Мошенники в России все чаще используют QR-коды для атак на банковские счета граждан. Они выманивают эти коды, чтобы затем снимать деньги с банковских счетов жертв. Кроме того, злоумышленники распространяют фальшивые QR-коды в общественных местах, направляя пользователей на фишинговые сайты, где персональные данные и информация о счетах попадают в их руки. Эту информацию предоставили представители Роскачества.

Эксперты рекомендуют избегать использования статических QR-кодов и отдавать предпочтение динамическим, создаваемым специально для каждой транзакции. При использовании бумажных QR-кодов важно убедиться в их подлинности и проверить, что они не были заменены мошенниками. Также необходимо проверять безопасность сайтов, на которые ведут QR-коды, убедившись в наличии защищённого соединения HTTPS перед вводом личных данных.

Злоумышленники также активно используют чат-боты в популярных мессенджерах для создания иллюзии официальных государственных сервисов. Они обещают различные социальные пособия и выплаты, выманивая у пользователей личные данные и информацию о банковских счетах. Важно помнить, что никакие государственные сайты не требуют предоставления личных данных через QR-коды.

Последнее время стало известно о новом виде мошенничества, связанном с арендой самокатов. Мошенники подменяют QR-коды на арендуемых объектах, направляя пользователей на фальшивые страницы. Это позволяет им собирать личные данные и платёжные информации от несчастных жертв. Руководитель Центра цифровой экспертизы Роскачества, Сергей Кузьменко, подчеркнул, что основная уязвимость пользователей заключается в их спешке и недостаточной внимательности.

Все права защищены