Топ-10 актуальных схем мошенников

Мошенники продолжают придумывать всё более изощрённые способы обмана, используя социальную инженерию, психологическое давление и современные технологии. Какие схемы мошенничества наиболее популярны и как защититься от них?

1. Мошенничество с пушкинской картой

Эта схема сегодня встречается всё чаще, она нацелена на держателей «Пушкинской карты». Мошенники находят подростков в социальных сетях и под предлогом помощи в выводе средств с карты выманивают у них конфиденциальные данные. Злоумышленники обещают пользователям быстрое и лёгкое получение наличных. Каждый, кто хочет обналичить деньги, должен сообщить полные данные карты, а также коды подтверждения из СМС.
Получив доступ к данным банковской карты, злоумышленники немедленно списывают все средства с баланса. После этого они прекращают общение, блокируют номер жертвы и свои аккаунты в соцсетях, чтобы скрыть следы.

Как защититься

- Никогда и ни при каких условиях не сообщайте посторонним реквизиты своей карты (номер, срок действия, CVC/CVV-код) и коды подтверждения из СМС. Это конфиденциальная информация, она должна быть известна только вам.
- Помните, что не существует легальных способов вывести наличные с «Пушкинской карты». Зачисленные на неё средства можно потратить только на культурные и образовательные мероприятия.
- Если вы столкнулись с подобным предложением, ни в коем случае не соглашайтесь. Прекратите разговор, а также сообщите о мошенниках в ваш банки в правоохранительные органы.

Правила кибербезопасности для школьников

Школьники активно используют смартфоны, что удобно и необходимо, но сопряжено с киберрисками

Читать

2. Кража аккаунта в маркетплейсе

Схема с кражей денег через взломанные аккаунты маркетплейсов активно распространяется. Мошенники, представляясь сотрудниками службы безопасности, звонят жертвам и под предлогом отмены подозрительной операции выманивают СМС-коды.

Скомпрометированный аккаунт магазина злоумышленники используют, чтобы заставить жертву сообщить коды от более важных сервисов — Госуслуг или онлайн-банка.

Получив доступ, мошенники могут:

- Оформить кредит в МФО через Госуслуги.
- Похитить деньги с ваших банковских счетов.

Как защититься:

- Никогда и никому не сообщайте коды из СМС. Настоящие сотрудники их не спрашивают.
- Не паникуйте. Прекратите разговор и перезвоните на официальный номер службы поддержки маркетплейса.
- Если звонок выглядит подозрительным, обратитесь в службу безопасности вашего банка или маркетплейса.

Безопасные покупки в интернете

Онлайн-покупки стали популярным и удобным способом приобретения товаров, но они сопряжены с рисками, такими как получение некачественных товаров или мошенничество. Чтобы избежать разочарований, важно выбирать проверенных продавцов.

Читать

3. Спасти родителей

Мошенники «целятся» в самых близких и дорогих нам людей. Под видом сотрудников полиции, ФСБ или Росфинмониторинга преступники звонят подросткам и сообщают страшную новость: родителям якобы грозит уголовное преследование за перевод денег за границу или незадекларированные доходы. Испугавшийся за маму или папу ребёнок готов на всё ради их спасения.

Злоумышленники требуют от детей провести «видеообыск» квартиры, показать на камеру все накопленные деньги и ценности, а затем передать их курьеру, чтобы «проверить» и «задекларировать». Такие совершённые под давлением действия приводят к потере семейных сбережений.

Так, в начале 2025 г. в Москве 14-летнего подростка заставили поверить в историю о «спасении родителей» и передать курьеру 300 тыс. рублей и иностранную валюту.

Как защититься:

- Объясните ребёнку, что ни один сотрудник полиции или госорганов не будет требовать деньги через курьера.
- Научите детей при любых тревожных звонках сразу обращаться к родителям.
- Установите правило: любые действия с деньгами и ценностями совершаются только после консультации с взрослыми.

