

Полиция предупреждает: осторожно мошенники!

СМС-атака стала инструментом новой многоходовой схемы, которую придумали мошенники. Представьте, вам присылают более сотни СМС с интервалом в несколько секунд. Среди этих сообщений скрывается код, который служит аналогом подписи под договором на получение онлайн-займа. Именно им хотят завладеть аферисты.

Преступники указывают телефон человека в заявке на заем и одновременно регистрируют на этот номер множество аккаунтов на разных сайтах: онлайн-магазинов, аптек, маркетплейсов, провайдеров услуг. Десятки, а иногда и сотни кодов подтверждения сыплются один за другим, это введет в замешательство кого угодно. В потоке сообщений трудно заметить, что одно из них – от микрофинансовой организации.

Пока СМС продолжают приходить, мошенники выходят на связь через соцсети или мессенджер и пытаются выманить данные. Например, они могут представиться сотрудниками оператора связи, предупредить о техническом сбое и попросить прислать скриншоты сообщений. Они якобы нужны, чтобы разобраться в проблеме и прекратить лавину спама.

Не стоит доверять незнакомцам, которые якобы стараются вам помочь. Любую информацию нужно перепроверять. Например, если на вас выходят от имени оператора связи, лучше выяснить, в чем проблема, а затем прекратить разговор и самостоятельно перезвонить на официальную горячую линию.

И конечно ни в коем случае нельзя никому передавать секретные коды и пароли из СМС и push-уведомлений от банков и других финансовых организаций. И нужно внимательно следить за тем, чтобы не выдать их случайно.

В случае, если Вы стали жертвой мошенников, обратитесь лично в ближайшем отделении полиции.

УУП МО МВД России «Макарьевский»