

• Актуально •

За 2024 год мошенники вывели со счетов россиян 27,5 миллиарда рублей, сообщил Центральный Банк. Это рекордная сумма за всю историю ведения статистики. В России ежедневно поступает около 10-15 миллионов звонков от мошенников, рассказали в СПЧ (Совет по правам человека при президенте России). В № 51 газеты «Киренга» от 20 декабря 2024 года заметка «Осторожно: кибермошенники!» рассказывала о реальных историях жителей Иркутской области, ставших жертвами таких преступлений. Предлагаем еще раз обратить внимание читателей на эту проблему, узнав о новых схемах обмана.

Т. Наумова из райцентра проголосовала в телеграм-канале за семью знакомой в онлайн-конкурсе. После этого близким и друзьям Т. Наумовой начали приходить голосовые сообщения с просьбами занять деньги. Голос девушки в этих сообщениях был создан искусственным интеллектом и полностью копировал ее, включая манеру речи. Один из друзей не понял, что голосовое сообщение пришло не от настоящей владелицы телеграм-канала, и перевёл мошенникам пять тысяч рублей на сторонний номер телефона.

В другом случае мошенник, выдавая себя за оператора МТС, убеждал пожилую женщину, что срок её договора на телефонный номер истёк. Однако пенсионерка знала, что это не так, ведь такой договор бессрочный. Увы, не все пожилые люди разбираются в юридических и технических нюансах и часто становятся жертвами обмана.

В третьем случае учительница из Иркутска А. Смирнова также едва не стала жертвой мошенников. Ей позвонил якобы «капитан полиции ГУВД Центрального района Москвы» через мессенджер Вайбер, который в 2024 году ещё пользовался популярностью. Звонивший заявил, что она обвиняется в преступлении в сфере экономической деятельности, назвал точный адрес иркутянки, и потребовал перевести определённую сумму на указанный им счёт. Он утверждал, что в случае перевода крупной суммы дело будет закрыто. Но девушка заметила несколько подозрительных моментов: почему полицейский звонит в Вайбере? почему он не сообщает никаких подробностей о якобы совершенном преступлении? и к тому же не знает географию России (мошенник заявил, что она проживает в Иркутске Новосибирской области). Благодаря своей бдительности и критическому мышлению учительница не перевела деньги мошенникам.

Последний случай, произошедший с Н. Антроповой из Усть-Кута, особенно печальный, так как он мог привести к более серьёзным финансовым потерям. Всё началось с того, что женщине позвонил сотрудник «Госуслуг» в Ватсапе. Он сообщил ей, что в её личном кабинете на портале «Госуслуг» появилась нотариальная доверенность на имя некоего Иванова.

Этот документ давал Иванову право распоряжаться всеми её счетами и был размещён в специальном разделе для подписания документов в приложении «Госключ». Н. Антропова, не подозревая о мошенничестве, заглянула в приложение и действительно обнаружила документ, подтверждающий наличие доверенности. Она была растеряна и напугана и не знала, как действовать в такой ситуации. Следуя указаниям липового сотрудника, женщина перевела 100 тысяч рублей на «специальный счёт» с кредитной карты. В ходе разговора с обманщиками она получила сообщение об одобрении кредита в Альфа-банке на сумму 1 миллион 600 тысяч рублей, который ей якобы также нужно перевести на «специальный счёт». Но по счастливой случайности у Н. Антроповой села зарядка на телефоне, и звонок прервался. На следующий день она поняла, что перевела мошенникам сто тысяч рублей, и написала заявление в полицию. Спустя год северянка еще «закрывает» кредитную карту.

В 2025 году схемы обмана становятся всё более изощренными. Важно быть начеку, чтобы не стать жертвой мошенников.

«Это я, срочно переведи на эту карту!..»

