Главное о новых мошеннических схемах

Каждый год злоумышленники придумывают новые мошеннические схемы для получения доступа к деньгам граждан, применяя при этом современные технологии и различные психологические уловки:

- использование чужих данных для входа в банковское приложение;
- взлом аккаунта в маркетплейсе;
- фишинговые ссылки, сайты, QR-коды;
- поддельные службы доставки;
- скачиваемые приложения;
- звонок от попавших в беду «родственников»;
- перевод денег на «безопасный счет»;
- лжеинвестиции;
- вредоносные программы под видом VPN;
- взлом личной страницы на сайте «Госуслуги».

Чтобы защитить свои деньги и персональные данные, не стоит принимать поспешных решений, особенно если вас торопят, пугают или обещают сверхприбыль:

- не доверяйте звонкам с неизвестных номеров;
- проверяйте отправителей СМС и номера звонков, названия сайтов;
- не переходите по подозрительным ссылкам;
- не скачивайте неизвестные приложения;
- не сообщайте коды, логины, пароли;
- не переводите деньги на «безопасные счета» и так далее.

Актуальные схемы мошенников

Назовем самые популярные мошеннические схемы в 2026 году.

1. Использование чужих данных для входа в банковское приложение

Особенностью такого вида мошенничества является то, что жертва сама, находясь под влиянием мошенников, предоставляет все данные для входа в банковское приложение. Для этого злоумышленники используют социальную инженерию. Они могут звонить и представляться сотрудником банка или представителем правоохранительных органов и под разным предлогом выманивать данные:

- код из СМС;
- номер банковской карты;
- код подтверждения/пуш-уведомления и так далее.

«Эти данные мошенники часто используют для получения доступа к мобильному приложению банка, в котором уже сами могут закрывать вклады, оформлять кредиты и далее выводить все средства на счета дропперов».

2. Взлом аккаунта в маркетплейсе

Этот вид мошеннической схемы реализуется с помощью поддельных уведомлений о блокировке аккаунта в маркетплейсе из-за подозрительной операции, необходимости пройти проверку безопасности, подтвердить

данные. Выманив у жертвы СМС-код или пароль для входа в личный кабинет, злоумышленники используют взломанный аккаунт в различных целях:

- для оформления заказов от имени его владельца;
- для использования привязанных к аккаунту банковских карт;
- чтобы вынудить человека сообщить коды для входа в такие важные сервисы, как сайт «Госуслуги», онлайн-банк и похитить деньги со счетов или оформить кредиты, займы;
- для смены реквизитов в аккаунте продавца, чтобы деньги за продаваемый товар уходили на счета мошенников;
- для размещения фейкового сообщения о выгодном предложении, акциях и получения оплаты без отправки товара покупателю.
-

3. Фишинговые ссылки, сайты, QR-коды

Мошенники могут использовать фишинговые ссылки, поддельные QR-коды, создавать сайты-двойники официальных сайтов маркетплейсов, банков, государственных структур.

Цель фишинга — сбор персональных данных или кража средств со счетов.

«Жертвы под воздействием мошенников самостоятельно вводят собственные банковские и персональные данные. Например, после получения информации о выигрыше крупной суммы (чтобы его получить и уплатить налог с выигрыша, нужно заполнить форму), необходимости заполнения бланка на получение псевдоиндексаций пенсий, иных придуманных мошенниками выплат и так далее».

4. Поддельные службы доставки

Мошенники придумали сразу несколько схем обмана, связанных со службами доставки. Перечислим их.

1. Двухэтапная схема. Человеку звонят от имени службы доставки о присланном ему букете цветов или ином товаре, для выдачи которого необходимо сверить данные с курьером. Затем разговор прерывается и приходит уведомление якобы от Роскомнадзора, что звонок распознан как небезопасный. Далее звонит соучастник, представляющийся сотрудником РКН, и сообщает, что мошенникам удалось получить доступ к сайту «Госуслуги», оформить заявку на микрозаем и прочее.

Для большей правдоподобности на телефон жертвы могут начать приходить коды от микрофинансовой организации для подтверждения займа. «Сотрудник» РКН предлагает помощь в возврате доступа к сайту «Госуслуги» и отзыве микрозайма. Для этого надо зайти на портал госуслуг, прислав код из СМС. Так преступники получают доступ к личному кабинету жертвы на портале.

2. Получение сообщения о том, что заказ готов к доставке и надо подтвердить адрес или оплатить некую сумму за хранение, дополнительный вес присланной посылки. Затем приходит ссылка для отслеживания, которая на самом деле является фишинговой и ведет на поддельную страницу, схожую с

официальным сайтом компании. Для подтверждения входа запрашиваются реквизиты банковской карты, код из СМС либо логин и пароль от онлайн-банка, после чего с карты списываются средства.
3. Иногда к человеку может приехать курьер с QR-кодом для оплаты, сканируя который, получатель заказа также перенаправляется на поддельный сайт. Далее, как в предыдущей схеме, при вводе данных мошенники получают доступ к деньгам.

5. Скачиваемые приложения

При такой мошеннической схеме от злоумышленников поступает звонок по разным каналам связи, чаще всего в мессенджерах. Для убедительности может использоваться логотип банка или подпись «Техподдержка». Клиента информируют, что в личном кабинете его банковского приложения замечены новые подключенные устройства или подозрительные операции.
Далее предлагается:

- скачать якобы «сертифицированное приложение» банка для проверки телефона на уязвимости;
- перейти по ссылке на фишинговый сайт с подробной инструкцией, объясняющей, как установить приложение;
- запустить новую программу и сообщить «оператору» идентификационный номер, который является кодом доступа;
- открыть свой мобильный банк.

