



ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА САМАРСКОЙ ОБЛАСТИ
**ПРОКУРАТУРА
ЦЕНТРАЛЬНОГО РАЙОНА
ГОРОДА ТОЛЬЯТТИ**
ул. Мира, 85, г. Тольятти, 445021



29.09.2026 № 07-12-2026/5494-26-214

На № _____

Главе городского округа Тольятти

Сухих И.Г.

445011, г. Тольятти, пл. Свободы, 4

tgl@tgl.ru

Начальнику У МВД России
по г. Тольятти

Чагаеву И.Б.

Заместителю начальника ОНД и ПР
ГУ МЧС России по Самарской
области

Гаврилову А.А.

ул. 40 лет Победы, 94, г. Тольятти,
445039

2NDPR@63.mchs.gov.ru

Начальнику территориального
отдела Управления
Роспотребнадзора по Самарской
области в городе Тольятти

Плужнову Р.Ю.

Московский проспект, д. 19,
г. Тольятти, Самарская область,
445032

tltpn@fsnsamara.ru

Уважаемые коллеги!

Администрация городского округа Тольятти Канцелярия (тел. 543-744)
РЕГИСТРАЦИЯ ВХОДЯЩЕЙ СЛУЖЕБНОЙ КОРРЕСПОНДЕНЦИИ
Вх. № 12232-6011
от 12.10.26

В целях минимизации фактов совершения в отношении работников органов и учреждений Самарской области и их близких родственников телефонных мошенничеств в настоящей памятке приведены популярные приемы и схемы мошенников, с которыми можно столкнуться в 2026 году.

Не стоит заблуждаться, что жертвами мошенников становятся лишь крайне доверчивые и технически неграмотные люди. Жертвой злоумышленников может стать каждый. Ведь преступники вооружены не только необходимыми техническими инструментами, но и прекрасно владеют методами психологической манипуляции, а арсенал их методов весьма разнообразен.

Вот основные приемы, которые используют мошенники:

– **социальная инженерия** – методы психологического воздействия на жертву с целью заставить её выполнить определенное действие, необходимое злоумышленникам (назвать код подтверждения или иную персональную

информацию, перевести деньги или отдать наличные добровольно). Это могут быть как звонки под видом различных организаций (банков, МВД, Социального фонда, поликлиники и т.д.), так и различные методы шантажа и прямых угроз (например, сначала жертве поступает перевод на карту от незнакомого лица, а затем её начинают запугивать соучастием в преступной цепочке по отмыванию средств);

– **технические атаки на аккаунты** – взлом путем простого перебора различных комбинаций для поиска нужного ключа. Современные хакерские программы способны буквально за минуту взломать цифро-буквенные пароли длиной 6–8 символов;

– **сим-своппинг** – получение тем или иным способом дубликата сим-карты жертвы (например, по поддельной нотариальной доверенности или через агента в офисе продаж). Благодаря этой копии злоумышленники будут получать все СМС-сообщения, адресованные жертве, в том числе коды для входа в личный кабинет банка, сотового оператора или на «Госуслугах»;

– **дипфейки** – смоделированный голосовой или видеоконтент, который имитирует речь и даже изображение реального человека. Жертва получает голосовое либо видеосообщение от имени родственника, друга или коллеги с тревожным содержанием, сводящееся к тому, что нет времени объяснять, просто срочно нужно перевести деньги по такому-то номеру или реквизитам.

– **тактика обратного действия** заключается в том, что жертву вынуждают связаться с мошенниками самостоятельно. Это нужно для того, чтобы обойти антифрод системы операторов (алгоритмы которых стали довольно успешно распознавать и блокировать звонки с подозрительных номеров) и обязательную маркировку звонков (когда при входящем звонке отображается не только номер, но и официальное название организации).

– **фишинг** – распространение через электронную почту, мессенджеры и соцсети ссылок на поддельные страницы, маскирующиеся под официальные сайты различных организаций (банков, интернет-магазинов, государственных служб и т.д.) с целью выведать персональные данные пользователей для входа в их аккаунты.

Среди распространенных схем телефонного мошенничества выделяются следующие.

Перевод денег на «безопасный счет». Злоумышленники звонят жертве, представляясь сотрудниками банка или представителями правоохранительных органов, и заявляют, что средства и репутация подвергаются серьезной угрозе. Обычно сообщается, что неизвестные лица получили несанкционированный доступ к счету или провели сомнительные операции. Для предотвращения возможного ущерба клиенту настоятельно рекомендуют немедленно перевести деньги на специальный «безопасный счет». Этот новый счет оказывается подставным, принадлежащим самим мошенникам. Цель схемы — вызвать панику и быстро вынудить жертву совершить необдуманные действия, пока она находится под впечатлением угрозы.