Злоумышленники всё чаще применяют нейросети для имитации человеческого голоса. Представьте, что вам звонит человек, голос которого вы хорошо знаете, — например, ваш супруг(а), мама или друг. Они просят вас срочно перевести деньги или занять определённую сумму. Вы доверяете этому голосу и, не подозревая подвоха, выполняете просьбу. На самом деле это преступник, использующий технологию синтеза речи, чтобы ввести вас в заблуждение. Согласно последним данным, в 2025 году количество таких случаев выросло в 2,3 раза по сравнению с предыдущим годом. Но кибертеррористы не остановились на голосовых звонках: теперь они используют фотографии для создания реалистичных клонов вашей внешности. Видеозвонки стали новым фронтом этой атаки, и не каждый сможет распознать, что на экране находится не ваш близкий человек, а мошенник.

МВД предупреждает о типичных фразах, которые используют мошенники: «Мама/папа, я в беде, срочно нужны

деньги», «У меня проблемы, помоги», «Это срочно, переведи на эту карту», «Телефон садится, скину реквизиты»... Если вы слышали подобные фразы, следует немедленно прекратить общение и перезвонить человеку на его номер.

"Я в беде,

МАКСимальный обман

Новый российский мессенджер, позиционируемый как безопасная альтернатива Телеграм и Ватсап, стремительно набирает популярность среди россиян. Всё больше людей переходят на платформу МАКС. Но и здесь не обходится без активности злоумышленников. Правонарушители адаптировались под национальный мессенджер, несмотря на то, что зарегистрироваться в МАКСе можно только через российскую и белорусскую сим-карты. По данным аналитиков МТС, первые случаи мошенничества в МАКС начались почти сразу после его запуска. Злоумышленники звонили, представляясь сотрудниками мессенджера, и под предлогом «активации защиты» или «регистрации аккаунта» просили код из смс. Этот код, как известно, используется как ключ к аккаунту на портале Госуслуг.

В ноябре на SOC-форуме по кибербезопасности зампред Сбера С. Кузнецов заявил, что переломить коренным образом статистику по потерям от телефонного мошенничества не удалось, несмотря на принимаемые меры. Об этом, по его словам, свидетельствуют данные, статистика, количество украденных денег у россиян.

Осенью этого года Л. Тарасова из Казачинска неожиданно получила звонок в МАКСе от сотрудника «Иркутскэнергосбыта». Её попросили подписать акт проверки. Девушка, погруженная в отправку рабочих писем в отделение почты России, не сразу осознала, что разговаривает с киберпреступником. Вскоре на её телефон пришло сообщение с четырёхзначным кодом. Наивная землячка без раздумий назвала этот код злоумышленникам. Выяснилось, что Л. Тарасова предоставила доступ не к

«Госуслугам», а к своему аккаунту на сайте «Сравни.ру» (интернет-сервис подбора финансовых и страховых услуг). В этот момент на телефон жертвы стали поступать многочисленные сообщения от различных государственных и коммерческих банков с уведомлениями об одобрении кредитов. Северянка немедленно зашла на портал государственных услуг и оформила самозапрет на получение кредитов.

Также пенсионеру из Ключей *Тi са f e e l a d o «A i a d a e» a M A K C e.* Звонивший с третьей попытки назвал имя

преследование из-за перевода денег или незадекларированных доходов, вызывая у детей страх и желание спасти родителей. Злоумышленники требуют от них провести «видеообыск» квартиры, показать на камеру все накопленные деньги и ценности и передать их курьеру для «проверки» и «декларирования». Один из таких случаев произошёл в начале 2025 года в Москве. 14-летний подросток, поверив в историю о «спасении родителей», передал курьеру 300 тысяч рублей и иностранную валюту.

Аферисты не знают жалости. После получения денег они продолжают издеваться над жертвами, предлагая им поджигать автомобили, банки, военкоматы или выполнять другие преступные действия. Такие случаи часто освещаются в российских СМИ.

