КРАЕВАЯ ГОСУДАРСТВЕННАЯ ГАЗЕТА

СПЕЦВЫПУСК НКК № 2
МАРТ 2026 г.

Выходит
с 1 июля 2008 г.

НКК
НАШ КРАСНОЯРСКИЙ КРАЙ

УЗНАВАЙТЕ
О СОБЫТИЯХ ПЕРВЫМИ
НА НАШЕМ САЙТЕ
GNKK.RU

И В ГРУППАХ В СОЦСЕТЯХ

ШКОЛА БЕЗОПАСНОСТИ

По данным полиции Красноярского края, благодаря масштабной профилактической работе в прошлом году количество случаев мошенничества снизилось в регионе на 12,5 %, при этом четверть из них была раскрыта. Но все же этот вид преступности не побежден: мошенники продолжают обманывать тысячи людей, и цифры ущерба колоссальные. В этом спецвыпуске мы расскажем, как вести себя, чтобы не стать жертвой злоумышленников.

10 000 жителей нашего края пострадали от действий мошенников в 2025 году. Среди потерпевших больше всего людей в возрасте от 30 до 39 лет.

1 799 преступлений, совершенных с использованием IT-технологий, случилось в нашем регионе за первые месяцы 2026 года.

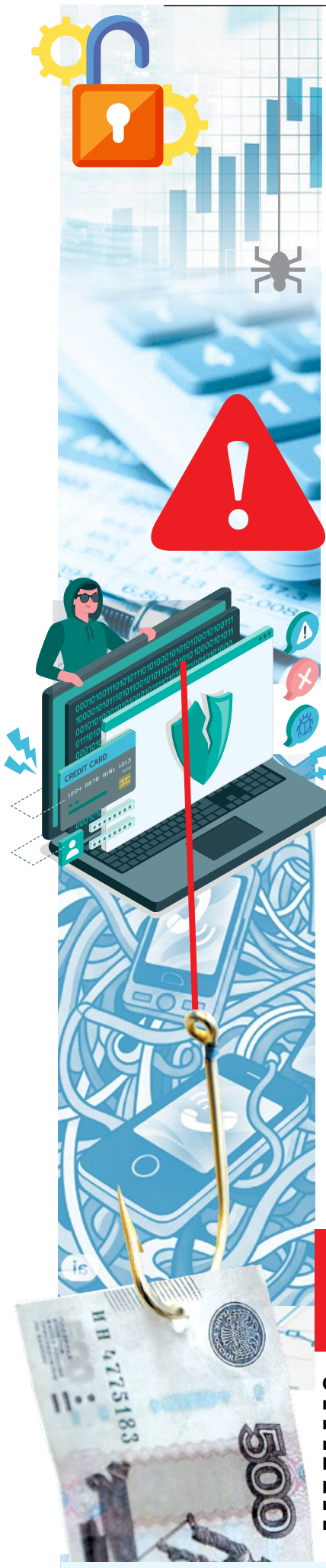
404 758 000 рублей – ущерб, причиненный потерпевшим в киберпреступлениях в Красноярском крае с начала текущего года.

32,3 % – их доля в общей структуре преступности.

Как ПРОТИВОСТОЯТЬ МОШЕННИКАМ

Иллюстрация ННК

В ЭТОМ ВЫПУСКЕ:



Полиция работает, жулики изобретают…

Киберпреступлений в крае становится меньше, но расслабляться не стоит, предупреждают в главке МВД по Красноярскому краю. Полиция работает, выявляя мошенников, но те, в свою очередь, становятся более изобретательными и все время придумывают новые способы отъема денег у населения.

В краевой полиции рассказали, что нынешний год в плане количества киберпреступлений начался относительно спокойно. Судя по статистике января, в новогодние праздники телефонных звонков от мошенников жителям края поступило на 35 процентов меньше, чем на каникулах 2025 года.

Статистика по итогам прошлого года тоже положительная: в 2025-м количество телефонных мошенничеств уменьшилось на шесть процентов, удаленных краж – на 17 процентов, на 20 процентов снизился ущерб, нанесенный злоумышленниками, – с 3,3 млрд рублей в 2024 году до 2,6 млрд в 2025-м.

На фоне общероссийских показателей наш регион в числе относительно благополучных.

– В прошлом году мы ежемесячно фиксировали до 700 киберпреступлений. С января этого года пошла хорошая динамика на снижение преступности в этой сфере. Мы зарегистрировали 436 фактов (в январе 2025-го – 676). Есть снижение и по итогам февраля, – сообщил **начальник управления по борьбе с киберпреступностью МВД России по Красноярскому краю Алексей Ткаченко.**

Такую динамику правоохранители связывают с работой, которая ведется сегодня в крае различными ведомствами. В борьбу с киберпреступниками включились не только органы внутренних дел, но и банки, правительство региона, различные ведомства, общественные организации. Полиция и прокуратура развернули серьезную профилактическую кампанию, направленную на противодействие мошенникам. Сотрудники МВД чаще, чем раньше, встречаются с жителями края – приходят на предприятия, в учебные заведения, разговаривают с людьми просто на улицах, объясняя, как не стать жертвами аферистов. Цель таких встреч – повышение правовой грамотности, информирование населения о новых жульнических схемах, уроки безопасности.

Однако в прошлом году более восьми тысяч жителей края все же пострадали от действий мошенников. Еще тысяча человек оказалась в числе потенциальных жертв: аферисты покушались на их средства, но переводы удалось остановить. При этом в группе риска сегодня все возрастные категории.

– Если раньше мы считали, что в первую очередь нужно обезопасить пожилых людей, то сейчас видим: жертвой аферистов может стать человек любого возраста, – продолжает Алексей Ткаченко. – Просто к каждому у мошенников свой подход. Начинают с маленьких детей. Воздействуют на них через приобретение игр, редких товаров, гаджетов со скидками. Студенты клюют на предложения легкого заработка. Молодых людей до сорока лет цепляют под предлогом получения дополнительных сверхдоходов с помощью инвестиций.

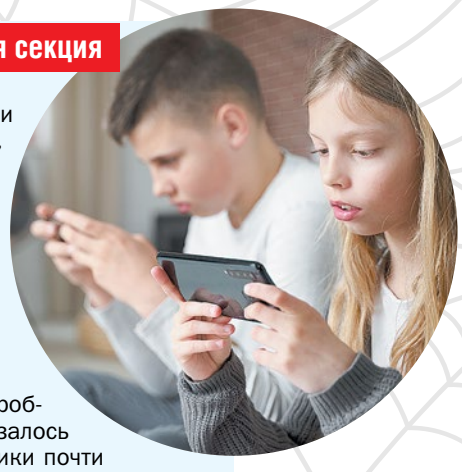
Правоохранители отмечают, что у мошенников в последнее время появился новый тренд: они активно ищут своих жертв на сайтах зна-

СПЕШИТЬ НЕ НАДО!
Мошенники часто запугивают жертву, убеждают ее молчать несколько дней, никому не рассказывать об операциях с деньгами, действовать быстро. Услышав такое, сделайте наоборот! Положите трубку и перезвоните родным и близким, коллегам, расскажите им о звонке, посоветуйтесь. А если уже перевели средства – сразу звоните в банк, предупреждайте о нежелательной операции, чтобы ее заморозили.