«После этого мошенники получают удаленный доступ к устройству, всю конфиденциальную информацию, данные онлайн-банка и пытаются похитить средства. Приложение, которое просят установить мошенники, является программой удаленного управления для телефонов».

6. Звонок от попавших в беду «родственников»

Злоумышленник по телефону представляется сотрудником правоохранительных органов и сообщает об угрозе уголовного преследования в отношении близкого родственника за перевод денег террористам, провоцирование ДТП в состоянии алкогольного опьянения или приведшего к человеческим жертвам и так далее. Для решения проблемы необходимо срочно перевести деньги по определенному номеру или реквизитам, при этом упор делается на срочность, чтобы не дать человеку времени прийти в себя.

Иногда мошенники используют дипфейки — моделируют голосовой или видеоконтент, имитируя речь человека или его изображение. В этом случае мнимый родственник сам сообщает о каком-нибудь приключившемся с ним несчастье и необходимости срочного перевода денег. При этом, как правило, он просит не перезванивать на его номер телефона и не спрашивать подробностей, так как некогда разъяснять, телефон сломан, разряжен и так далее.

7. Перевод денег на «безопасный» счет

Одна из самых распространенных мошеннических схем. В ее основе всегда лежит социальная инженерия. Позвонив, мошенник представляется сотрудником правоохранительных органов или службы безопасности банка.

Он начинает запугивать жертву, сообщая, что его банковскому счету или депозиту грозит опасность, и сейчас с ним проводится подозрительная операция, что может говорить о попытке преступников завладеть средствами.

«Далее идет просьба/требование перевести все деньги на “безопасный” счет, который на самом деле является подставным и принадлежит мошенникам».

Как заявили в Банке России, «безопасных» счетов для спасения денег не существует.

8. Лжеинвестиции

В этой мошеннической схеме предлагается вложить деньги в «выгодный проект», криптовалюту или акции с высокой доходностью. Для старта, как правило, достаточно небольшой суммы.

Для оформления предлагается перейти по ссылке на поддельный сайт криптовалютной платформы, известной компании, брокерского сервиса.

Чтобы усыпить бдительность гражданина, после внесения средств на балансе в личном кабинете может отобразиться ложная информация об успешно заключенной сделке, росте прибыли по акциям, повышении курса крипты и так далее.

Но как только пользователь решает вывести средства, появляются дополнительные условия:

- за вывод необходимо заплатить комиссию;
- доход облагается налогом, который надо уплатить заранее через сайт;
- вывод возможен только с какой-то минимальной суммы: как правило, она в разы больше, чем размер средств, находящихся на балансе, поэтому предлагается внести недостающие деньги.

Как только гражданин совершает перевод, связь с «менеджером» прекращается, а деньги уходят мошенникам.

9. Вредоносные программы под видом VPN

Злоумышленники размещают свою программу на официальном сайте магазина приложений, затем обновляют ее, добавляя шпионские функции и маскируя под VPN-сервис. Скачав VPN из сомнительного источника, владелец гаджета открывает мошенникам доступ к личной переписке, фотографиям, банковским реквизитам, паролям и так далее. В результате человек теряет деньги, становится жертвой шантажистов, от его имени могут совершаться различные мошеннические действия.

10. Взлом личной страницы на сайте «Госуслуги»

Получение кода от портала госуслуг — желанная цель многих мошенников. Для этого используются самые разные способы:

- телефонные звонки с различными вариантами обмана, когда необходимо сообщить код из СМС, на самом деле являющийся кодом от портала госуслуг: например, о взломе портала, установке домофона и заключении в связи с этим договора, блокировке сим-карты из-за истекшего срока действия договора, якобы положенных социальных выплатах, возможности пройти бесплатное медобследование в ведущей клинике и так далее);
- фишинговые сайты;
- вредоносное ПО и прочее.

На сайте «Госуслуги» хранится большой объем персональных данных, включая ФИО гражданина, дату его рождения, адрес проживания, паспортные данные, СНИЛС, ИНН, другую информацию. Через портал можно зайти в личный кабинет на сайте ФНС, оформить кредит в банке и так далее.

Советы, как защититься и сохранить свои деньги

Несколько полезных советов:

- не переходите по ссылкам из сообщений незнакомцев, поступающих в мессенджеры и на электронную почту;
- сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;
- не устанавливайте неизвестные приложения, реальные сотрудники никогда не попросят установить приложение на смартфон;
- проверьте название сайта, на который собираетесь зайти, вместо Sberbank.ru, например, мошенники могут использовать sber-bank.com, sberbak.ru или любые другие варианты;
- никогда и ни при каких обстоятельствах не сообщайте посторонним коды подтверждения из СМС, пароли и логины от личных кабинетов, реквизиты банковской карты (ее номер, срок действия, пин-код, CVC/CVV код);
- остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение; – лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор;
- никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети или мессенджере, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;
- действуйте обдуманно, не торопливо
- никогда не переводите деньги на «безопасные счета», их просто не существует.

«Если вам звонит незнакомый человек, представившись сотрудником банка, правоохранительных органов, и торопит, угрожает, переходит на тему денег и необходимости совершить какие-то действия под его руководством — это 100% мошенники. Немедленно прекратите общение»