Тревожный звонок. Жертве звонят лжесотрудники полиции, больницы

или прокуратуры, утверждая, что близкий человек оказался в бедственном положении, например попал в серьезную аварию или задержан правоохранительными органами. Сначала мошенники рисуют максимально мрачный сценарий дальнейшего развития событий, а затем предлагают выход: спасение здоровья или свободы близкого требует немедленного перевода крупной суммы денег на определенный счет или передачи наличных курьеру. Часто для создания иллюзии реальности происходящего используются поддельные голоса, фото или видеоизображения. Схема весьма похожа на предыдущую, её цель – шокировать жертву и вынудить заплатить выкуп.

Сверхприбыльные инвестиции. Мошенники выдают себя за финансовых консультантов или представителей инвестиционных компаний, предлагая участие в уникальных проектах с обещаниями сверхприбыли. Обычно они рекламируют свои фиктивные финансовые достижения через привлекательные сайты, социальные сети и Telegram-каналы, заполненные поддельными положительными отзывами. Цель схемы – привлечь жертву вложениями в псевдопроект. Чтобы укрепить доверие и стимулировать внести крупную сумму, жертве могут позволить вывести «доход» от первого вложения. Но после повторного крупного пополнения счета мошенники перестают отвечать на запросы, оставляя потерпевшего без вложений и прибыли.

Инфоцыганство. Мошенники привлекают потенциальных жертв заманчивой картинкой красивой жизни и громкими обещаниями. Они позиционируют себя как гуру в определенной сфере, например в маркетинге или психологии, уверяя, что можно мгновенно обогатиться или легко достигнуть любых других целей. Для этого достаточно купить их дорогостоящий курс по личностному росту, финансам или взаимоотношениям и т.д. В качестве доказательства, что методика работает, мошенники демонстрируют свой шикарный образ жизни и приводят отзывы несуществующих адептов, рассказывающих о чудесных изменениях в жизни благодаря пройденному обучению. Но вскоре выясняется, что курсы оказались пустышкой: оплаченная программа состоит из поверхностных советов, бесполезных методик и общей воды. Цель схемы – привлечь наивных людей, верящих, что можно заработать большие деньги, не обладая серьезными компетенциями и не прикладывая больших усилий. Как злоумышленники получают доступ к аккаунтам пользователей.

Звонки под видом сотрудников различных организаций. Тут фантазия телефонных мошенников поистине безгранична: насчитывается уже не один десяток легенд, под которыми они звонят гражданам. Чаще всего злоумышленники представляются сотрудниками банков, Пенсионного фонда, поликлиники, сотовых операторов, коммунальных служб и др. В последнее время участились звонки под видом сотрудников службы доставки, а с момента частичной блокировки зарубежных мессенджеров – звонки под видом сотрудников МАХ. Цель схемы – любыми способами заставить жертву назвать проверочный код для доступа в банковский личный кабинет или на «Госуслугах». Далее, войдя в цифровые сервисы, преступники получают

полный контроль над финансами и документами человека: могут вывести все деньги со счетов, оформить на имя пострадавшего кредиты, совершить от его имени сделки с недвижимостью и т.д. Иногда преступники прибегают к многоуровневой схеме: сначала выманивают проверочный код, а затем сообщают о взломе личного кабинета и далее в зависимости от легенды либо запугивают, либо предлагают спасти финансы на «безопасном» счете.

Обратный звонок. В последнее время мошенники сменили тактику: теперь не они осаждают телефонные линии абонентов, а вынуждают им перезванивать. Жертве присылается сообщение, побуждающее к незамедлительным действиям, например: «Ваш аккаунт взломали, срочно обратитесь в техподдержку...», «На вашем счете образовалась задолженность, для восстановления доступа к услугам свяжитесь...», «Мы произвели списание за подключенную платную услугу, подробности по...» и далее идет номер телефона, куда нужно звонить для уточнения всех обстоятельств. Скорее всего, указанный номер даже будет начинаться с 8-800, что придаст ему официальности, но на самом деле жертва дозвонится в кол-центр мошенников. Цель схемы – в конечном итоге выманить у жертвы проверочный код. Кроме того, существует отдельная разновидность мошенничества, связанная с вынужденным звонком на платные номера. Пока жертву переключают с одного «специалиста» на другого, с баланса списываются крупные суммы.