Крючки и ловушки

С пострадавшими от мошенников работает не только полиция, но и общественники. Они выделяют четыре возрастные группы, к которым аферисты применяют разные методы воздействия и обмана. Председатель палаты правозащитных организаций Гражданской ассамблеи Красноярского края, руководитель региональной общественной организации по защите интересов заемщиков Юрате Армонайтите рассказала об этих группах и дала советы, как обезопасить своих близких.

Детская секция



Объектам обмана от 7 до 15 лет. Мошенники работают с ними через соцсети, онлайн-игры и мессенджеры. Ребенку пишут якобы ровесники с похожими интересами, проблемами, увлечениями. С ним дружат, играют, поддерживают… И постепенно собирают информацию.

Дальше сценарий развивается по нарастающей: вовлечение в игру, просьбы о донатах, а затем самое опасное – давление и запугивание. Ребенку могут внушить, что он «совершил преступление», и заставить выполнять действия: зайти в банковское приложение родителей, перевести деньги, забрать наличные из дома, кому-то передать, уйти из дома, выключить телефон и не выходить на связь.

Ключевой инструмент преступников – страх и срочность.

Главный совет родителям: поговорите с ребенком. Не после проблемы, а до нее. Ребенок должен твердо знать: если что-то показалось странным, он может прийти к вам без страха и стыда. Мошенники почти всегда говорят: «Не рассказывай родителям». И если дети боятся наказания или крика, они будут молчать.

Важно выставить ребенку «красные флаги», которые будут сигналами опасности:

- давление и срочность («делай прямо сейчас!»);
- просьбы сохранить тайну от взрослых;
- обещания денег, призов, бонусов;
- сообщения «от имени взрослых» с просьбой помочь или перевести деньги;
- любые запросы кодов, паролей, данных карты.

! Главное правило, которое ребенок должен запомнить: если просят что-то скрыть от родителей – ЭТО ОПАСНО.

Уязвимая молодежь

В этой группе те, кому от 15 до 30 лет. Одна из самых уязвимых категорий. Здесь мошенники эксплуатируют стремление молодых людей быть самостоятельными и быстро заработать. Возможностей у них много, а опыта пока мало. Этим и пользуются аферисты.

У большинства молодых людей еще нет имущества или накоплений, поэтому давление идет по другим направлениям: оформление кредитов и займов, участие в криптопирамидах, продажа банковских карт, так называемое дропперство, когда человека используют как посредника для обналичивания или передачи украденных денег.

Триггеры, которые должны насторожить:

– «легкий заработок»,
– «ничего сложного»,
– «просто забрать и передать»,
– «оформи карту – получишь процент».

Поведетесь на них – станете соучастником уголовного преступления. Важно понимать: не бывает простых, легких и быстрых денег, это на 99 процентов криминал! А любые противоправные действия с вашей стороны, даже если вас запугивали или давили, юридически остаются вашей ответственностью.

Поэтому здесь уже не «родители разберутся». Здесь каждый отвечает сам за себя и перед законом.

! Очень практический совет: найдите в своем окружении одного взрослого, которому вы доверяете, или специалиста, с кем сможете обсуждать любую странную или «слишком выгодную» информацию. Не принимайте финансовых решений в одиночку и на эмоциях.

Финансовая зрелость – это не умение быстро заработать. Это умение вовремя сказать «стоп» и проверить, во что вас пытаются втянуть.

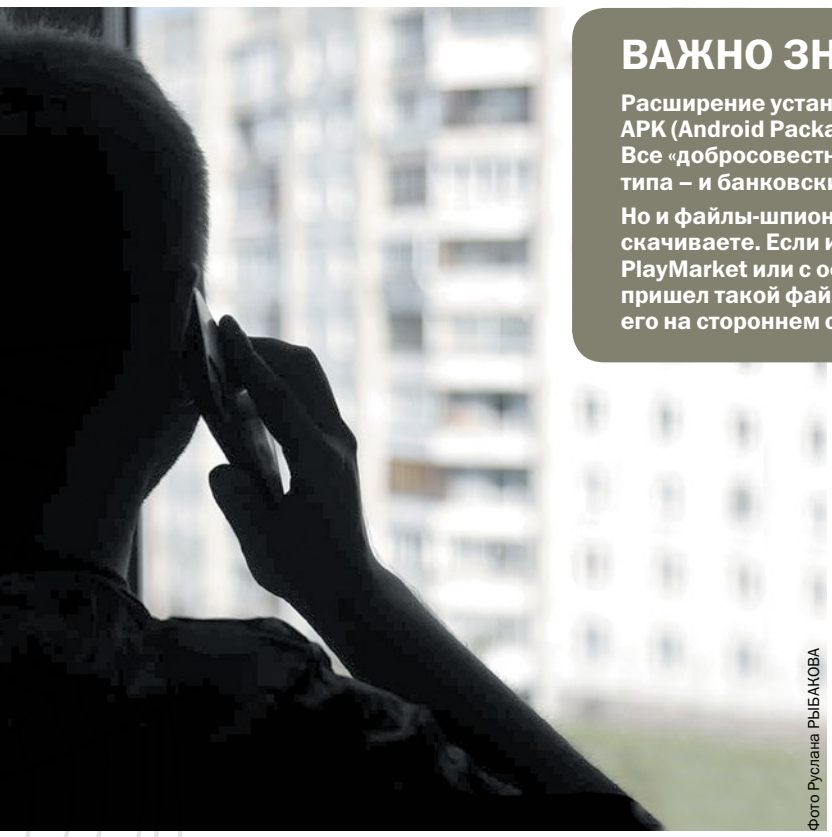


Фото Руслана РЫБАКОВА

ВАЖНО ЗНАТЬ

Расширение установочных архивных файлов для «Андроида» – это три буквы: APK (Android Package Kit). Внутри такого файла находятся компоненты программы. Все «добросовестные» приложения устанавливаются с помощью файлов такого типа – и банковские, и сервисные. Например, SberbankOnline.apk или Yandex.apk.

Но и файлы-шпионы тоже имеют такое расширение! Поэтому смотрите, откуда что скачиваете. Если из официального магазина приложений – например, RuStore, PlayMarket или с официального сайта учреждения – это одно дело. Но если вам пришел такой файл из неизвестного источника, от незнакомца, или вы скачали его на стороннем сайте, – совсем другое. Удаляйте его немедленно, не открывая!

комств, где размещают анкеты от имени привлекательных и обеспеченных парней и девушек. Пообщавшись некоторое время с потенциальной жертвой, в том числе по телефону, новый знакомый (или знакомая) открывает своей новой подруге (или другу) секрет: «Хорошей жизни я добился с помощью инвестиций – достаточно зарыть свои золотые под деревом (я подскажу, под каким), и через некоторое время… У меня и трейдер хороший есть, я вас познакомлю. Схема абсолютно надежная и проверенная!»

Сначала предлагают попробовать – рискнуть десятью тысячами. Человек рискует. И получает доход. Затем мошенники предлагают ему поставить по-крупному: внести миллион, а через неделю получить в два раза больше. Но чтобы внести деньги, нужно заплатить страховку, затем налог на прибыль и за вывод средств со счета. То есть, чтобы вывести миллион, необходимо отдать три миллиона, а то и пять.

Правоохранители предупреждают: в этой схеме дохода не дождетесь. Изначально с вами играют мошенники.

Также аферисты активно взялись за молодежь и детей.

