отношении него возбуждено уголовное дело.

Воспользовавшись взволнованным состоянием человека аферисты убеждают пенсионера снять сбережения и для избежания неприятностей и сохранности передать их курьеру. Что человек и делает, лишаясь своих накоплений».

6. Неправильно оформленный запрет на кредиты

Мошенники воспользовались недавно заработавшим самозапретом на кредиты для обмана граждан. Они звонят людям от имени сотрудников «Госуслуг» и уверяют, что запрет установлен неверно, чтобы исправить ситуацию, нужно пройти по ссылке, которую присылают в мессенджере, якобы чтобы исправить заявление. После того, как человек по ней переходит, он попадает на сайт, имитирующий «Госуслуги», вводит свои данные для входа, и они попадают к мошенникам.

7. Звонок от «дочери» или «сына» с применением дипфейков

Жительница Воронежа рассказала об удивительном способе обмана с помощью видео и голоса ее дочери. Мать студентки рассказала, что ей поступил видеозвонок от дочери. Она находилась в странном месте, за ее спиной было видно решетку, и женщина подумала, что девушка попала в отделение полиции. В ходе разговора «дочь» сказала, что у нее проблемы, и требовала без вопросов перевести 100 тысяч рублей. Как выяснилось, мошенники подделали лицо девушки с помощью дипфейка.

8. «Приглашение в коллегию присяжных» или «повестка в суд»

Мошенники начали через электронную почту или мессенджеры вызывать россиян для якобы участия в коллегии присяжных заседателей, для отказа от которого требуют переходить по ссылкам и указать причины неявки. Мошенники начали писать гражданам от имени сотрудников силовых структур и направлять якобы вызовы в правоохранительные или налоговые в связи с подозрением в соучастии в мнимом преступлении. Злоумышленники к таким «вызовам» зачастую прикрепляют активные ссылки, переход по которым предоставит мошенникам доступ к паролям от различных приложений, включая банковские. За неявку обещают наступление административной и уголовной ответственности.

9. «Квартира выставлена на продажу»

«В правоохранительные органы обратилась 77-летняя местная жительница, которая стала жертвой мошенников. Пенсионерке в мессенджере позвонил якобы правоохранитель и сообщил, что ее квартира выставлена на продажу злоумышленниками. Чтобы не потерять недвижимость, женщине порекомендовали самостоятельно ее продать и перечислить вырученные деньги на «защищенный счет». При этом заверили, что жилище останется в ее собственности.

Потерпевшая выполнила все рекомендации и за несколько платежей перевела мошенникам около 50 тысяч долларов. Лишь когда новая владелица попросила ее покинуть квартиру, а звонивший перестал выходить на связь, женщина поняла, что стала жертвой аферистов».

10. Замена электросчетчиков

Мошенники выманивают код для доступа «Госуслугам», представляясь сотрудниками крупных энергосбытовых компаний. Все больше пострадавших фиксируется от данной мошеннической схемы, которая распространилась по всей России: им поступают звонки от якобы представителей коммунальных служб. «Специалисты» назначают время для поверки и замены электросчетчиков, сообщают о необходимости перерасчета платежей или предлагают скидку на ЖКХ. «Каким бы ни был предлог, цель одна - запросить у жертвы код из СМС для доступа к «Госуслугам».

11. Декларирование денежных средства

«Как сообщает прокуратура города Москвы, все началось со звонка. 72-летней москвичке позвонила любезная девушка и сообщила, что необходимо прийти и получить доплату для Ветеранов труда. Девушка сказала, что будет много людей, а она может оформить все без очереди, для этого нужен только номер СНИЛС, который пенсионерка ей продиктовала.

Дальше в дело вступили «правоохранители», которые напугали женщину, сообщив, что она якобы перевела деньги недружественной стране и теперь находится на контроле.

Окончательно запугав пенсионерку предстоящим визитом «сотрудников» с понятыми, лжеследователь сообщил, что все имеющиеся дома деньги необходимо «задекларировать» и передать «дежурному» по району, который придет к ней домой. После проверки информации все денежные средства обещали вернуть. Введенная в заблуждение пенсионерка передала женщине-курьеру более 1,3 млн рублей и 1 тыс. долларов США.