Атаки на телефонные номера и аккаунты. В сценариях нападения могут использоваться разнообразные техники: от прямого технического взлома, до перехвата проверочных кодов через дубликаты сим-карт или установленные шпионские программы. Например, на фоне массовых ограничений интернета участились случаи атак через публичные Wi-Fi-сети. Отдельно стоит выделить схему со взломом аккаунта на маркетплейсах. Преступники заранее создают на онлайн-площадках поддельные магазины. Затем оплачивают несуществующие товары банковскими картами, привязанными в личных кабинетах покупателей, после чего бесследно исчезают. Цель мошенников – добыть доступ к личным кабинетам, украсть средства и осуществить действия от имени владельца аккаунта.

Кража данных через поддельные сервисы, ссылки и QR-коды. Приглашение поучаствовать в конкурсе от популярного бренда или проголосовать по просьбе знакомого человека. Переход по ссылкам на фальшивые страницы популярных магазинов, где покупатели оставляют реквизиты карт, думая, что оплачивают реальный заказ. Сканирование поддельных QR-кодов, размещенных поверх настоящих. Все это – наиболее частые примеры фишинга. Целью фишинга является сбор персональных данных и их дальнейшее использование в мошеннических схемах либо прямая кража денег со счетов.

Лучшая защита от мошенников – это ваша личная бдительность. Следуя простым правилам, вы сможете значительно снизить риск финансовых потерь:

– не доверяйте звонкам лиц, представляющихся сотрудниками различных

организаций. Всегда перезванивайте сами, но только по официальным телефонам, чтобы уточнить поступившую информацию;

- запомните: настоящие сотрудники никогда не будут запрашивать проверочные коды, личные данные или настаивать на незамедлительном совершении каких-либо действий. Немедленно прекратите разговор, если почувствовали давление или попытку выведать персональную информацию;

- избегайте случайных знакомств. Ни в коем случае не соглашайтесь на оказание помощи незнакомцам, которая заключается в предоставлении банковских реквизитов или номера телефона для переводов;

- если получили перевод от неизвестного лица, сообщите об этом в банк;
- скачивайте приложения только в официальных магазинах, запретите установку программного обеспечения из неизвестных источников в настройках смартфона;

- добавьте в закладки браузера наиболее часто посещаемые интернетресурсы, чтобы реже переходить по внешним ссылкам; – создайте уникальные пароли для каждой учетной записи, избегая слишком простых комбинаций, и регулярно их обновляйте;

- включите двухфакторную аутентификацию везде, где это возможно, чтобы дополнительно защитить свои аккаунты (для входа в учетную запись потребуется ввести не только логин и пароль, но и проверочный код);

- используйте защищенные сети Wi-Fi (для подключения к которым нужен пароль), не передавайте важную информацию через публичные точки доступа;

- не переходите по ссылкам, полученным от неизвестных отправителей (особенно в мессенджерах или через новые чаты в СМС);

- не доверяйте невероятно выгодным предложениям: огромным скидкам от мнимых продавцов; работодателям, обещающим легкий заработок; финансовым организациям, сулящим нерыночные процентные ставки и т.п.;

- заведите отдельные карты для оплаты покупок на маркетплейсах и других онлайн-площадках. Не храните на них деньги, а пополняйте на нужную сумму непосредственно перед покупкой;

- на «Госуслугах» установите самозапреты на выдачу займов и кредитов, получение сим-карт и проведение сделок с недвижимостью без вашего личного участия;

- установите родительский контроль на устройства, которыми пользуются дети;

- договоритесь с близкими о секретных кодовых словах, которые помогут убедиться в реальности собеседника в ситуации подозрения на обман. Расскажите об опасности пожилым родственникам и детям. Объясните, какими методами чаще всего пользуются мошенники, какую информацию нельзя сообщать и как вести себя в ситуациях, когда незнакомец представляется сотрудником банка и госструктур.

Необходимо помнить, что мошенники отличаются фантазией и гибкостью, они непрерывно изобретают новые способы обмана, адаптируясь к

изменениям в законодательстве и технологиям. Большинство мошеннических схем основано на эксплуатации человеческой доверчивости, желании легкой выгоды или эффекте неожиданности, когда жертву застают врасплох, не оставляя времени на анализ ситуации. Задача каждого человека – оставаться начеку и учиться определять угрозу. Для этого необходимо постоянно повышать собственную киберграмотность, следя за публикациями о современных методах мошенничества.

Прошу вас и подчиненных вам работников (подведомственных подразделений, организаций и учреждений) внимательно ознакомиться с данной памяткой под подпись, а также рекомендую довести её содержание до сведения родственников и иных близких лиц.

Прокурор района

В.В. Лошкарев

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 35BD7BD76EDBAA3BC287E9FE26D85960

Владелец Лошкарев Вадим Вадимович

Действителен с 16.02.2026 по 12.05.2027