– Студенты, обманутые мошенниками, начали приходить к нам в 2023 году, и уже третий год мы плотно работаем с этой категорией населения, – рассказывает начальник управления по борьбе с киберпреступностью. – А в последнее время аферисты перестали стесняться и совершают преступления в отношении детей. Заставляют их переводить деньги со счетов родителей, угрожая мнимым обыском, призывают помочь «спасти родителей от госизмены». Самый яркий пример – недавняя пропажа сына одного предпринимателя, которого искали по всему Красноярску.

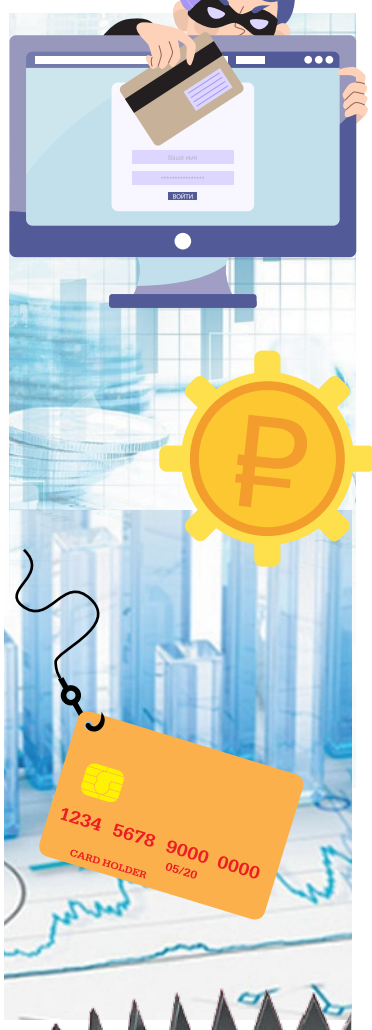
Программы-грабители

Сейчас набирает обороты новый вид киберпреступлений – с использованием вредоносного программного обеспечения. Достаточно убедить гражданина установить приложение, а дальше оно само сделает то, что нужно злоумышленнику, рассказали в полиции.

Это может быть любое приложение – банковское (точней, псевдобанковское), по увеличению скорости интернета, для обхода блокировок. Вредоносная программа открывает преступникам полный доступ к мобильному телефону – она слышит звук, просматривает видео, отслеживает геопозицию, перехватывает сообщения. Вплоть до того, что код, например, от «Госуслуг» могут видеть только мошенники, а владелец телефона даже не подозревает, что на его данные покушаются.

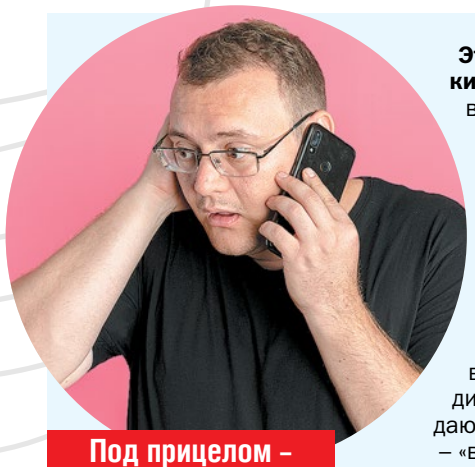
– После установки такого приложения аферисты некоторое время наблюдают за вашим устройством, и только потом начинают действовать, – поясняет Алексей Ткаченко. – Как только приходит зарплата или просто пополняется счет, все средства списываются.

Все действия происходят тайно, вы даже не подозреваете, что находитесь под колпаком у мошенников. Поэтому не нужно открывать непонятные фото и видеофайлы, даже отправленные знакомыми. Чаще всего в различных мессенджерах просят: пройди по ссылке, посмотри – ты на фото или нет, проголосуй за ребенка. Не надо этого делать! А тем более вводить свои данные для подтверждения какой-то операции. Сначала позвоните своему знакомому и спросите, действительно ли он отправлял вам приглашение, – предупреждает начальник управления по борьбе с киберпреступностью.



Юрист-правозащитник объясняет приемы воздействия мошенников на людей

Под прицелом – активные



Это люди от 30 до 60 лет. Основная цель кибермошенников. Потому что именно у этой возрастной группы уже есть деньги, имущество, стабильный доход и хорошая кредитная история. В отличие от молодежи, здесь почти не играют в «легкий заработок». Здесь работают, эксплуатируя страх.

Главные триггеры – потеря денег, работы, репутации и безопасности семьи.

Сценарии обычно выглядят так: звонки «из банка», «из полиции», «из налоговой», «из службы безопасности», сообщения о якобы взломанных счетах, попытках оформить кредит, подозрительных переводах. Человеку создают ощущение неминуемой катастрофы:

– «ваши деньги прямо сейчас выводят»;

– «на ваше имя оформляют кредит»;

– «вы проходите по делу»;

– «если не действовать срочно – потеряете все».

Дальше включается классическая схема: давление, срочность и изоляция. Вас торопят, не дают подумать, запрещают кому-либо рассказывать «в интересах следствия». И под этим психологическим прессингом люди сами переводят деньги, оформляют кредиты, продают имущество и передают средства мошенникам.

Что нужно запомнить как «Отче наш» представителям этой группы:

- никакие вопросы с деньгами, счетами или «уголовными делами» не решаются по телефону или в мессенджере;
- если вас пугают – это уже признак мошенничества;
- никогда не действуйте в режиме «прямо сейчас». Возьмите паузу. Перезвоните в банк по номеру с карты, а не по тому, что вам продиктовали. Позвоните близкому человеку. Проговаривание ситуации вслух часто мгновенно разрушает схему;
- ни один настоящий сотрудник банка, полиции или спецслужб не будет просить вас переводить деньги, брать кредиты «для сохранности» или участвовать в «операции».

! Не геройствуйте в одиночку. Введите правило: любые тревожные финансовые ситуации сначала обсуждать с близким человеком.

Не молоды, но доверчивы

Те, кто старше 60. Одна из самых уязвимых категорий. И тут дело не в наивности. Просто это поколение выросло в мире, где слову «врач», «соцслужба» или «полиция» принято было верить без сомнений. Ну и технологии для многих остаются сложными – проверить информацию в интернете, отличить поддельный номер от настоящего умеют далеко не все.

К этому добавляется еще один важный момент – одиночество. Людям не хватает общения, поэтому они легко идут на контакт, охотно разговаривают, делятся переживаниями. И этим очень цинично пользуются преступники.

Основной канал воздействия – телефон и СМС. Обычно разговор начинается резко:

– «с вашего счета пытаются снять деньги»;

– «ваш родственник попал в беду»;

– «положена выплата»;

– «срочно продиктуйте код».

И сразу – требования: назвать данные, передать информацию, перевести деньги, снять наличные и отдать курьеру.

Здесь одних предупреждений вроде «будьте осторожны» недостаточно. Из-за возраста, здоровья и стресса человек может просто растеряться. Поэтому важно регулярно быть на связи со своими родными – не формально, а по-настоящему общаться.

Практичные вещи, которые реально работают:

– у мобильного оператора можно подключить блокировку звонков и СМС с незнакомых номеров;

– включить фильтры спама хотя бы на свой телефон, чтобы вы видели подозрительные сообщения;

– наличные лучше держать в банке – со счета их сложнее снять под давлением;

– в банке можно оставить дополнительный контактный номер детей, это часто помогает остановить подозрительные операции.

Убедите своих пожилых родных: если кто-то торопит, пугает и требует денег, сначала звонить вам. Без стыда, без «не хотела беспокоить».

Легких денег не бывает

Станешь дроппером – сядешь в тюрьму!

