**Новая схема хищения средств через СБП**

Мошенники начали использовать еще один способ выманить деньги. На этот раз через Систему быстрых платежей (СБП).

Обман начинается с того, что человек оставляет на сайте заявку на приобретение какого-то дорогостоящего товара. Затем ему поступает звонок или сообщение от «сотрудника магазина». Он сообщает, что товар есть в наличии и его можно купить со скидкой. Но при одном условии – оплату через СПБ по QR-коду.

После этого злоумышленник присылает в мессенджер ссылку на страницу с формой оплаты по QR-коду. Покупатель подтверждает платеж, и деньги отправляются на счет афериста.

Чтобы не стать жертвой злоумышленников:

- Следует общаться со службами поддержки онлайн-магазинов через официальные сайты или приложения.

* Не стоит сохранять для оплаты в личных кабинетах кредитные карты и карты с овердрафтом.
* Для оплаты товаров на маркетплейсах – завести отдельную карту.
Каждый пятый мошенник использует в своих схемах мессенджеры за 2023 год доля таких атак выросла вдвое: с 12 до 22,5%.

Почему мошенникам так нравятся мессенджеры? Там нет систем фильтрации подозрительных звонков в отличие от сотовых операторов.
Собеседник может скрыть свой номер, а вместо этого поставить любой аватар и подпись. Например, название и логотип банка, интернет-магазина, портала «Госуслуги» или данные не подозревающего об этом человека.
У мошенников могут быть разные легенды: обычно они выдают себя за следователей, сотрудников организаций или ведомств. Случается, даже, что они пишут сотрудникам организаций якобы от имени начальства. Цель у них одна — выманить деньги и секретные данные.

Поэтому важно соблюдать правила информационной гигиены — не сообщать полные реквизиты карты, коды из СМС и другие секретные данные.
И, конечно, перепроверять информацию, если с вами разговаривают о деньгах и торопят. Даже если это сообщение от кого-то из старых знакомых.