Как защитить ребёнка от телефонных мошенников

Телефонные мошенники, воздействуя на детей, получают деньги родителей и ценные вещи семьи. Узнайте, как защитить ребёнка и не поерять ценные вещи.

Читать

4. Звонок на незнакомый номер

Мошенники заставляют человека самому им позвонить, чтобы обойти блокировки операторов. Злоумышленники имитируют уведомления о «взломе аккаунта на Госуслугах», «несанкционированном доступе» или «утечке персональных данных». Сообщение, которое приходит вслед за этим — через email, мессенджеры или СМС с неофициального номера — содержит требование немедленно позвонить на указанный телефонный номер «службы поддержки» или «безопасности» для экстренного решения проблемы.

Когда человек перезванивает по указанному номеру, он попадает в мошеннический контактный центр и ведёт разговор с мошенниками. Далее под предлогом «защиты счёта» или «блокировки взлома» у пользователя выманивают конфиденциальные данные: пароли, коды из СМС, паспортные данные или убеждают самостоятельно перевести сбережения на «безопасный счёт».

Получив доступ к аккаунтам и банковским приложениям жертвы, мошенники способны осуществить полный вывод средств с банковских счетов и карт, оформить кредиты и займы на имя жертвы, использовать персональные данные для дальнейшего шантажа или мошеннических схем.

Как защититься:

- Никогда не звоните по номерам из сообщений от неизвестных контактов.
- Помните: официальные службы не просят перезванивать на мобильный номер.
- Для проверки информации самостоятельно найдите официальный телефон службы поддержки на сайте организации и позвоните туда.
- В финансовых вопросах никогда не спешите. Не поддавайтесь панике. Остановитесь и критически оцените ситуацию.

Кто и зачем звонит и пишет нам с незнакомых номеров

Все мы знаем о телефонном мошенничестве, и тем не менее, попадаемся на уловки преступников. Как распознать мошенников и вовремя прекратить разговор?

Читать

5. Мошеннический VPN

Мошенники маскируют вредоносные программы под полезные расширения и VPN-сервисы, используя человеческое доверие и желание обойти ограничения. Они размещают свои продукты в официальных магазинах приложений, где после обновления внедряют шпионские функции. Такие программы могут тайно делать скриншоты, следить за действиями пользователя и красть конфиденциальные данные: банковские реквизиты, пароли, личную переписку. Это приводит к финансовым потерям, шантажу и мошенническим действиям от имени жертвы.

Как защититься:

- Избегайте использования бесплатных VPN-сервисов и прочих подозрительных «удобных» расширений.

- Не скачивайте сервисы по совету или рекламе из сомнительных источников.
- Внимательно изучайте разрешения, которые запрашивает расширение при установке.
- Не используйте непроверенные средства для обхода блокировок.
- Отдавайте предпочтение известным VPN-сервисам, чья репутация подтверждена независимыми аудитами безопасности и многолетней историей работы на рынке.
- Часто смотрите установленные расширения браузера. Удаляйте ненужные или подозрительные. Делайте это регулярно.

Как защитить своё мобильное устройство?

Мобильные устройства — наше всё. Мы практически не выпускаем их из рук, храним там контакты, сообщения, фото и видео, пароли от аккаунтов, данные банковских карт. Что сделать для того, чтобы всё это не попало в руки киберпреступников?

Читать

6. Мошенничество от имени старших по дому

Злоумышленники звонят или пишут в мессенджерах жильцам, представляясь старшими по дому или подъезду. Под предлогом формирования новой базы данных для управляющей компании или «для нужд ЖКХ» они просят владельцев квартир подтвердить свои паспортные данные и другую личную информацию.

При этом настоящие старшие по дому предупреждают жильцов, что никогда не собирают подобные сведения – так делают только мошенники.

Получив доступ к персональным данным жертвы, злоумышленники могут:

- Узнать кредитную историю и финансовую информацию.
- Войти в личный кабинет Госуслуг для оформления займов.
- Использовать данные для дальнейшего шантажа или мошеннических звонков.

