Как мошенники крадут деньги с помощью QR-кодов

Покупать продукты в магазине, выбирать блюда на ужин в ресторане и оплачивать коммуналку теперь можно по QR-коду. Это удобно, но мошенники научились использовать технологию в своих целях

Что такое QR-коды и зачем они нужны

QR-коды — это улучшенная версия штрихкодов, которые сканируют на кассе в супермаркетах. На QR-кодах в определенном порядке располагают черные и белые квадратики. Для нас они выглядят хаотично, но камера смартфона считывает их как двоичный код, то есть последовательность нулей и единиц.

Потом эти числа автоматически переводятся в понятные нам данные — например, ссылку на сайт или надпись.

С помощью QR-кода можно:

- перейти на сайт;
- подключиться к беспроводному интернету;
- считать текст;
- позвонить или отправить SMS по номеру, который вшит в код;
- посмотреть геолокацию.

После ухода Apple Pay и Google Pay из России такой способ кодирования данных начали активнее вводить для денежных переводов. Это удобно: покупку можно оплатить без карты.

Работает все так: на кассе магазина вы сканируете QR-код, где зашифрованы реквизиты счета компании, куда вы хотите перевести деньги. Банк, в котором она обслуживается, подключен к Системе быстрых платежей (СБП). Когда вы сканируете код, данные о счете и сумме подтягиваются в приложение банка. Вы подтверждаете перевод, и деньги уходят получателю. При этом не нужно вводить номер, срок действия и CVV своей карты и другие личные данные.

По данным ЦБ, QR-кодами для оплаты пользуется каждый третий житель страны. Технология безопасна, но в ней есть лазейки: закодировать можно фишинговый сайт, чат с мошенниками или подменные реквизиты. Этим и пользуются злоумышленники.

Мошенники снимают деньги по QR-коду в банкомате

С помощью QR-кода можно снимать деньги в банкоматах — для этого нужно сформировать код в приложении банка. Чтобы снять наличные денежные средства, достаточно просто сделать скриншот кода.

Схема обмана. Мошенники могут позвонить, представиться сотрудниками банка и сообщить, что на вас пытаются взять кредит. Чтобы отменить заем прямо сейчас, они просят перейти в приложение банка, сформировать QR-код и прислать его скриншот.

Мошенник вводит в заблуждение и говорит, что этот код нужен для защиты денег, хотя на самом деле с его помощью можно снять деньги со счета клиента. Причем никаких дополнительных подтверждений для этого не нужно.

Что делать. Не верьте людям, которые связываются с вами и представляются сотрудниками банка. Даже если их номер определяется как номер банка, собеседник говорит убедительно и знает ваши личные данные.

Скорее всего, мошенник будет вас торопить. Не поддавайтесь панике и не делайте ничего по его просьбе, даже если он настаивает, что с вашего счета могут украсть все деньги.

Лучше положите трубку и перезвоните в банк сами — так вы будете уверены, что говорите с представителем компании. Сотрудники настоящего банка не возражают, когда клиенты так делают, и спокойно продолжают разговор.

Заманивают в чаты через рекламу

QR-коды печатают на объявлениях, афишах, листовках — отсканировать их удобнее, чем набирать ссылки вручную. Но нужно быть внимательными: если код размещен на афише концерта или квитанции на оплату ЖКУ с верными реквизитами, то, скорее всего, это безопасно. Но если вы увидели на асфальте объявление, где обещают избавить от кредитов или найти высокооплачиваемую работу, переходить по ссылке может быть небезопасно.

Схема обмана. Мошенники вешают рекламные объявления, раздают листовки или рисуют граффити прямо на асфальте. Там они обещают помочь с пособиями для многодетных семей и пенсионеров, найти работу с высокой зарплатой или списать долги.

Злоумышленники указывают, что подробную информацию можно получить по QR-коду, он ведет в чат-бот в мессенджере. Там якобы для оформления пособий, заявки на трудоустройство или получения услуг мошенники запрашивают личные данные, а затем крадут деньги с карты.

Что делать. Не сканируйте QR-коды на сомнительных объявлениях, листовках или сайтах. Если отсканировали и перешли на сайт — не вводите личные или банковские данные и не давайте согласие на скачивание файлов оттуда.

Еще лучше — установите приложение, которое будет предупреждать о вредоносных ссылках или позволит копировать адрес сайта с QR-кода. Подойдут бесплатные SecScanQR, QR Scanner или QR & Barcode Scanner.

