В современном обществе одним из самых распространенных видов преступлений является мошенничество, то есть хищение чужого имущества путем обмана или злоупотребления доверием, в том числе совершенное дистанционным способом с использованием информационно-коммуникационных технологий. Данный вид мошенничества совершается как правило без физического контакта с потерпевшим.

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

Чтобы не стать жертвой кибермошенников необходимо придерживаться некоторых правил.

Защищайте компьютер от вредоносных программ. Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами.

Чтобы Ваша работа в Интернете была более безопасной:

- установите современное лицензионное антивирусное программное обеспечение, регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы;
- устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки;
- никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников, подозрительные файлы лучше немедленно удалять;
- используйте сложные пароли, не связанные с вашей жизнью;
- расширение файла – это важно! Особую опасность могут представлять файлы со следующими расширениями: *ade, *adp, *bas, *bat; *chm, *cmd, *com, *cpl; *crt, *eml, *exe, *hlp; *hta, *inf, *ins, *isp; *jse, *lnk, *mdb, *mde; *msc, *msi, *msp, *mst; *pcd, *pif, *reg, *scr; *sct, *shs, *url, *vbs; *vbe, *wsf, *wsh, *wsc.

Мошеннические действия часто совершаются с использованием банковских пластиковых карт. Помните, что Ваша безопасность в Ваших руках, поэтому:

- никому и никогда не сообщайте ПИН-код карты;
- выучите ПИН-код либо храните его отдельно от карты;
- не передавайте карту другим лицам – все операции с картой должны проводиться в Вашем присутствии;
- по всем возникающим вопросам обращайтесь в отделение банка;
- насторожитесь, если от Вас требуют немедленных действий или представляется чрезвычайная ситуация;
- если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка.

Мошенничество совершается также с использованием телефона. Будьте бдительны:

- не общайтесь с посторонними людьми по телефону и не сообщайте номера своих банковских карт, коды доступа, смс - сообщения которые поступают к Вам на телефон;
- перед тем как перевести денежные средства на номер сотового телефона лица, которое сообщает Вам, что он Ваш родственник и попал в трудную ситуацию – свяжитесь с родственниками по достоверно известным Вам телефонам и уточните информацию;
- если Вам сообщили, что Ваша карта заблокирована обращайтесь в отделение банка, не выполняйте указания по телефону.

Мошенники знают психологию людей. Будьте внимательны и осторожны при общении с посторонними лицами.