Эволюция обмана

Ситуация с кибермошенничеством в России в 2026 году напоминает бег по замкнутому кругу, а старые схемы мошенников работают лучше новых технологий.

С одной стороны, банки и операторы связи отчитываются о блокировке миллионов подозрительных звонков и предотвращении хищений на астрономические суммы – только за первый квартал 2026 года удалось остановить перевод средств на сумму почти 14 триллионов рублей. С другой стороны, жители российских городов продолжают терять большие суммы денег, подвергаясь всё новым мошенническим атакам. Например, только в Новосибирской области за три месяца 2026 года кибермошенники похитили порядка 500 миллионов рублей, а раскрываемость таких преступлений едва превышает 34 процента. «Борьба идёт, а воз и ныне там» – эта фраза как нельзя лучше описывает ситуацию, в которой технологии защиты развиваются, но человеческая доверчивость и страх остаются самым уязвимым звеном.

Вредоносный MAX

Одна из свежих схем, с которой россияне столкнулись в апреле 2026 года, связана с домовыми чатами в мессенджерах, включая государственный мессенджер «MAX». Под разными именами (сосед, управа, участковый и т.д.) рассылают сообщения с приглашениями: по собранию какому-то, по залитию, по видео о правонарушении... Кроме этого, жители домов получают приглашения в группы, где якобы обсуждаются насущные вопросы – установка шлагбаумов, видеокамер, замена мусорных контейнеров. Мошенники создают фейковые общедомовые чаты, наполняют их подставными аккаунтами, которые имитируют активное обсуждение, а затем под видом голосования или срочной поверки счётчиков присылают фишинговые ссылки.

Так, согласно данным СМИ в середине апреля житель Челябинска Владимир едва не стал жертвой такой схемы. Его добавили в группу с названием «Общее собранее жильцов» – с орфографической ошибкой, которая сама по себе должна была насторожить. Чат выглядел правдоподобно: соседи обсуждали установку теплового пункта, шлагбаума и раздельный сбор мусора. Но Владимира смутило несколько деталей. Во-первых, в чате состояло всего пять участников – для дома на 110 квартир явно маловато. Во-вторых, управляющая настаивала на срочности: проголосовать нужно было за один вечер, и даже тем, кто не поддерживает инициативу, предлагалось «обязательно пройти форму через бот». Когда Владимир спросил адрес дома, ответа не последовало – и он понял, что столкнулся с мошенниками.

Хотели как лучше...

По данным управления МВД Челябинска, официально зафиксированных случаев мошенничества с общедомовыми чатами в «MAX» пока нет. Однако в ведомстве подчеркивают: схемы, связанные с выманиванием данных через подозрительные ссылки, остаются распространёнными. Ссылки могут вести на фишинговые сайты или запускать установку вредоносных программ, которые способны получить доступ к данным телефона. Эксперты центра исследования киберугроз Solar 4RAYS уже обнаружили в «MAX» вирус «Мамонт», который может похищать персональные данные пользователей Android и получать доступ к банковским приложениям.

А вот московские полицейские вообще призывают не устанавливать «MAX». Как сообщил крупный телеграм-канал «Топор. Экономика», после переноса домовых чатов в нацмессенджер участковые ежедневно фиксируют по 5–6 жалоб от жителей ЖК.

Примечательно, что государственный мессенджер «MAX» изначально позиционировался как безопасная альтернатива WhatsApp и Telegram, работу которых Роскомнадзор ограничил в августе 2025 года. Власти обязали управляющие компании и ТСЖ с 1 сентября 2025 года перенести все домовые чаты в «MAX». Однако, как показала практика, мошенники быстро освоили новую платформу. Более того, эксперты отмечают, что в «MAX» проще идентифицировать пользователей, а само приложение при установке получает доступ к мониторингу действий владельца телефона. Стоит ли рассчитывать на безопасность MAXa, после такого? Даже депутат от КПРФ Николай Коломейцев на заседании фракции сообщил, что его аккаунт в мессенджере «MAX» уже несколько раз подвергался взлому, и это при том, что приложение позиционируется как безопасное.

Старые добрые махинации

Параллельно с атаками на домовые чаты мошенники продолжают использовать классическую схему с фальшивыми уведомлениями от «Госуслуг» и Мос.ру. Жителям приходят письма с неизвестных почтовых доменов, где сообщается о подозрительном входе в аккаунт. Якобы система зафиксировала использование чужих данных для входа с указанием времени, модели устройства и IP-адреса. Человеку предлагается срочно позвонить в «техническую поддержку», чтобы спасти аккаунт. На деле номер ведёт прямо в call-центр мошенников.

В январе 2026 года член комитета Госдумы по информполитике Антон Немкин предупреждал: мошенники построили новую схему обмана именно на страхе быть взломанным. Они массово рассылают фишинговые сообщения, маскирующиеся под уведомления от госсервисов, предлагают провести проверку защиты аккаунта и запрашивают данные для доступа к личным кабинетам. Передавая эти данные – логин, пароль, а затем и код из SMS, – человек фактически сам открывает мошенникам доступ к своему аккаунту на «Госуслугах». А дальше с персональными данными можно сделать что угодно: оформить заявление, попытаться взять кредит, изменить информацию в профиле или использовать аккаунт жертвы для дальнейших атак на её знакомых.

