**Схемы мошенничества с использованием QR-кодов**

Многие банки стали оказывать услугу – «Снятие наличных денег по QR-коду». Суть такой услуги проста: в мобильном приложении банка, установленном на телефоне клиента, можно сформировать QR-код, который нужно считать устройством банкомата – то есть клиент даже не дотрагивается до банкомата, а все операции производит в мобильном приложении. Это удобно и безопасно: не нужна пластиковая карта, не нужно дотрагиваться до кнопок и экрана банкомата, то есть мошенники не смогут похитить данные через накладки на банкоматы – так как этот этап исключен. Как удобной банковской услугой воспользовались мошенники и что надо знать, чтобы не попасть на уловки [в интервью РИА Новости](https://ria.ru/20250601/moshennichestvo-2020257184.html) рассказал Максим Семов, председатель комитета по повышению финансовой грамотности Ассоциации российских банков, эксперт проекта НИФИ Минфина России «Моифинансы.рф».

Однако и тут вмешалась социально-криминальная инженерия: мошенники начали звонить клиентам банков и, представившись работниками этих банков, сообщали, что на клиента только что был оформлен кредит и сформирован QR-код на снятие всей суммы кредита в банкомате. Доблестная служба безопасности все пресекла, но снятие наличных по QR-коду должен остановить сам клиент. Для этого ему нужно срочно перейти в приложение банка, сформировать QR‑код и прислать его скриншот.

Соответственно, если те, кто верил словам звонящего, формировали QR-код и высылали его скриншот, то мошенники моментально снимали деньги в банкомате через процедуру «Снятие наличных по QR-коду» - ведь никаких других подтверждений для этой операции не требовалось.

Сейчас банки совершенствуют процедуры и в более доступной форме рассказывают клиентам об услуге, но в целом, эта услуга изначально не учитывала приемы социально-криминальной инженерии.

Вообще, операции с помощью QR-кода удобны и безопасны при выполнении сторонами установленных условий. Слабым местом тут опять является клиент – банк максимально обезопасил процедуры, но заставить клиента соблюдать требования информационной безопасности и финансовой гигиены порой бывает трудно.

И тут кроется возможность, перспектива использования QR-кодов мошенниками: подмена статического QR-кода в магазине (когда такой код указан на наклейке на кассе, а не формируется при каждой операции новый); рекламные объявления, содержащие QR-коды (кстати, запрещенные в части регионов), которые запускают списание средств без подтверждений; наклейка подменных QR-кодов на меню в ресторанах для оплаты чаевых через QR-код (деньги уходят мошенникам, а не официантам) и так далее. Известны случаи, когда мошенники подменивали наклейки QR-кодов на прокатных самокатах, велосипедах – в общем, перспектив для развития мошеннических схем в данном методе, увы, много. Но это и означает перспективы для развития антифрод-систем, банковский систем, предотвращающих попытки хищения средств клиентов.