«А что я такого сделал? Просто перекинул деньги знакомого со своей карты на другую, он меня попросил…» Такую фразу полицейские, расследующие дела в сфере киберпреступности, нередко слышат от фигурантов этих дел. Но если раньше за дропперство не предусматривалось уголовной ответственности, то с прошлого года определена строгая мера наказаний: даже разовая передача банковской карты за вознаграждение грозит тремя годами колонии, а организаторы схем могут получить до шести лет.

С 5 июля 2025 года в России вступил в силу так называемый закон о дропперах, который внес изменения в статью 187 Уголовного кодекса – «Неправомерный оборот средств платежей».

Но сначала объясним простыми словами, что за зверь такой – дроппер.

Это участник мошеннических схем, чья банковская карта или счет используются для перевода, обналичивания или отмывания похищенных у жертв денег. Термин происходит от английского drop (сбрасывать): дропперы служат промежуточным звеном, помогая преступникам скрыть следы хищений.

Дропперы работают за вознаграждение: получают либо процент от перевода, либо заранее оговоренную сумму. По оценкам экспертов, разброс тарифов за их услуги составляет от 500 руб. до 100 тыс. руб. в зависимости от «пропускной способности» счета дроппера и его амбиций. В теневом сегменте интернета встречаются предложения для «продвинутых» дропов, превышающие 200 тыс. руб.

Нет, мы не рекламируем криминальный способ заработка, мы предупреждаем: сегодня участникам таких схем грозит тюрьма!

И потом доказывай судье: «я же просто переводил деньги, а не крал их у кого-то». Будешь сидеть.

Большинство дропперов – это подростки, озабоченные поиском легких денег. Есть также безработные, пенсионеры, закоренелые должники, мигранты. Их общая черта – финансовая неустойчивость, которой искусно пользуются преступники.

Правоохранители выделяют следующие типы дропов:
- **ОБНАЛЬЩИКИ** – снимают наличные в банкоматах;
- **ТРАНЗИТНИКИ** – перечисляют средства на другие счета;
- **ЗАЛИВЩИКИ** – вносят наличные на счета и распределяют их.

Вот две самые распространенные схемы, по которым происходит вербовка в дропперы:

ЛЕГКИЙ ЗАРАБОТОК ОНЛАЙН. Под видом работодателей в соцсетях, мессенджерах и на сайтах объявлений мошенники предлагают быстрые деньги за простые переводы. Жертве поручают принимать поступившие средства на свою карту и сразу перечислять их другим получателям, оставляя себе небольшой процент.

«ОШИБОЧНЫЙ» ПЕРЕВОД С ПРОСЬБОЙ О ПОМОЩИ. Аферисты организуют поступление крупной суммы на счет ничего не подозревающего человека, чаще пожилого. Затем отправитель в панике умоляет вернуть средства, но уже другому лицу, суля благодарность за помощь.

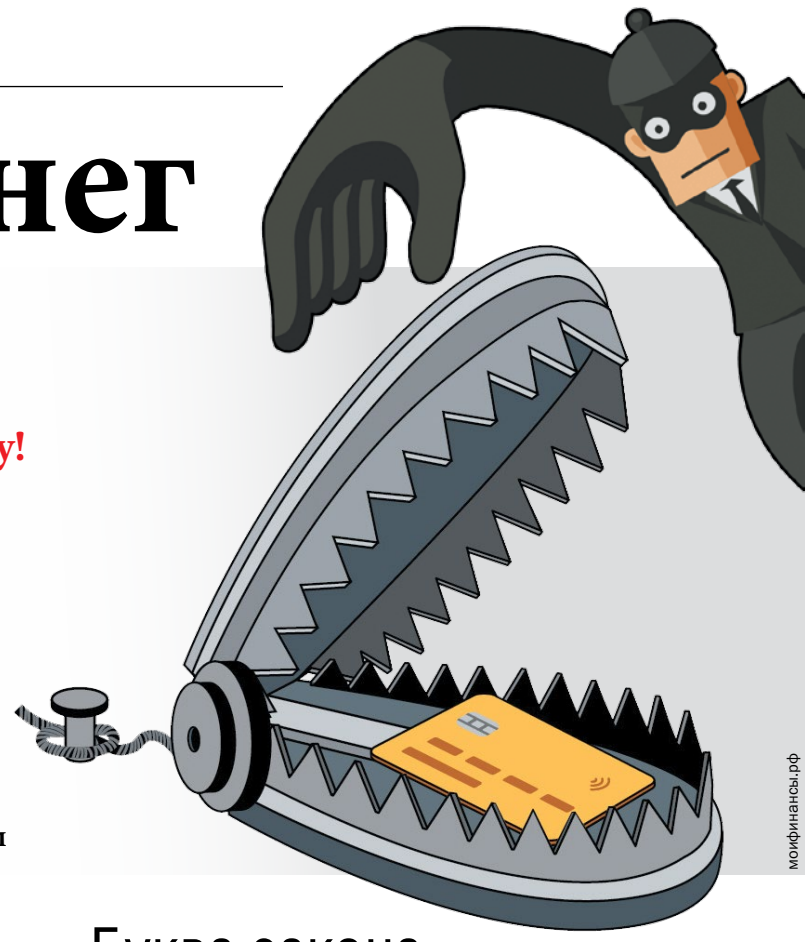
Есть и менее известные, но не менее опасные схемы, их количество зависит только от фантазии жуликов. Вот некоторые.

КРИПТОВАЛЮТНЫЙ ПОСРЕДНИК. Под видом покупателя цифровых активов мошенник получает реквизиты продавца. Затем третье лицо (дроппера) убеждают перевести деньги на эти реквизиты, представляя их как безопасный счет для сделки. Здесь дропперу также обещают процент или крипту как вознаграждение.

ФИКТИВНАЯ ВАКАНСИЯ В КОМПАНИИ. Через соцсети предлагают подработку с условием открыть карту для нужд бухгалтерии. После оформления сообщают об отмене вакансии, оставляя реквизиты карты у себя.

МАРКЕТПЛЕЙС-ОБМАН. Преступники предлагают подработку за оценку товаров, платят немного, чтобы завоевать доверие. Потом просят оформить новую карту для бонусов – на самом деле для перевода украденных денег.

«ПОМОГИТЕ ПОЙМАТЬ ПРЕСТУПНИКОВ». Мошенники, выдавая себя за оперативников, предлагают жертве стать агентом, внедрившись в преступную группу. Для этого нужно принять на свой счет украденные средства, чтобы завоевать доверие бандитов.



Буква закона

В последнее время проблема дропперства превратилась в эпидемию: мошенники создали целую индустрию по вербовке подставных лиц.

Старая редакция статьи 187 УК РФ с такими преступлениями эффективно не работала. Все понимали масштаб проблемы, но следствию приходилось идти сложным путем – через мошенничество группой лиц, или искать еще какие-то законные способы отправить дропперов под суд. Часто организаторы уходили от ответственности, жулики отделывались штрафами.

Сейчас ситуация изменилась, и **новая редакция статьи 187 УК РФ сделала дропов и дроповодов** (организаторов) **полноправными фигурантами уголовных дел.**

ПОПРАВКАМИ К СТАТЬЕ НАЗНАЧЕНЫ СРОКИ И ШТРАФЫ:

- **до трех лет колонии и штраф от 100 тыс. до 300 тыс. рублей** за передачу своих реквизитов, а также за проведение операций по указанию третьих лиц;
- **до шести лет колонии и штраф от 300 тыс. до 1 млн рублей** (с возможным дополнительным штрафом до 500 тыс.) за торговлю чужими реквизитами.

