Мошенничество с доставкой («Посылка с сюрпризом»).

С развитием технологий мошенники не стоят на месте. Они активно изучают цифровые привычки россиян, используют уязвимость психологии и внедряют сложные схемы обмана. Если раньше классическим мошенничеством считался звонок от «лжебанкира», то сегодня арсенал злоумышленников стал гораздо шире и изощреннее. Одним из наиболее распространенных цифровых угроз является мошенничество с доставкой.

Эта схема стала массовой с ростом популярности онлайн-шопинга.

Как работает:

Вам приходит SMS-сообщение от имени известной курьерской службы или почты России. В нем говорится, что вашу посылку не могут доставить из-за неполной информации, неоплаченного сбора или проблем с таможней. Для решения вопроса предлагается перейти по ссылке, которая ведет на фишинговый сайт-клон официальной службы.

Что требуют:

На поддельном сайте вас просят «уточнить данные», ввести реквизиты банковской карты для «оплаты небольшого сбора» (обычно 50-500 рублей) или скачать вредоносное приложение под видом «трекера для отслеживания». После ввода данных злоумышленники получают полный доступ к вашему счету.

Как защититься:

- Всегда проверяйте трек-номер посылки напрямую в личном кабинете магазина или на официальном сайте курьерской службы.
- Помните: настоящие курьерские службы никогда не просят перевести деньги по SMS для получения посылки.

Разъяснение подготовил прокурор Клинцовского района:

Василий Родин