Подработка или преступление

Дропперы (это участники мошеннических схем, чья банковская карта или счёт используются для перевода, обналичивания или отмывания похищенных у жертв денег) находят в телеграм-каналах, где обещают быстрый заработок. Многих привлекает отсутствие требований к опыту работы, образованию и официальному трудоустройству.

Единственное условие – наличие банковской карты или доступа к онлайн-банку. Однако у таких соискателей неизбежно возникнут проблемы. Сначала с банками, а затем и с правоохранительными органами. При расследовании интернет-мошенничества полицейские часто выходят на дропперов – владельцев банковских счетов, куда жертвы переводили деньги. Неважно, знал ли владелец карты о своём участии в преступной схеме или нет, – он всё равно становится её участником. К тому же появились дропперы – курьеры. Курьер, который перевозит похищенные наличные деньги с помощью обмана, берет свой «гонорар» за проделанную работу из этих же средств. Федеральный закон от 24 июня 2025 года № 176-ФЗ рассматривает дропперов как участников преступной деятельности и предусматривает юридическую ответственность, даже если они не осознают своего участия в незаконных действиях.

Мошенники используют базы данных, содержащие не только номера телефонов, но и личные сведения: имена, фамилии, адреса, места работы. Когда мошенник обращается к вам по имени, мозг воспринимает это как знак легитимности. Возникает иллюзия, что собеседник знает о вас всё, хотя на самом деле это лишь уловка.

срочно нужны деньги!"



и отчество мужчины и сказал, что на днях придёт мастер поменять домофон. Необходимо сделать новые электронные ключи, а если мужчина откажется, то не сможет попасть в свой подъезд со старыми ключами. Если бы мошенник был знаком с деревенскими реалиями, где отсутствуют многоквартирные дома с домофонами, то не был бы послан в известном направлении...

Поверят даже продвинутые пользователи интернета

Киберпреступники обманывают не только доверчивых пенсионеров, но и подростков. Представляясь сотрудниками полиции, ФСБ или Росфинмониторинга, они сообщают, что родителям грозит уголовное

«Необходимо исчерпать кредитный потенциал»

Ещё один способ обмануть россиян – «многоходовая» схема. Об этом корреспонденту рассказал врио начальника ИВС ОП МО МВД России «Усть-Кутский» А. А. Худонов:

– Случаи киберпреступлений в Казачинско-Ленском районе происходят примерно два раза в неделю. Недавно магистральнику поступил подозрительный звонок. Сначала аферист по классическому сценарию предложил северянину назвать код из смс. Мужчина понял, что разговаривает с мошенником, когда услышал, как его собеседнику подсказывает другой человек: «Держи его на линии, он почти поверил». Потерпевший сразу же завершил разговор, радуясь, что не попался на уловки злоумышленников. Но на этом история не закончилась. Вскоре на его электронную почту пришло сообщение от портала «Госуслуги», где говорилось, что он стал жертвой мошенников и на его имя пытаются оформить кредит. Не подозревая подвоха, мужчина позвонил по номеру горячей линии портала. «Оператор», который, как оказалось, тоже был аферистом, сказал, что необходимо исчерпать свой кредитный потенциал. Мужчина согласился, оформил кредит на два миллиона рублей и перевёл их на «безопасный счёт», как ему сказали. Теперь северянин вынужден выплачивать кредит...

Чтобы оградить себя от мошенников, никогда не называйте коды из смс и данные карты по телефону, даже если собеседнику удалось вас убедить. Ни один банк или госструктура не запрашивает эти данные при звонке. Подключите у оператора связи услуги «Определитель номера» и «Антиспам». Эти функции обычно предоставляются бесплатно или за символическую плату

и помогут вам избежать нежелательных звонков. Ваш номер может быть уже в списках мошенников. Но только вы решаете, станете ли их жертвой. Будьте бдительны и думайте критически. Это лучшая защита в цифровом мире. Помните, что мошенники надеются на вашу невнимательность и доверчивость.

М. Леонидова