Дополнительно у мошенника конфискуют все доходы от преступной деятельности.

Поэтому трижды подумайте: нужен ли вам такой «заработок»?

А чтобы не стать инструментом преступников, соблюдайте два несложных правила:

1. **Никогда не участвуйте в цепочках «получи – переведи» даже для знакомых.** Если просят принять платеж от «клиента А» и отправить «партнеру Б», откажитесь – это классическое отмывание.
2. Проверяйте неожиданные поступления: **при получении неизвестного перевода не тратьте финансы и не возвращайте их самостоятельно – немедленно звоните в банк для отмены операции.** Трата таких средств попадает под ст. 160 УК РФ о растрате.

Из полицейской практики

19-летнюю девушку из Зеленогорска подозревают в дропперстве.

Следствие установило, что втянули ее в преступный бизнес по классической схеме: она откликнулась на вакансию в одном из популярных мессенджеров. Ей предложили заработок за передачу своих паспортных данных и реквизитов банковской карты. Мадемуазель получала чужие деньги на свою карточку и переправляла их далее по инструкции жуликов, оставляя себе небольшую комиссию за каждую транзакцию.

За одни сутки через ее банковский счет прошло приблизительно 80 тысяч рублей, за что она получила вознаграждение в сумме две тысячи. После выполнения задания контакт с организаторами оборвался.

В ходе следствия выяснилось, что один из пострадавших, житель Нижнего Тагила, отправил девушке 42 тысячи рублей в качестве предоплаты за покупку электронного девайса на торговой площадке, однако обещанный товар не получил. Деньги были направлены на счет обвиняемой и затем ушли третьим лицам.

Зеленогорские полицейские возбудили уголовное дело по статье 187 УК РФ (вот они, поправочки, – работают!), и теперь дропперше грозит до трех лет за решеткой. Продолжаются проверки на предмет ее причастности к другим эпизодам мошенничества.

Жизнь сломана. А оно того стоило?

“Нам нужен номер карты твоей мамы…

Как детские игры могут оставить всю семью без штанов

Для современных детей компьютерные игры – целый мир. Со своими законами, ценностями, кумирами. Некоторые зависают в таких играх сутками напролет. Однако злодеи в этом мире водятся не только виртуальные, но и вполне реальные. Общение ребенка с ними может обернуться финансовой катастрофой для всей семьи.

Изображение сгенерировано нейросетью

Из полицейской практики

В августе прошлого года семилетний ребенок из Ачинска отправил мошенникам больше двух миллионов рублей с карты бабушки.

Внук 54-летней женщины играл на своем телефоне в онлайн-игру. Он решил положить деньги на счет аккаунта. Для этого мальчик взял телефон бабушки и в мессенджере связался с подставными «консультантами» игры. По инструкции мошенников он вывел с банковской карты бабушки больше двух миллионов рублей и отправил на счета аферистов, которых до сих пор ищут.

Кибермошенники давно освоили игровое пространство и научились красть деньги у россиян, обманывая детей и подростков, у которых еще нет своих сбережений (хотя бывают исключения). Зато деньги есть у родителей, чьи дети увлечены онлайн-играми, где требуется покупать виртуальные предметы за игровую валюту. Ее можно приобрести не только в процессе самой игры, но и в обмен на реальные деньги. На этом и основаны схемы обмана.

От атаки мошенников с этой стороны не защищены даже финансово грамотные родители, которые соблюдают кибергигиену и не ведутся на обычные уловки аферистов. А вот дети этого еще не умеют. Мошенники входят к ним в доверие в ходе игры, а затем предлагают «прокачать» персонажа за счет игровой валюты.

Вот история одной москвички, попавшая в газеты.

«Мой 10-летний сын хорошо учится, мне всегда казалось, что он очень сообразительный мальчик. Недавно я застала его за разговором по видеосвязи с незнакомой девушкой, при этом он держал в руках мой смартфон. Заметив меня, девушка сразу отключилась. Я заподозрила неладное и сразу же проверила свой банковский счет – оттуда исчезли все мои сбережения, 390 тысяч рублей. Банк принял жалобу, но возвращать деньги отказался. Для него все выглядело так, будто я сама зашла в банковское приложение, закрыла свой вклад и несколькими переводами отправила деньги совершенно незнакомым людям. По словам менеджера, я сама виновата, потому что должна была лучше следить за тем, кто и как пользуется моим смартфоном».

Впрочем, и мелочевкой на детских картах преступники не брезгуют. Тем более что это не всегда и мелочевка. В некоторых обеспеченных семьях у детей на счетах хранятся неплохие суммы на карманные расходы.

Подросткам предлагают купить или продать игровой аккаунт, внутриигровую валюту, редкие скины (внешний вид игрового персонажа или внутриигрового предмета).

Причем все обставляют максимально правдоподобно: «у нас спецкурс», «скидка только для своих». Подросток переводит деньги напрямую «продавцу» и в лучшем случае остается без средств, в худшем – получает в придачу еще и блокировку. Очень популярна аренда аккаунтов за деньги.

Если пожилые люди часто теряют голову от общения со лжеследователями или «сотрудниками ФСБ», то дети без ума от игрового процесса и общения с фанатами любимой игры. Преступники втираются к ним в доверие постепенно, день за днем хвалят, общаются на разные темы, интересуются делами, дарят игровую валюту за выполнение простых заданий.

Затем задания становятся все сложнее и азартнее, приз – больше, и, наконец, новый «друг» уговаривает ребенка получить вознаграждение за «челлендж» настоящими деньгами на счет мамы или папы. Для этого ребенку нужно взять банковские карты и смартфон родителей, а преступники уже подскажут ему, что нужно сделать, чтобы он раскрыл для них конфиденциальные данные для доступа к счетам. Например, могут попросить сделать скриншот экрана маминого смартфона или установить на него какое-нибудь приложение. Иногда предлагают перейти из чата в видеоконференцию, где продолжают обрабатывать малолетнюю жертву.

К детям в доверие жулики втираются в чатах популярных игровых сообществ. Спросите своего ребенка, какие из них сегодня популярны и на какие темы там общаются, – узнаете много нового. Там легко завести разговор об игре, о покупке скинов, прокачке или продаже аккаунтов. А дальше уже идет вовлечение в схемы. Большая часть подростков даже не успевает понять, что общается не с ровесником, таким же геймером, а со взрослым профессиональным манипулятором.

Чтобы обмануть взрослого, мошенники пытаются его запугать: «вас посадят», «вы потеряете все сбережения». К детям другой подход. Злоумышленники формируют позитивный образ и создают атмосферу доверия. В семье бывает так, что в отношениях с родителями ребенку как раз доверия и не хватает, даже если мама и папа этого не осознают. А тут у него появляется новый душевный друг в онлайн-игре, который его понимает, сочувствует, выслушивает…

Хотя страх, говорят психологи, тоже может применяться в этой схеме, но уже после того, как ребенок почувствует доверие. Тогда манипулятор способен испугать подростка, например, потерей игрового аккаунта, если тот не выполнит очередное задание.

Словом, приемов обработки детей и подростков много – от лести и сочувствия до угроз и психологического давления. Но цель у жуликов всегда одна: получить доступ к чужим банковским картам и счетам.

