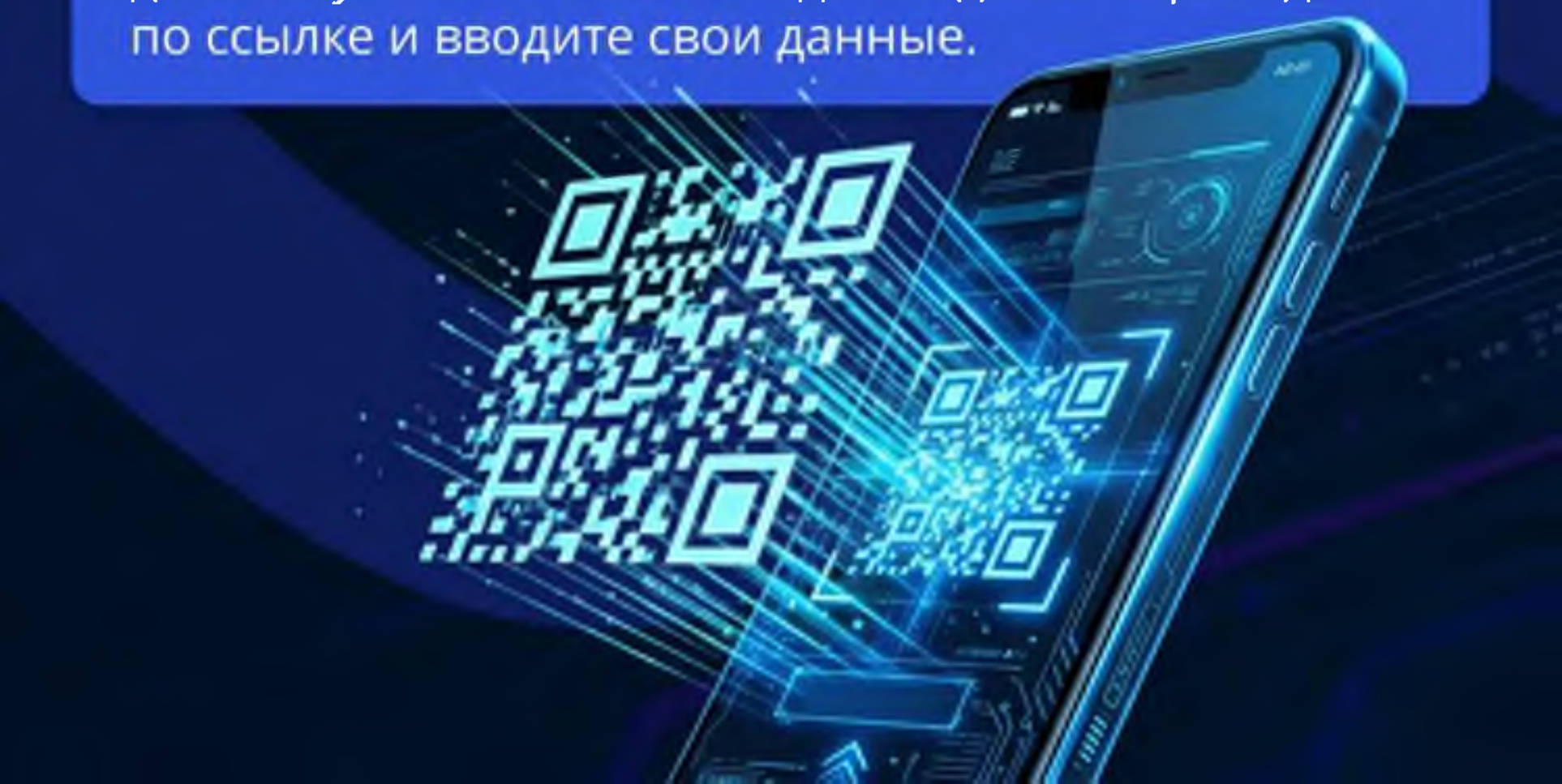


Квишинг: как мошенники используют QR-коды

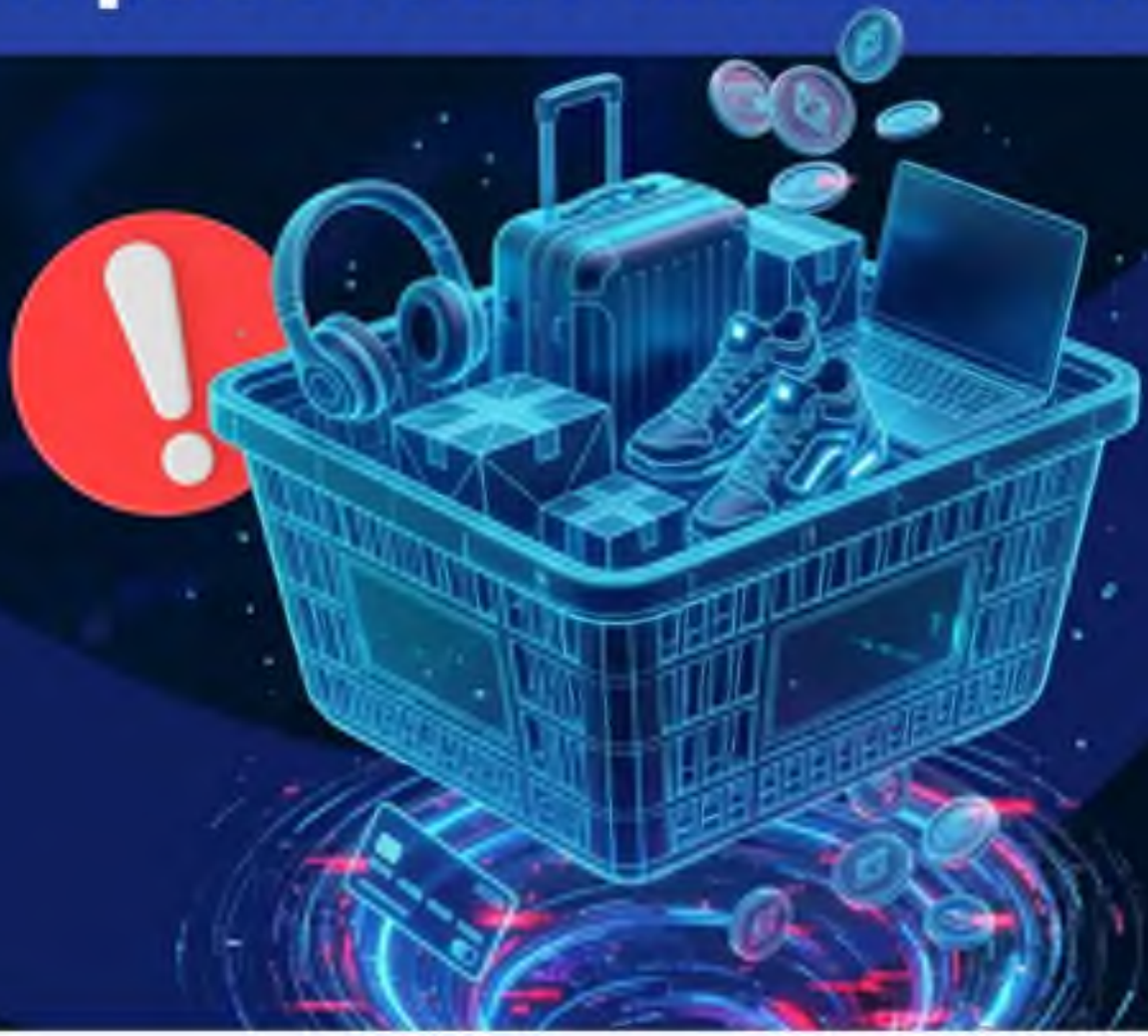
Что такое квишинг

Это разновидность фишинга — интернет-мошенничества, при котором аферисты пытаются получить доступ к данным.
Вредоносная ссылка зашифрована в QR-коде.

Сам по себе код не опасен — деньги и личные данные утекают только тогда, когда вы переходите по ссылке и вводите свои данные.



Как работают мошенники



Злоумышленники присылают QR-код — якобы для оплаты товара. Если его отсканировать, вы попадёте на поддельный сайт банка или магазина. **Как только вы введёте там номер карты или код из СМС, преступники мгновенно получат доступ** к вашим деньгам.

Почему QR-коды опаснее ссылок

РФ



При обычном фишинге пользователь видит подозрительную ссылку. **QR-код скрывает адрес до сканирования. Визуально поддельный код не отличается от настоящего.**

Схема при бронировании отелей и покупке туров

РФ

Аферисты создают фальшивые аккаунты турагентств, отправляют QR-код для оплаты. Вы переведёте деньги, но не получите ни билетов, ни подтверждения брони. В таких схемах люди теряют сотни тысяч рублей.



Где чаще всего подделывают QR-коды

Основная угроза — в интернете: при онлайн-сделках, бронировании, покупке авиабилетов. Подмена кодов на парковках и в общественных местах встречается, но редко — они там на виду, и преступникам сложнее оставаться незамеченными.



Важно!

Всегда проверяйте домен — это главная защита от квишинга!

Достаточно посмотреть на буквы и символы в адресной строке — мошенники стараются использовать домены, похожие на настоящие сайты. **Например: sber-6ank.ru вместо sberbank.ru.**



Что делать, если попались на уловку

- **Срочно заблокируйте карту через мобильное приложение** банка или по телефону его горячей линии
- **Обязательно сделайте скриншоты всей переписки с обманщиками** — это ваши главные доказательства
- **После этого сразу обратитесь в полицию**: чем быстрее вы подадите заявление, тем выше шанс найти преступников и вернуть деньги



Другие рекомендации



- **Не сканируйте QR-коды от незнакомых людей**
- **Не вводите данные карт и коды подтверждения** на подозрительных страницах
- **Используйте антивирусы** и встроенные механизмы проверки безопасности в браузерах и мобильных системах