Как защититься:

- Никогда не сообщайте личные данные по телефону или в мессенджерах.
- Всегда проверяйте информацию. Если получили подобный запрос, свяжитесь со старшим по дому или управляющей компанией по известному вам номеру телефона.
- Не поддавайтесь давлению, прекратите разговор. Мошенники часто торопят, не оставляя времени на размышления.

Схемы обмана для взлома аккаунта Госуслуг

Перечисляем уловки мошенников, которые они используют, чтобы получить доступ к аккаунту Госуслуг

Читать

7. «Работа» для студентов

Мошенники предлагают молодым людям работу с высоким доходом и простыми обязанностями. Для трудоустройства не требуется опыт. Под предлогом оформления злоумышленники вынуждают жертв совершить ряд действий. Например, открыть зарплатный счёт в определённом банке, пройти платное обучение или внести страховой депозит.

Цели мошенников:

- Хищение денег под любым предлогом: обучение, страховка, комиссия за перевод.
- Получение доступа к банковским счетам и снятие средств (через фишинговые ссылки или реквизиты, которые мошенники выманили у жертвы).
- Сбор персональных и паспортных данных для дальнейших махинаций, например, оформления кредитов.

Как защититься:

- Относитесь скептически к предложениям о высокой зарплате без требований к опыту.
- Никогда не переводите деньги за трудоустройство. Любые предоплаты за обучение, страховку или «служебные карты» — это стопроцентный обман.
- Не открывайте счета и не передавайте реквизиты карт по просьбе незнакомого «работодателя» в интернете.
- Прежде чем совершать любые действия, найдите официальные контакты компании и уточните условия вакансии.

Как противостоять психологическому воздействию мошенников

Телефонные мошенники обманывают людей, используя психологические приемы: создают ложное доверие, представляясь сотрудниками банков или госорганов, играют на страхах (угрожают кражей денег или проблемами у близких), давят и торопят, не давая времени подумать.

Читать

8. Похищение денег от имени «собственников квартиры»

Квартиросъемщики стали новой мишенью для финансовых аферистов. Злоумышленники рассылают сообщения от имени арендодателей с просьбой перечислить очередной платёж по новым банковским реквизитам.

Как работает схема

1. Арендатор получает СМС или сообщение в мессенджере с уведомлением об изменении реквизитов для оплаты.
2. Под предлогом технических работ или смены расчётного счёта мошенники требуют сделать срочный перевод.
3. После перечисления денег «арендодатель» перестает выходить на связь.

Как защититься:

- Вопрос о смене реквизитов всегда уточняйте у арендодателя по проверенному номеру телефона.
- Не совершайте срочных переводов без устного подтверждения реального арендодателя.
- В случае получения подозрительного сообщения немедленно позвоните собственнику жилья.
- Используйте для оплаты только те банковские реквизиты, которые были предоставлены при заключении договора.

Как узнать телефонных мошенников

Узнайте, как распознать уловки телефонных мошенников.

Читать

9. Новая MAXинация мошенников

В июле были зафиксированы случаи мошенничества, связанные с платформой MAX (она была представлена российским гражданам в качестве национального мессенджера).

Как работает схема

Злоумышленники звонят, представляются сотрудниками MAX и убеждают срочно зарегистрироваться в новом сервисе. Ссылаясь на интеграцию MAX с госсервисами, пользователя просят продиктовать код подтверждения из СМС. На самом деле код приходит с портала Госуслуг. Если сообщить его мошенникам, то они получат доступ к личным данным гражданина, его документам и финансам. Затем поступает второй звонок, и мошенники сообщают собеседнику, что его аккаунт Госуслуг взломали. Пугают оформлением кредитов и переводом денег на финансирование экстремистов. Чтобы защитить средства, жертва должна срочно перевести их на «безопасный счёт» или отдать наличные курьеру.