Чтобы обмануть взрослого, мошенники пытаются его запугать. К детям другой подход. Злоумышленники формируют позитивный образ и создают атмосферу доверия

Три важных совета

Психологи как один твердят: чтобы у ребенка не было соблазна доверяться чужим людям и откровенничать с ними в чатах онлайн-игр и вообще в интернете, родители должны стать для него главными авторитетами. Именно с ними у него должны установиться доверительные отношения, а не с какими-то проходимцами из игрового чата.

– Нужно постоянно налаживать контакт, учить ребенка говорить о своих чувствах и переживаниях, не ругать за честный рассказ о каких-то негативных вещах. Также стоит оценить степень зависимости от онлайн-игр. Она может оказаться столь велика, что дети решаются на что угодно из-за страха потерь в виртуальном мире, – предупреждает **психолог Ксения Швецова.**

Все это правильно. Выстраивать доверительные отношения с детьми надо. Контролировать длительность пребывания в интернете – тоже. Но процесс это долгий, кропотливый. А вам надо защитить свои деньги прямо сейчас. Отключить ребенку интернет? Отобрать у него смартфон и компьютер? Вы сами понимаете, что это нереально. Поэтому вот вам три совета, которые работают сразу – здесь и сейчас.

1. **Всегда прячьте свои карты и наличные деньги в максимально надежное место – так, чтобы ребенок до них не добрался.**
2. **Смартфон тоже не оставляйте на видном месте.** Ушли из дома – прячьте или берите с собой. Поставьте на него надежный цифровой пароль для разблокировки.
3. **Установите контроль над действиями ребенка в интернете с помощью специальных приложений.** Их сегодня десятки – и для смартфона, и для домашнего компьютера. В любом магазине приложений наберите в поисковой строке: «родительский контроль». Почитайте в интернете о каждом, посмотрите отзывы и выберите самый для вас подходящий.

Это может случиться с каждым

Шесть «если» и алгоритмы действий, когда вас уже обманули

1 ЕСЛИ вы осознали, что стали жертвой мошенников

Признайте, что произошел несчастный случай.

ЗАПОМНИТЕ:
деньги утрачены не потому, что вы допустили ошибку, а потому, что мошенники совершили преступление. На вашем месте мог оказаться любой. Мошенники прибегают ко все более изощренным способам обмана, которые предугадать невозможно. Оказавшись под психологическим воздействием, бывает сложно вовремя распознать обман. Это не зависит от возраста, уровня интеллекта, образования или занимаемой должности.

Поэтому не нужно паниковать и заниматься самобичеванием, это делу не поможет. А нужно взять себя в руки и действовать.

2 ЕСЛИ проникли в ваш личный кабинет на портале «Госуслуги»

Действовать нужно быстро: срочно меняйте пароль к банковским сервисам и звоните на горячую линию портала «Госуслуги» – **8 800 100-70-10.**

Ваш личный кабинет еще не взломан, но вы получили код для доступа в него, который не запрашивали? Значит, вас пытаются взломать.

Немедленно смените пароль для доступа на «Госуслуги». Желательно, чтоб это была хаотичная комбинация букв, цифр и знаков.

Затем проверьте, не было ли подозрительных действий в учетной записи, чтобы понять, в каких организациях мошенники хотели взять кредиты. Свяжитесь с этими организациями.

Уточните, есть ли заявления от вас, и сообщите, что их подавали не вы.

3 ЕСЛИ жулики получили доступ к вашей банковской карте или банковскому приложению

В ПЕРВУЮ очередь нужно заблокировать карту и уведомить банк о произошедшем.
Позвоните на горячую линию учреждения и подайте заявление в офисе банка о несогласии с проведенной операцией. Все действия желательно выполнить в первый же день, как только вы узнали о случившемся.

Есть несколько способов БЛОКИРОВКИ КАРТЫ:

- через мобильное приложение банка;
- на сайте банка в вашем личном кабинете;
- по телефону горячей линии.

Контактный номер службы поддержки обычно указан на обратной стороне карты и на сайте банка.

! Родных, друзей и работодателя надо предупредить, чтобы они не отправляли деньги на скомпрометированную карту.

4 ЕСЛИ злоумышленники взломали телефон

Свяжитесь с мобильным оператором, все аккаунты привяжите к другому номеру, предупредите родных.

Зайдите в «Настройки» → «Приложения». Удалите все, что вы не устанавливали сами или что вызывает сомнения.

! На другом устройстве войдите в почту, соцсети, онлайн-банк и прочие сервисы и обновите там пароли. Используйте длинные комбинации с буквами, цифрами и символами.

Включите двухфакторную аутентификацию. Важно подключить СМС-код или подтверждение входа через приложение. Тогда одного пароля хакеру будет недостаточно.

Просканируйте телефон антивирусом. Если он ничего не обнаружил, возможно, вирус глубоко засел в системе. Поэтому лучше выполнить сброс до заводских параметров, создав перед этим резервную копию фото и документов в облаке.

5 ЕСЛИ атакованы ваши соцсети и мессенджеры

Предупредите родных и друзей о взломе, смените пароль, включите двухфакторную идентификацию, закройте аккаунты, отключите все привязанные к аккаунтам устройства, обратитесь в службу поддержки.
Если не можете войти на свою страницу, попросите друзей пожаловаться на аккаунт, чтобы его закрыли.

! Бывает, что взломщик успел сменить пароль, и вы оказались «за дверью». Не спешите создавать новый аккаунт. Восстановить доступ почти всегда возможно.

Если у вас была настроена двухэтапная аутентификация, используйте опцию «Забыли пароль?» на экране входа.
Сервис отправит инструкцию по сбросу на резервный e-mail-адрес, который вы указывали. Это самый надежный способ вернуть контроль. Еще хорошо помогает контрольный вопрос, который вы указали при регистрации в соцсети.

6 ЕСЛИ ваши деньги украли через поддельный сайт или интернет-магазин

Нужно подать заявление в ближайшее отделение полиции или на сайте МВД.
В нем указать подробные обстоятельства происшествия – дату, сумму перевода, кому и за какой товар переводили деньги. Приложить доказательства произошедшего: скриншоты переписки с мошенниками, их реквизиты и номера телефонов, справку о переводе денег.

Есть смысл пожаловаться на интернет-магазин в Роспотребнадзор.
Ведомство защищает права потребителей. Обращайтесь туда, если столкнулись с недобросовестным продавцом. Обращение рассматривают в срок до 30 дней. Если понадобятся дополнительные проверки, его продлят. Сотрудники Роспотребнадзора могут запросить дополнительные документы или информацию.

На этой странице мы расскажем о нескольких свежих эпизодах, связанных с мошенничеством (все случаи произошли в нашем крае), и объясним, что было потерпевшими сделано неправильно и как нужно было поступить в каждой конкретной ситуации.

Уж сколько раз твердили миру…

Было сделано так, а надо было – вот так

Жулики? Впервые слышу

В ноябре 2025 года красноярской студентке поступил звонок якобы от сотового оператора. Неизвестные убедили девушку продиктовать СМС-код и номер СНИЛС под предлогом переоформления сим-карты.

Как только разговор закончился, в мессенджере с ней связались «специалисты МФЦ» и «Центробанка»: в вашем личном кабинете на «Госуслугах» орудуют мошенники, которые уже оформляют кредит.

