**Тюкалинская межрайонная прокуратура разъясняет**

**Как не стать жертвой кибермошенников**

Цифровые технологии дают новые возможности и облегчают многие операции с денежными средствами, в том числе провести онлайн-переводы и оплатить покупку товаров, получить государственные услуги (через официальные приложения банков и государственных органов). Вместе с этим, значительно возросло количество граждан, ставших жертвами мошенников, в данном случае кибермошенников.

Наиболее часто граждан вводят в заблуждение при поступлении телефонных звонков от якобы службы безопасности банков, в связи с несанкционированными списаниями денежных средств со счетов. Полагая, что звонок поступил во спасение их сбережений, они передают преступным элементам сведения о кодах, поступающих в смс-сообщениях, о реквизитах банковских карт (включая CVV-код). В настоящее время преступники активно используют также и другой способ хищения денег путем «вскрытия» личных страниц в социальных сетях («ВКонтакте», «Одноклассниках» и др.), ведения переписки от чужого имени, в результате чего денежные средства переводятся лицу, выступающему от имени пользователя, находящегося в категории «друзей», который якобы просил деньги в долг и т.п.

В связи с этим, гражданам необходимо проявлять повышенную бдительность при общении с неизвестными лицами при использовании средств телекоммуникаций. Нельзя никому сообщать (даже работникам банков) реквизиты банковских карт, пароли, коды, пин-коды, CVV-коды, коды из смс- сообщений. При поступлении звонка от сотрудников банка прервать разговор и самим перезвонить в банк. Нельзя передавать банковские карты третьим лицам. Незамедлительно сообщить в банк об утрате банковской карты, мобильного телефона с «привязанной» к номеру банковской картой или о смене телефонного номера. Не оставлять без присмотра телефоны, с «привязанной» к номеру банковской картой. При заключении сделок купли-продажи, онлайн оплату проводить только с проверенными контрагентами.

22.11.2024