На следующий день к пенсионерке приехал курьер и передал ей коробку, в которой, со слов «следователя», находились деньги, а также два конверта с документами, однако вскрывать коробку пенсионерке запретили, убедив, что это возможно только в присутствии уполномоченного сотрудника и понятых.

Через два дня женщине вновь позвонили и начали убеждать в необходимости дальнейшей декларации денежных средств, находящихся на ее счетах в банке. Однако она заподозрила неладное и обратилась в правоохранительные органы».

12. Подарок с подвохом

«Недавно профильный Telegram-канал «Эксплойт» об интернет-технологиях опубликовал историю девушки-врача.

Ей позвонили в дверь и передали анонимный подарок — букет цветов. Это — первый этап схемы. Получатель уверен, что это приятный сюрприз, и принимает подарок. Единственное, что его заботит, — это личность отправителя: кто же, мол, этот тайный поклонник? Через некоторое время начинается второй этап: злоумышленники звонят жертве и вежливо просят помочь. Они объясняют, что курьер не успел оформить какие-то документы или допустил ошибку, а им для строгой отчетности нужно знать, что букет точно дошел получателю.

Есть и другая вариация второго этапа: злоумышленники звонят и говорят, что произошла ошибка, и подарок предназначался другому человеку.

Дальше схема начинает напоминать любые другие.

Злоумышленники говорят нечто вроде: «Если вам доставили букет, и с ним всё хорошо, продиктуйте, пожалуйста, код из СМС-сообщения». Либо, если проигрывается сюжет «произошла ошибка», фраза звучит как: «Для отмены заказа продиктуйте код из СМС».

В некоторых случаях жертве через мобильный поступают деньги (обычно около 10-15 тыс.), а затем ее требуют их вернуть через СМС-код, запугивая уголовной ответственностью за кражу.

13. Имитация взлома Госуслуг

Мошенники используют схему обмана со «взломом» профиля на «Госуслугах». Суть схемы: злоумышленники отправляют на почту человека письмо с предупреждением о входе в аккаунт с «нового устройства». Аферисты оставляют и номер сотрудника «техподдержки», который на самом деле перенаправляет жертву в украинский колл-центр. Похожая схема с указанием фейкового номера поддержки также применяется на созданных мошенниками справочных сайтах.

14. Инсценировка похищения ребенка

«Угрожали тюрьмой и детским домом: телефонные мошенники инсценировали похищение ребенка и требовали 3 млн рублей у родителей в качестве выкупа.

Аферисты позвонили 11-летнему мальчику и, представляясь сотрудниками «Роскомнадзора», сообщили, что родители якобы являются пособниками преступников и необходимо выполнять телефонные указания, иначе родителей посадят в тюрьму, а его отдадут в детский дом. Испуганный ребенок, действуя по указанию злоумышленников, провел обыск в квартире, но ничего не нашел. Затем звонившие сказали мальчику сесть в такси и доехать якобы до их «сотрудницы», которую они выдавали за правоохранителя.

У подъезда жилого дома ребенка встретила пожилая женщина, которая незадолго до случившегося сама стала жертвой мошенников и действовала по их

указанию. Она проводила мальчика к себе в квартиру, где спустя непродолжительное время ребенка обнаружили уже настоящие правоохранители. Родители мальчика пояснили, что им звонили неизвестные, сообщали, что сын похищен, требовали выкуп 3 млн рублей, а также присылали фото ребенка.»

15. Лжедоставка

Одна из новых схем получила название «Вам доставка».

Злоумышленники эксплуатируют популярность интернет-торговли. Человеку поступает звонок якобы от службы доставки известного (а иногда и выдуманного) маркетплейса.

Голос на другом конце провода сообщает радостную новость: долгожданная посылка оплачена отправителем и уже в пути. Для пущей убедительности имитируется рабочий шум офиса на фоне, а «сотрудник» обращается к жертве по имени-отчеству. Суть легенды сводится к тому, что нужно лишь сверить номер квитанции, который вот-вот придёт в СМС. И вот тут начинается самое главное: сообщение действительно приходит, но с подозрительной пометкой «код подтверждения». На осознание того, что это ловушка, у жертвы буквально одна секунда. Если не среагировать мгновенно, деньги уйдут моментально.