✗ В итоге, выполняя инструкции «кураторов», девушка в течение нескольких месяцев (!!!), вплоть до середины февраля 2026 года, получая стипендию, пенсию и выплаты, под диктовку жуликов переводила деньги через криптокошельки и виртуальные карты, которые сразу же удаляла по требованию мошенников. Ущерб составил 2,5 млн руб. Полицейским девушка призналась, что о видах мошенничества она знает плохо.

✓ Услышав по телефону от человека, которого вы знать не знаете, требование продиктовать какой-то код из СМС или сообщить личные данные по телефону, надо было просто положить трубку. Без разговоров! А в интернете нужно не только просматривать рилсы, фоточки и рецепты салатов, но и читать новости, статьи, следить за ситуацией в стране. Это полезно. Вряд ли человек, который хоть немного знаком с актуальной информационной повесткой, попался бы на такой примитивный развод, о котором сегодня рассказывают из каждого утюга.

Ключи от сейфа надо прятать!

16-летнему мальчику из Красноярска позвонили якобы из службы доставки. Подросток подумал, что это может быть подарок от мамы к дню рождения.

✗ Он продиктовал код. Ему тут же перезвонил лжесотрудник из Минцифры и сообщил, что все сбережения семьи под угрозой. Пригрозив тюрьмой и мальчику, и его отцу в случае обращения в полицию, мошенники попросили снять на видео комнаты, чтобы «задекларировать» средства. Мальчик и снял. В кадр попал сейф. Мошенники заставили его взять оттуда 10,5 миллиона рублей и передать курьеру, который назвал кодовое слово.

✓ Уважаемые родители! Объясняйте своим детям, что нельзя общаться с людьми, которые грозят им тюрьмой. А услышав такие угрозы, надо сразу позвонить папе с мамой. Выстраивайте доверительные отношения с ребенком, чтобы он в случае любой опасности не боялся обращаться к самым близким людям. Проведите с ребенком беседу: как нужно действовать в подобных ситуациях, как изощренно порой действуют мошенники. Наконец, ключи от сейфа носите все же с собой, а если там кодовый замок – код не обязательно знать детям.

Все начиналось романтично…

Жительница края, женщина вполне зрелого возраста, познакомилась с мужчиной на сайте знакомств. На фотографии он выглядел импозантно: немолодой приятный англичанин. Тщательно коверкая письменные русские слова, мужчина рассказал, что работает главным инженером на корабле в Северном море, и признался, что очень одинок. А уже на третий день общения согласился приехать в Сибирь и прожить оставшиеся дни с новой знакомой. Но чтобы добраться до порта в Норвегии, ему нужно нанять лодку до берега. Всего за 87 тысяч рублей.

✗ Женщина перевела товарищу Бендеру все свои сбережения – 43 тысячи. Моряк тут же куда-то исчез. Может, утонул, подумала влюбленная пенсионерка. И обратилась в полицию. Там объяснили, что это был не англичанин. А шансы вернуть деньги призрачны, как силуэт «Летучего голландца» в Северном море.

✓ Дорогие женщины, помните: порядочные мужчины не просят у дамы сердца денег на третий день знакомства. Тем более если представляются одинокими импозантными англичанами. В Сети такие мошенники рыщут стаями, и выдавать себя они могут за кого угодно. Но вы не теряйте голову. Научитесь быть недоверчивыми.

Изображение сгенерировано нейросетью

И снова «безопасный счет»…

Одной пенсионерке пришло сообщение в «Телеграме» якобы от ее бывшей организации, где она раньше работала: «нужно оцифровать ваш стаж». В сообщении была ссылка, после перехода по которой ей сообщили о взломе аккаунта на «Госуслугах».

✗ Затем поступил звонок в MAX: незнакомец представился сотрудником Росфинмониторинга, а потом убедил женщину перевести накопления на «безопасный счет» – наличными через NFC в банкоматы известного банка. Под контролем мошенника пенсионерка сделала десятки переводов по 200–500 тыс. руб. каждый на общую сумму 14 млн руб. Этого жуликам показалось мало. Они заставили женщину дважды слетать в другой город: там, где она жила, нужные банкоматы не работали. И уже там она сняла еще 7,7 млн рублей и перевела их жуликам. В итоге потерпевшая потеряла все свои немалые сбережения. А потом переписка в мессенджерах с «сотрудником Росфинмониторинга» удалилась. И женщина поняла, что ее обманули. В полиции пенсионерка объяснила следователям: «Я видела плакаты о мошенниках везде, но думала, со мной такого не случится».

✓ Еще раз напоминаем: сотрудники госорганов никогда не звонят гражданам через мессенджеры. А фразы «безопасный счет», «переведите ваши деньги», «идите к банкомату и снимите», услышанные по телефону от любого незнакомого человека, кем бы он ни представлялся (хоть премьер-министром страны), должны действовать на каждого разумного гражданина как удар током, как отрезвляющая оплеуха, как ведро холодной воды на голову. И человек, услышав такое, должен сразу положить трубку. Почему пенсионерка этого не сделала – остается только догадываться. Может, растерялась, может, жулики были очень убедительны. Поэтому будьте внимательны, станьте недоверчивыми, дайте себе время подумать, если на том конце провода заговорили о ваших деньгах и счетах. Положите трубку и обратитесь за советом к близким или коллегам.

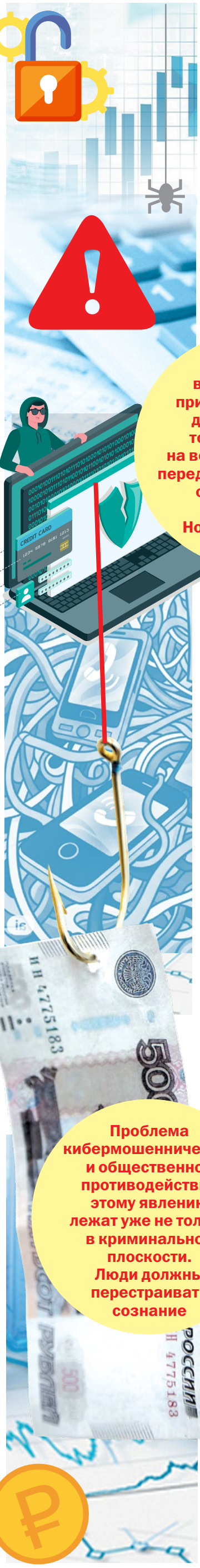
Лес с волками

Жительнице нашего края в одном из мессенджеров написал незнакомец, который представился успешным бизнесменом. Он предложил женщине вложить деньги в верное дело, которое даст хорошую прибыль.

✗ Она, как ни странно, поверила. И вложила «в дело» все свои личные сбережения, а потом взяла три кредита в разных банках. На протяжении восьми месяцев (!!!) женщина «инвестировала» более 4,5 миллиона рублей. Но прибыли так и не дождалась, а «успешный бизнесмен», выжав ее, как лимон, перестал выходить на связь. И только тогда женщина догадалась…

✓ Потерпевшую очень жаль. Но, услышав предложения от совершенно незнакомых людей куда-то «вложиться», сделать какие-то «инвестиции», поиграть на бирже и т. д., нужно не продолжать общение с этими людьми, а беспощадно и сразу их блокировать! Во всех мессенджерах, телефонах и почтовых сервисах.

ЗАПОМНИТЕ:
инвестиции – это такой темный лес с такими злобными волками, что и более подготовленных людей, со специальным финансовым образованием, там оставляют без штанов. Не лезьте в сферу, в которой совершенно не смыслите. Предложения об инвестировании ни по телефону, ни в мессенджерах не делаются. А если вы их получили от кого-то, знайте: это ШАРЛАТАНЫ!



