

**ПОПУЛЯРНЫЕ СХЕМЫ
МОШЕННИЧЕСТВА ЧЕРЕЗ
ПЛАТЕЖНЫЕ ПЛАТФОРМЫ**

САЙТЫ-КЛОНЫ ПОПУЛЯРНЫХ ИНТЕРНЕТ-МАГАЗИНОВ

Злоумышленники создают поддельные сайты-копии настоящих, чтобы добраться до платежных реквизитов пользователя. Фальшивку почти невозможно отличить от оригинала. Жертва вводит данные карты на фейковой странице оплаты — и они оказываются в руках мошенников.



ФАЛЬШИВЫЕ СТРАНИЦЫ СБП

Мошенники используют поддельные формы для имитации интерфейса системы быстрых платежей. Чтобы усложнить отслеживание, аферисты могут присылать QR-коды или ссылки на региональные платежные системы.



ФАЛЬШИВЫЕ САЙТЫ ДЛЯ АРЕНДЫ НЕДВИЖИМОСТИ

Часто злоумышленники размещают объявления об аренде на реально существующих площадках, но сразу переводят общение в мессенджеры. Когда дело доходит до бронирования — отправляют жертву на поддельный ресурс.



ПРЕДЛОЖЕНИЯ ПОКУПКИ НА СОМНИТЕЛЬНЫХ САЙТАХ ИЛИ В БОТАХ

Мошенники создают сайты-однодневки с «крайне выгодными» товарами, билетами или услугами. Жертва оплачивает товар, но он не приходит. Может потребоваться дополнительная «предоплата», затем связь с продавцом обрывается.



КАК ОБЕЗОПАСИТЬ СЕБЯ?

- Не доверяйте низким ценам на товары и услуги. Совершайте покупки на официальных ресурсах.
- Скачивайте приложения только в проверенных источниках.
- Не переходите по сомнительным ссылкам от незнакомцев.

