Новые способы мошенничества в 2022 году

По итогам 2021 года объем кибермошенничества достиг рекордного уровня. За девять месяцев 2021 года злоумышленники похитили у россиян около 9 млрд рублей – примерно по 3 млрд. рублей в квартал, что в 1,3 раза больше, чем за аналогичный период 2020 года. Нет никаких оснований полагать, что в 2022 году мошенничества станет меньше и не появятся его новые виды.

НОВЫЕ ВИДЫ МОШЕННИЧЕСТВА В 2022 ГОДУ

Геополитический кризис оказался на руку мошенникам. В первые же дни после введения санкций против России и ЦБ РФ злоумышленники начали пытаться заработать на вводимых ограничениях. Схема не нова – жертве все так же предлагают перевести деньги на «безопасный счет», только мотивируют это тем, что так средства можно будет «спасти от потери после отключения России от системы международных переводов SWIFT».

При этом виде мошенничества перевести деньги с банковской карты на подставные счета доверчивым гражданам предлагают не только по телефону, но и в социальных сетях. Злоумышленники активно пользуются приемом «полуправды» – берут действительный инфоповод, кроме того, клиенты попавших под санкции банков могут испытывать затруднения с некоторыми операциями (например, оплата через Google Pay, Apple Pay), поэтому доверие к мошенническим звонкам и постам в социальных сетях возрастает.

Еще один новый способ мошенничества – сбор денег на якобы гуманитарные нужды.

НОВЫЕ СПОСОБЫ МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

Способы мошенничества с банковскими картами

Банковские карты остаются главной целью преступников, которые используют и старые способы телефонного или интернет-мошенничества, и изобретают новые виды для кражи средств граждан.

Давно известны, но тем не менее срабатывают:

- звонок из службы безопасности банка;
- сообщение о выигрыше в лотерею;
- СМС о том, что карта заблокирована.

Конечная цель мошенников всегда одна – узнать личные данные: номер карты, срок ее действия, CVC/CVV-код или коды из СМС-сообщения, с помощью которых они входят в личный кабинет онлайн-банка жертвы и переводят деньги со счетов либо оформляют на человека кредит.

В 2022 году стало известно о новом способе мошенничества с банковскими картами. Злоумышленники заманивают людей в фейковые инвестиционные проекты, а для того чтобы усыпить их бдительность, переводят на карту некоторую сумму денег, в среднем 10–15 тыс. рублей. У потенциальной жертвы возрастает доверие, снижается чувство осторожности, человек переводит мошенникам гораздо больше средств в надежде на высокий доход.

ЗВОНКИ ИЗ МВД ИЛИ СЛЕДСТВЕННОГО КОМИТЕТА

Мошенник под видом сотрудника полиции

Не самый новый вид мошенничества, но все еще остается актуальным в 2022 году. Мошенники звонят под видом сотрудника МВД, представляются лейтенантом полиции или работником следственного комитета и сообщают гражданину, что прямо сейчас с его счета происходит хищение средств или на него оформляют кредит. Для спасения денег или недопущения оформления кредита следует перевести средства на «безопасный счет» или самостоятельно оформить кредит и тут же вернуть его, опять же на якобы специальный счет. Иногда потенциальной жертве предлагают дойти до банкомата, снять

средства и передать их «сотруднику полиции», который участвует в спецоперации по поимке преступников.
Алгоритм действий:

- положить трубку;
- если на телефон поступают СМС, не отправлять ответные сообщения;
- проверить состояние счетов, карт в мобильном или онлайн-банке;
- при возникновении сомнений, подозрений – самостоятельно позвонить в банк и проконсультироваться о дальнейших действиях.

Важно! Сотрудники банка никогда не выясняют количество денег на счете или в каких еще банках у клиента открыты счета, не спрашивают CVC-, CVV-код, не предлагают перевести деньги куда-либо.

НОВЫЕ СПОСОБЫ МОШЕННИЧЕСТВА НА ПОРТАЛЕ ГОСУСЛУГ

Новые виды мошенничества через Госуслуги
С 2022 года вступает в силу нововведение – россияне смогут регистрировать сделки с недвижимостью через портал государственных услуг напрямую в Росреестре. Таким образом, распорядиться собственным домом, квартирой, земельным участком можно будет не выходя из дома, в личном кабинете Госуслуг. Казалось бы, удобно, быстро? Однако некоторые юристы и участники рынка недвижимости опасаются, что с внедрением в 2022 году этой услуги появятся и новые виды мошенничества. Ведь злоумышленники взламывают аккаунты пользователей на любых порталах, в том числе и на портале государственных услуг. Для безопасности сделок с недвижимостью используется ЭЦП (электронная цифровая подпись), но мошенники научились обходить и это препятствие. При помощи методов социальной инженерии владельца такой подписи заставляют совершить какие-либо действия или раскрыть конфиденциальные данные. Затем от имени жертвы оформляется сделка, и под залог полученной преступным путем недвижимости на подставных людей берется крупный кредит.
Также уже в 2022 году портал «Госуслуги» предупредил пользователей о новых видах мошенничества со взломом аккаунта, связанным с QR-кодом вакцинации. Мошенники звонят жертвам от имени сотрудников портала и просят граждан продиктовать код из СМС-сообщения якобы для активации или привязки QR-кода к странице пользователя. Цель злоумышленников – попасть в личный кабинет человека и завладеть его персональными данными, которые они затем используют в преступных целях, например, для оформления кредитов и займов.
Как обезопасить себя:

- настроить двухфакторную аутентификацию для входа на Госуслуги;
- наложить запрет на совершение регистрационных действий с принадлежащим гражданину объектом недвижимости без его личного участия, обратившись в МФЦ или кадастровую палату.

СПОСОБЫ МОШЕННИЧЕСТВА НА АВИТО И ЮЛЕ

Виды мошенничества на Авито
Популярные виды обмана:

- «покупатель» предлагает перевести предоплату;
- предложение обмена со ссылкой для просмотра;
- мошенничество с доставкой.

Мошенники по-прежнему атакуют пользователей сайтов объявлений. Виды мошенничества при продаже на «Авито» и «Юле» примерно одинаковы – злоумышленник звонит продавцу, представляется заинтересованным покупателем, просит номер карты для перевода предоплаты, а потом, под разными предлогами, узнает одноразовый СМС-пароль для входа в интернет-банк и списания денег с карты либо оплаты картой жертвы покупок в интернете. Другой вариант – потенциальную жертву «ведут» до банкомата, в котором якобы требуется произвести некие действия для подтверждения прохождения

предоплаты. На самом деле человек подключает к своей карте номер телефона мошенника, который получает доступ к мобильному и онлайн-банку.
Также мошенники могут прислать СМС с предложением обмена на товар, размещенный на «Авито». Фотографию объекта для обмена предлагается посмотреть, пройдя по ссылке. Не стоит этого делать, там может быть файл с вирусом, с помощью которого мошенники получат доступ к онлайн-банку, или фишинговый сайт с формой для введения персональных данных.
Существует и способ мошенничества с доставкой на «Авито» или «Юле». Продавец выводит покупателя на общение в мессенджеры и вместо собственных сервисов доставки сайтов объявлений предлагает воспользоваться сторонней курьерской службой. Мошенник узнает личные данные покупателя – Ф.И.О., адрес и номер телефона, а затем присылает ссылку на сайт курьерской службы, где нужно оплатить товар банковской картой. При этом покупателю обещают, что продавец получит деньги только тогда, когда он заберет товар у курьера. Ссылка ведет на фейковый сайт, выглядящий идентично сайту курьерской службы, а деньги уходят злоумышленникам.
Меры безопасности:

- не переходить для общения в мессенджеры, пользоваться ресурсами сайта объявлений;
- не сообщать никому такие данные карты, как CVV-код, срок действия, коды из СМС-сообщений;
- пользоваться службой доставки, предлагаемой «Авито» или «Юлой».

НОВЫЕ ВИДЫ МОШЕННИЧЕСТВА С КРИПТОВАЛЮТАМИ

Мошенничество с криптовалютами
По сведениям ЦБ РФ, в 2021 году в России выявлена 871 финансовая пирамида, более половины которых (52,7%) привлекали средства в криптовалюте или рекламировали вложения в различные несуществующие криптовалютные активы.
Однако криптовалюты – уже привычное явление для многих, не так давно появилась набирающая популярность технология NFT и новые виды мошенничества с нею. В частности, мошенники начали распространять вредоносные программы для нелегального майнинга криптовалют и кражи средств с криптокошельков через уникальные токены NFT и мобильные приложения.
В 2022 году зафиксирован и такой новый вид мошенничества, как «криптовалюта в подарок». Злоумышленники делают фишинговые рассылки и сайты-подделки с предложениями вместо традиционных наскучивших подарков удивить друзей, близких и любимых презентом в виде криптовалюты. Однако если человек перечисляет деньги за псевдокрипту, вывести деньги с ресурса не удастся.
Еще один сценарий – предложение удвоить объем своей крипты, послав на некий кошелек любую сумму и получив обратно в два раза больше. Часто такие сообщения рассылаются в соцсетях от имени известных личностей, например, Илона Маска, с пояснением, что он хочет сделать подарок своим подписчикам. Стоит ли говорить, что отправить криптовалюту на указанный кошелек можно, а вот получить назад и в два раза больше уже не получится.
Совет один – быть бдительными. Поскольку большинство граждан все же не очень хорошо ориентируется в вопросах криптовалют, стать жертвой мошенников очень просто.