Изображение сгенерировано нейросетью

Если раньше воры работали примитивно, ломая двери и сейфы, то сегодня у них на вооружении самое передовое электронное оборудование и нейросети. Но это те же воры

Соблюдайте цифровую гигиену

Десять тысяч человек пострадали от действий кибермошенников в Красноярском крае в прошлом году. И хотя, по данным полиции, количество зарегистрированных преступлений в цифровой сфере снизилось на 12,5 процента по сравнению с 2024 годом, ущерб гражданам от действий жуликов все еще огромен: за два месяца этого года – более 440 млн рублей! С помощью одних только правоохранительных органов проблему эту не решить, соблюдать правила цифровой гигиены сегодня должен каждый.

Привыкли к хорошему

Современные технические достижения облегчают нашу жизнь и экономят время. Но из-за того, что эти достижения имеют еще и побочные эффекты, не станем же мы от них отказываться?

Как только человечество научилось производить электроэнергию и поставило электричество себе на службу, тут же стали фиксироваться смерти и травмы от ударов током. Люди пересели на автомобили, стали передвигаться быстро и с комфортом – смерти и увечья в ДТП не заставили себя долго ждать. Причем с ростом количества автомобилей на душу населения росло и количество погибших на дорогах.

Но никому и в голову не приходит прекратить пользоваться электричеством или машинами потому, что они несут опасность и даже смерть. Мы просто стараемся эксплуатировать эти достижения прогресса грамотно, соблюдая определенные правила электробезопасности, дорожного движения…

Ровно то же происходит и в сфере кибертехнологий.

Цифровая революция принесла нам неисчислимое количество плюсов. Вспомните, как мы раньше стояли в очереди в сберкассу, чтобы всего лишь заплатить за ЖКХ. Сколько циферок надо было вписать в бланк – все эти ОКАТО и БИКи. А переводы родным и близким на почте? Снова очередь, бланки, и пока еще этот перевод дойдет…

Сейчас операции, на которые раньше уходили часы и дни, мы делаем за секунды. Купить билеты – хоть в кино, хоть на самолет, – записаться к врачу, отправить документы партнеру – все это можно сделать не выходя из дома. А наши «Госуслуги»? Один из лучших электронных сервисов в мире, многие страны нам завидуют, у них такого нет. От какой бюрократической рутины они нас избавили! В стране уже выросло поколение, которое не мыслит жизни без этого сервиса.

Из каждого утюга

Но есть и минусы. Пользуясь тем, что цифровая среда – пространство, в котором можно хорошо спрятаться или выдать себя за другого, здесь раскинули сети жулики всех мастей. В сущности, те же воры. Но если раньше эта публика работала примитивно, ломая двери и сейфы, то на вооружении современного ворья самое передовое электронное оборудование и нейросети, с помощью которых они крадут деньги у граждан, не соблюдающих правила безопасности в цифровой среде.

Хотя об этих правилах нам сегодня твердят из каждого утюга: не верьте, не бойтесь, перепроверяйте, кладите трубку, не диктуйте коды, не разбрасывайтесь личными данными…

Вряд ли у кого-нибудь повернется язык сказать, что государство ничего не делает, чтобы защитить население от кибермошенников. Сотрудники полиции и прокуратуры встречаются с людьми в трудовых и учебных коллективах. Да чуть ли не по квартирам ходят, рассказывая об уловках жуликов. О них предупреждают по радио, телевидению, в газетах. Созданы цифровые сервисы для защиты от этой категории преступников…

Но по-прежнему находятся люди, которые будто отгородились стеной от общества и живут в каком-то своем мире, не имея представления, что там, за этой стеной, происходит. Иначе как можно объяснить, что каждый божий день кто-то ведется не на сложные психологические схемы (это еще можно было бы понять), а на мошеннические приемы, о которых нам все уши прожужжали? «Вам звонят из полиции, на вашем счете замечена подозрительная активность», «продиктуйте код из СМС», «хотите заработать на бирже?» И человек послушно идет туда, куда ведут его мошенники. Снимает деньги в банкомате, переводит их на «безопасный счет». Или отдает их незнакомому телефонному аферисту, чтобы «инвестировать в бизнес». Еще одна, стотысячная по счету, жертва в стотысячный раз глотает одну и ту же наживку. В полиции пишется очередной протокол. Следователи в очередной раз перелопачивают мировую паутину в поисках воров. Все опять идет по кругу.

Новые смыслы

Психологи, анализируя действия мошенников, говорят, что те сегодня активно используют методы социальной инженерии – способы психологического воздействия на человека. Многие из них основаны на спекуляции обычными человеческими чувствами и поведенческими паттернами, такими как страх, паника, азарт, любопытство, желание легкого заработка. Все это используется для того, чтобы заставить жертву совершить нужные мошеннику действия: перевести деньги на «безопасный счет», выдать конфиденциальную информацию, взять кредит. При этом жертве не дают времени подумать, ввергают ее в ситуацию стресса, давят на нее, угрожают.

Все это пусть и хитроумные, но пока еще «человеческие» меры воздействия. Судя по тому, как стремительно развиваются технологии, впереди нас ждут более интересные времена. Расцветает, как дурман на пустыре, искусственный интеллект. И уже через год вы будете разговаривать со своим родственником по видеосвязи, не подозревая, что это не он, а цифровой фантом. Да, такое есть уже и сегодня, но по некоторым признакам опытный человек определит, что это нейросеть. Через год и опытный не отличит.

Становятся все изощренней программы-шпионы, которые преступники разными способами пытаются внедрить в ваше электронное устройство, чтобы взять его под контроль. (Поэтому нужно быть трижды внимательным, когда что-то скачиваешь на компьютер или телефон!)

Государство, как было сказано выше, ведет постоянную борьбу с новым видом преступности: в полиции и прокуратуре созданы специальные отделы по противодействию кибермошенникам, в них работают лучшие специалисты.

И все же проблема киберпреступности и общественное противодействие этому явлению лежат уже не только в криминальной плоскости. Люди должны перестраивать сознание. И здесь еще поле непаханое для психологов, социологов, даже для философов. Прогресс и его последствия – это вообще проблема, я считаю, прежде всего философская, нравственная, а потом уже техническая. На наших глазах рождаются новые смыслы и правила. Если хотите, новая киберэтика, принципы которой нам еще предстоит изучить. Что интересно, писатели-фантасты середины XX века предсказывали наступление эпохи, в которой мы сейчас живем. Но это долгий разговор, открывайте Кларка, Брэдбери, Азимова, Булычева… Удивитесь.

А пока просто соблюдайте правила цифровой гигиены. О них мы рассказываем практически в каждом номере НКК и в этом спецвыпуске – тоже.

Проблема кибермошенничества и общественное противодействие этому явлению лежат уже не только в криминальной плоскости. Люди должны перестраивать сознание

Спецвыпуск НКК № 2 «Школа безопасности. Как противостоять мошенникам». Главный редактор И. Г. Акентьева. Автор текстов Сергей Бурлаку.
Изготовлено по заказу агентства печати и массовых коммуникаций Красноярского края. Тираж 100 000 экз. Заказ № ****.
Подписано в печать **.04.2026. Отпечатано в типографии ИП Воротников Д. А., 660075, Красноярский край, г. Красноярск, ул. Республики, 51, стр. 1.