**Прокуратура Киренского района информирует:**

Способы совершения хищения с использованием информационно-коммуникационных технологий постоянно совершенствуются, что создает определенные сложности для правоохранительных органов в раскрытии преступлений указанной категории.

Одним из самых распространенных видов хищения является телефонное мошенничество. Как правило, от имени сотрудников банков России, мошенники сообщают потерпевшему о несанкционированных списаниях денежных средств с банковских карт или сообщают о необходимой блокировки банковской карты. Далее, мошенники, войдя в доверие, просят предоставить определенные данные карты владельца или сообщить смс-код, поступивший на его телефон. В результате чего, как правило, происходит списание денежных средств с банковского счета.

Нужно помнить, что сотрудники банка при общении с клиентом банка никогда не просят сообщить ему реквизиты банковской карты.

Способы совершения хищения с использованием информационно-коммуникационных технологий постоянно совершенствуются, довольно распространенным способом мошенничества на сегодняшний день является мошенничество в социальных сетях. В данном случае мошенники, с помощью взлома персональной страницы в социальных сетях, обращаются от лица потерпевшего с просьбой о помощи, а именно о переводе денежных средств на банковский счет, либо просят реквизиты карт, чтобы перевести деньги.

**Способы совершения хищения банковских средств с использованием информационно-коммуникационных технологий разнообразны, необходимо соблюдать определённые правила.**

1) заходите в интернет-банк только с официального сайта банка;

2) установите и регулярно обновляйте антивирусное программное обеспечение на своем компьютере (планшете, смартфоне);

3) никому не сообщайте логин и пароль, используемые для входа в интернет-банк;

4) регулярно меняйте пароль, при этом рекомендуем использовать максимально сложный пароль, состоящий из букв разного регистра и цифр. Чем проще пароль, тем проще его взломать и даже угадать (если, например, в качестве пароля вы используете свою дату рождения или имя и т.п.);

5) если банк предоставляет возможность использовать дополнительные средства идентификации для входа в интернет-банк и (или) для подтверждения проводимых операций (одноразовые пароли, смс-коды и т.п.), используйте их;

6) храните одноразовые коды в недоступном для третьих лиц месте, никому их не сообщайте;

7) в случае возникновения нештатных ситуаций, например «зависание» системы, появление сообщений об ошибках, подозрительное изменение внешнего вида сайта, невозможность получения доступа к интернет-банку и т.п., срочно сообщите об этом в контакт-центр банка.

**Будьте внимательны и осторожны при общении с посторонними лицами.**