**Новые способы мошенничества.**

В 2020 году на территории Лоухского района зарегистрировано 28 тяжких преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Большую часть данных преступлений составляют дистанционные хищения денежных средств с банковских счетов граждан (27 преступлений).

В 1 полугодии 2021 года на территории района зарегистрировано 9 таких преступлений.

Несмотря на неоднократное освещение в средствах массовой информации способов мошенничества, граждане продолжают доверять злоумышленникам, которые изобретают все новые способы обмана.

Приведем некоторые новые способы дистанционного мошенничества.

**Звонок от «оператора».**

Мошенники представляются операторами популярных сотовых компаний и пытаются узнать у граждан их персональные данные, в т.ч. данные паспорта. Свой интерес к данным граждан «операторы» объясняют необходимостью проверки личности абонента.

В случае, если граждане отказываются назвать свои данные, мошенники начинают уверенно перечислять все негативные последствия, если граждане не сообщат свои данные, в т.ч. необходимость личной явки в офис для подтверждения личности, заполнение документов, а также угрожают отключить им сотовую связь и заблокировать sim-карту.

Как правило, заполучив персональные данные граждан, мошенники оформляют микрокредиты или регистрируют фирмы-однодневки.

**Фиш-хейт.**

Мошенники создают закрытый аккаунт в социальных сетях, с которого, для привлечения внимания к своей странице, оставляют оскорбительные комментарии к постам пользователей.

Доверчивые пользователя, заинтересовавшись, кто оставляет им такие комментарии, пытаются выяснить личность недоброжелателя, переходят по ссылке из профиля и вводят свои логины и пароли для аутентификации на подставном сайте, напоминающем популярные соцсети.

Таким образом мошенники получают контроль над аккаунтом пользователя в социальной сети.

Наиболее распространен данный способ мошенничества в Instagram.

**«Представители банка».**

Мошенники, которые звонят гражданам от лица банковских работников, придумали новую схему.

Злоумышленники говорят, что на рассмотрении в банке находится заявление о смене номер мобильного телефона, на который приходят уведомления по банковской карте.

Для отмены данной операции мошенники предлагают назвать данные банковской карты (номер, срок действия, имя держателя и т.п.), а также назвать свое кодовое слово.

Таким образом они запугивают клиентов банка у которых выведывают данные банковских карт и впоследствии списывают с них денежные средства.

Аналогичным образом мошенники вводят в заблуждение граждан, сообщая, что поступила заявка на оформление кредита на их имя. После чего также предлагают сообщить персональные данные и реквизиты банковских карт в целях аннулирования заявки на предоставление кредита.

**Как не стать жертвой мошенников.**

В первую очередь нельзя никому сообщать сведения о своих банковских счетах и банковских картах.

Нельзя вводить на сомнительных сайтах данные своих банковских карт. Совершать покупки в сети Интернет только на проверенных сайтах. При этом внимательно проверять даже знакомые сайты что бы не попасть на сайт-двойники.

Нельзя переводить денежные средства с одного счета на другой по указанию кого-либо.

В случае возникновения каких-либо вопросов или подозрений необходимо самостоятельно обратиться в отделение банка.

Прокуратура Лоухского района призывает граждан к большей бдительности и внимательности к своим персональным и банковским данным.