16. Саморазоблачение мошенников

Мошенники усыпляют бдительность россиян, имитируя по телефону свое разоблачение. Суть схемы: аферист звонит от имени курьера, неумело пытается выведать СМС-код, который тут же приходит с неизвестного номера. Через секунду он просит «повисеть» на линии и «прокалывается», якобы забывая выключить микрофон. «За кадром» он с подельниками обсуждает, как выведать тог самый код из СМС. В этот момент человек на другом конце провода все «понимает», но игра на этом не заканчивается. В нее вступает фейковый сотрудник «Роскомнадзора», который «засек» злоумышленника. Он звонит жертве, сообщает о мошенниках и просит уже ему — настоящему сотруднику - сообщить персональные данные или код из СМС.

17. Онлайн-обыск

«22 января возбуждено уголовное дело о мошенничестве, жертвой которого стала 18-летняя бердчанка. Схема началась традиционно: на телефон девушке пришло смс-сообщение с неизвестного номера о том, что кто-то получил доступ к её личному кабинету на Госуслугах. В этом же сообщении был указан телефон техподдержки, по которому взволнованная бердчанка тут же позвонила.

С этого момента девушка и попалась в лапы аферистов. Там ей сообщили, что её личный кабинет взломан и перевели на якобы сотрудника Росфинмониторинга. «Сотрудник» сообщил ей, что на её имя оформлен кредит, а эти деньги пошли на нужды и поддержку чужой армии. Далее её соединили с «сотрудником ФСБ», который сообщил ей, что на девушку завели уголовное дело. Прикрывающийся Федеральной службой безопасности мошенник перезвонил ей по видеосвязи: девушка увидела, что в кабинете за столом сидит мужчина в костюме, а на стене портрет президента. В процессе разговора девушку настолько сильно запугали, что когда аферист заявил ей, что он прямо сейчас проведёт обыск по видеосвязи, то она безропотно согласилась. Свои слова он подкрепил демонстрацией постановления о возбуждении уголовного дела. Бердчанка прошлась с телефоном по квартире и сняла

неизвестному человеку всё, что в ней имеется, включая наличие ювелирных украшений.

Дальше девушка села в такси, которое ей вызвали аферисты, сдала все имеющиеся украшения в ломбард и получила за них деньги. Там, по легенде мошенников, золотые изделия должны были оценить, чтобы указать их стоимость в документах обыска, и вернуть обратно. Вырученные деньги в сумме более 100 тысяч рублей и имеющуюся наличность местная жительница положила на «безопасный счёт» в банке».

18. Новая сим-карта

Телефонные мошенники придумали схему, в которой обманывают россиян якобы открытой на их имя подарочной сим-картой. Мошенники для реализации схемы представляются сотрудниками одного из российских мобильных операторов, сообщая абоненту об открытой на него подобной сим-карте с уже записанной суммой - к примеру, 450 рублей. Они заверяют, что, если абонент не нуждается в данной сим-карте, ее можно закрыть, а деньги - вывести на свой банковский счет. Но якобы для вывода денег им нужны персональные данные, такие, как ФИО, данные паспорта, банковской карты и так далее. Они могут также попросить установить приложение для удаленного доступа или передать код, который приходит в СМС. А если не выполнить указанные действия сразу, то деньги будут потеряны. Получив нужные им данные или сразу же доступ к учетным записям, телефонные мошенники получают доступ и к деньгам на счетах. В связи с этим, не нужно доверять подобным предложениям и не сообщать посторонним лицам свои личные данные.

19. СМС-бомбинг

Аферисты начали использовать техники так называемого SMS-бомбинга - это вид кибератаки, при которой массово отправляются сообщения на мобильный номер конкретного человека. Сразу после этого жертве начинают поступать звонки якобы сотового оператора, который сообщает о том, что они видят массовую SMS-атаку, и предлагает вам выход из ситуации, но через подтверждение ваших персональных данных и кодов из СМС.