Ещё одно направление, которое активно развивают мошенники, – использование темы здоровья. В апреле 2026 года в компании Angara Security сообщили, что злоумышленники начали копировать интерфейс раздела «Моё здоровье» на портале «Госуслуги» и создавать на его основе фишинговые страницы. Потенциальных жертв просят ввести номер телефона и подтвердить действия с помощью кода, тем самым предоставляя мошенникам доступ к личным данным. Следующим этапом становится массовый обзвон от имени техподдержки «Госуслуг», банковских работников или даже силовиков – все они пытаются убедить человека в якобы произошедшей утечке данных, чтобы запугать и вынудить перевести деньги.

А царь-то ненастоящий!

Особого внимания заслуживает возвращение схемы «фейк-босс» в обновлённом, технологически более опасном формате. В апреле 2026 года граждан предупредили: злоумышленники начали рассылать видеосообщения и совершать звонки, имитируя не только голос, но и внешность руководителей компаний с помощью дипфейков. Если раньше аферисты ограничивались подменой номера или текстовыми сообщениями от имени начальника, то теперь технологии позволяют создавать убедительные аудио- и видеоподделки. Для создания правдоподобного дипфейка используются открытые источники: записи выступлений, интервью, видеоконференции. Сотрудник компании может получить видеозвонок якобы от своего руководителя с требованием срочно перевести деньги или передать конфиденциальные данные.

Особенно эффективными такие атаки делают давление на срочность и авторитет «первого лица». При этом технический порог входа в подобные схемы стремительно снижается: если ещё недавно создание качественного дипфека требовало серьёзных ресурсов, то сегодня доступны относительно простые инструменты, позволяющие автоматизировать этот процесс. Это означает, что подобные атаки могут быстро масштабироваться и выходить за пределы точечных инцидентов.

Не менее цинично выглядит схема «убитый сосед», о которой МВД рассказывало ещё в январе 2026 года. Человеку звонит якобы участковый и сообщает, что соседнюю квартиру ограбили или убили жильца, а сейчас проводится секретная операция по поимке преступника. Жертву просят помочь: снять все деньги со счетов и передать курьеру для «помеченных купюр» или «оплаты услуг понятого», при этом строжайше запрещается рассказывать об этом родственникам. Схема рассчитана на чувство страха и гражданского долга. Сотрудники правоохранительных органов никогда не будут просить обналичить личные денежные средства и передать их курьеру – об этом в МВД напоминают отдельно.

Холодный рассудок

Как же обезопасить себя в этой новой реальности, где поддельным может оказаться даже сосед по лестничной клетке или звонок от собственного руководителя? Эксперты и представители МВД сходятся во мнении: главное оружие – это холодный рассудок.

Прежде всего, необходимо всегда перепроверять информацию. Если вас добавили в «домовой чат» или прислали ссылку на голосование, свяжитесь со старшим по дому или председателем ЖСК по телефону, который вы знаете давно, и уточните, действительно ли создаётся такая группа. Позвоните в управляющую компанию по официальному номеру, указанному на квитанции. Мошенники часто создают срочность и подталкивают к быстрым действиям, но в таких ситуациях спешка – главный риск.

Крайне важно и активировать двухфакторную аутентификацию во всех мессенджерах и на портале «Госуслуги». Это значительно усложнит взлом, даже если пароль окажется скомпрометирован. Никогда и никому не пересылайте коды из SMS, какой бы убедительной ни была легенда. Ни настоящий председатель, ни сотрудник банка, ни тем более сотрудник полиции никогда не попросят вас назвать код, который пришёл на телефон. А если порталу «Госуслуги» необходимо о чём-то оповестить пользователя, его сообщения появляются только внутри приложения или в личном кабинете на сайте – никаких ссылок для «проверки защиты аккаунта» государственные сервисы не рассылают.

Доверяй, но проверяй

Также рекомендуется отключить автоматическую загрузку медиафайлов в мессенджерах и не переходить по подозрительным ссылкам, особенно если вас торопят. Помните: настоящие опросы собственников проводятся официально – через управляющую компанию, с оформлением протоколов и, как правило, на очных собраниях жителей. Обычно вся эта процедура занимает не один день и не одну неделю. Ну а если же вы всё-таки перешли по ссылке или заподозрили неладное, действовать нужно незамедлительно. Смените пароли от всех важных аккаунтов, начиная с почты и «Госуслуг». Проверьте список устройств, с которых выполнен вход, и завершите подозрительные сеансы. Свяжитесь с банком по официальному номеру, чтобы заблокировать карты или счета. И, конечно, напишите заявление в полицию.

Показательная деталь: в январе 2026 года общее количество зарегистрированных преступлений в России сократилось на 17 процентов по сравнению с аналогичным периодом прошлого года. Количество мошенничеств всех видов уменьшилось на 16,3 процента, а преступлений, совершённых с использованием IT-технологий, – на 25,7 процента. Однако эти цифры не должны успокаивать. Снижение статистики может объясняться разными причинами – от нежелания жертв обращаться в полицию до перехода мошенников на более точечные, сложно выявляемые схемы. Главное, что остаётся неизменным: мошенники не взламывают сложные коды, они взламывают доверие, человеческую готовность помочь соседу, испугаться за свои сбережения или подчиниться авторитету «начальника». Единственная надёжная защита – это принцип «доверяй, но проверяй», помноженный на базовую цифровую грамотность.

Мария Климанова