Как защититься:

- Помните: сотрудники MAX никогда не звонят пользователям с подобными просьбами. Подобные звонки — это попытка мошенничества.
- Если вам поступил такой звонок — сразу завершите разговор. Не поддавайтесь на угрозы и не выполняйте требования незнакомцев.
- Проверяйте информацию на официальных сайтах. При малейших сомнениях обращайтесь к специалистам сервисов.
- Никому и никогда не сообщайте СМС-коды, полученные для входа на порталы и в приложения.
- Если вы всё же сообщили свой код, срочно смените пароли, включите двухфакторную аутентификацию, свяжитесь с поддержкой. При необходимости обратитесь в банк.

Настройки конфиденциальности и приватности в мессенджерах

Мы выяснили, что эту возможность использует лишь каждый пятый владелец аккаунта. Что такое конфиденциальность профиля пользователя в мессенджере, как она связана с кибербезопасностью и почему надо задуматься о настройках безопасности?

Узнать больше

10. Украсть деньги через NFC: «бесконтактный» обман

Мошенники всё чаще используют технологии бесконтактной оплаты для кражи средств с банковских карт. Они звонят жертве, представляясь сотрудниками банка или правоохранительных органов, и сообщают, что якобы взломаны Госуслуги, зафиксированы незаконные транзакции или жертва финансирует ВСУ. Для «защиты» средств предлагают установить специальное приложение на смартфон.

После этого жертву просят приложить свою банковскую карту к телефону и ввести PIN-код. При этом мошенники успокаивают жертву: карта остаётся у неё на руках, поэтому PIN-код вводить не опасно. На самом деле приложение считывает данные карты через NFC и передаёт их мошенникам, которые в этот момент находятся у банкомата. Злоумышленники прикладывает своё устройство с таким же приложением к терминалу банкомата. Терминал считывает устройство мошенника как карту жертвы, поэтому после ввода PIN-кода преступник получает доступ к её личному кабинету и может снять все деньги со счетов.

Бывают ситуации, когда мошенники действуют иначе:

Звонят с незнакомого номера или через мессенджеры и неожиданно сообщают шокирующую новость, например: «по вашему счёту зафиксированы незаконные транзакции» или «взломана ваша учётная запись на Госуслугах» и т. п.

Мошенник стремиться запугать жертву и предлагает «спасти» денежные средства, установив на телефон специальное приложение. Направляет файл через мессенджер. Этот файл содержит вредоносное ПО, которое активируется на устройстве. После чего злоумышленник предлагает обналичить деньги со всех имеющихся счетов и внести их на специальный «безопасный счёт» через банкомат. Для этого надо приложить к банкомату телефон со включенным NFC сигналом.

Мошенник диктует цифры, с помощью которых, по его словам, жертва подтверждаете перевод на так называемый безопасный счёт. На самом деле это PIN-код от карты дропа, и человек сам вносит наличные на чужой счёт.

Словарь по теме:

NFC

Антивирус

PIN-код

Установленная под воздействием мошенников специальная программа ретранслирует NFC-сигнал на устройство дропа. Банкомат считывает сигнал телефона как карту. И это позволяет злоумышленнику после ввода ПИН-кода, который выманивают обманом,
войти в ваш личный кабинет и снять деньги со счетов.

По данным компании F6, только за первый квартал 2025 года ущерб от таких атак составил 432 млн рублей.

Как защититься:

- Не устанавливайте приложения из непроверенных источников или по ссылкам из сообщений.
- Держите PIN-код в секрете, не вводите в приложениях, которые не являются официальными банковскими программами.
- Ограничьте использование NFC, включайте его только при необходимости и отключайте после использования.
- Установите антивирусное ПО на свой смартфон и регулярно обновляйте его.
- Будьте бдительны и не доверяйте незнакомым звонкам, особенно если вас просят установить приложения или предоставить конфиденциальную информацию.