Подменяют QR-коды в заведениях

Во время пандемии многие кафе и рестораны в целях гигиены убрали меню, распечатанное на бумаге, и заменили их на электронное. Обычно это небольшая наклейка с QR-кодом, которую размещают прямо на столе, ее нужно отсканировать с помощью камеры смартфона. Тогда пользователь получает ссылку, которая ведет на PDF-файл или сайт. Звучит безобидно, но мошенники могут воспользоваться и этим.

Схема обмана. Мошенники незаметно для персонала подменяют QR-коды для меню или чаевых официанту, а также клеят свой QR-код поверх кода заведения — чтобы клиенты вместо файла с меню открывали фишинговый сайт. А вместо того, чтобы перевести чаевые сотрудникам, отправляли деньги злоумышленникам.

Подменные QR-коды могут вести на вредоносные сайты, установку программ или чат со злоумышленниками.

Что делать. Прежде чем навести камеру, проверьте, не наклеено ли что-то поверх QR-кода заведения.

Если оставляете чаевые, перед переводом убедитесь, что по ссылке верно указано название банка, сервиса онлайн-чаевых или ресторана: фейковые платежные ссылки обычно маскируют под настоящие, а название банка может отличаться от реального буквально на одну букву.

QR-код должен вести на ссылку, которая начинается не с http, а с https: последняя s говорит о безопасном подключении — secure. Значит, вы передаете данные по защищенным каналам, поэтому риск их кражи минимален.

Добавляют QR для скачивания фейковых приложений

QR-код может вести на скачивание файлов или приложений. Но не всем приложениям стоит доверять: как и в случае со страницами в интернете, их могут создать злоумышленники.

Схема обмана. Мошенники создают приложение, которое копирует дизайн и функциональность популярных площадок: банков, сайтов объявлений, государственных сервисов. А потом оставляют QR-коды на скачивание на сайтах, которые похожи на официальные, или в обычных бумажных объявлениях. Если вы скачаете такое приложение и введете в нем конфиденциальные данные, они попадут в руки к злоумышленникам.
Что делать. Скачивайте приложения из официальных магазинов приложений, самые популярные из них — App Store и Google Play. Если удобнее установить приложение, используя QR-код, убедитесь, что сканируете код на официальном сайте.

Какие еще технологии используют мошенники

Еще одна технология, которая стала широко распространена, — NFC. Она позволяет двум устройствам рядом передавать информацию друг другу без подключения к интернету. Например, с ее помощью можно оплачивать проезд транспортной картой, установить ассистента для умного дома, а в самолетах — скачивать фильмы или программы даже без интернета.

Эту технологию часто используют для бесконтактной оплаты. Скорее всего, NFC-модуль есть в вашем смартфоне, планшете и умных часах.

NFC — безопасная технология: при оплате чип передает персональные платежные данные из приложения банка в зашифрованном виде. Но мошенники пользуются тем, что в стрессовой ситуации пользователи выдают им личную информацию.

Схема обмана. Преступники звонят по телефону, говорят, что с карты якобы пытаются украсть деньги, и убеждают перевести их на безопасный счет. При этом они уверяют, что могут помочь защитить деньги, но для этого нужны личные данные — номера карт, пароль от личного кабинета, код из SMS.

Когда злоумышленники попадают в личный кабинет, они оформляют дополнительную виртуальную карту, запрашивают у вас код из SMS и переводят на нее деньги со всех счетов. В банкомате мошенники обналичивают средства с помощью NFC: банкомат считывает данные виртуальной карты с телефона мошенников, преступники вводят ПИН-код и снимают деньги.

Есть еще одна мошенническая схема, когда мошенники не запрашивают конфиденциальные данные карты. Сначала злоумышленники под видом сотрудников банка звонят человеку и убеждают, что с его карты пытаются снять деньги, а потом сообщают данные своей карты — якобы «безопасного» счета, который нужно привязать к смартфону с помощью платежной системы для бесконтактной оплаты. Затем они называют адрес банкомата с NFC-считывателем, куда просят сначала приложить карту, а потом смартфон. Жертва думает, что переводит деньги самой себе на «безопасный» счет, привязанный к ее устройству. Но пластиковая карта находится у мошенников, поэтому они могут снять с нее все деньги.

Что делать. Не доверяйте звонящему, даже если он представился сотрудником службы безопасности банка, звучит убедительно, называет вас по имени-отчеству и знает другую личную информацию.

Не называйте свои данные и ничего не делайте по просьбе звонящего. Если сомневаетесь — лучше сбросьте вызов и перезвоните в банк сами.