**Механизмы защиты прав граждан от преступных посягательств с использованием информационно-телекоммуникационных технологий**

Практически каждый человек использует цифровые технологии. Удобно, не выходя из дома, при помощи сотового телефона оплатить услуги, перевести денежные средства родственнику, знакомому. Но помимо положительных аспектов внедрение цифровых технологий имеет и негативную (криминогенную) сторону.

На государственном уровне принимаются меры для защиты граждан от противоправных посягательств на денежные средства, находящиеся на банковских счетах. Например, усилено наказание за хищение денежных средств с банковского счета или электронных денежных средств до 6 лет лишения свободы.

Мошенники используют различные схемы, вынуждая жертву сообщить необходимую им информацию либо совершить ряд действий. При этом мошенники используют человеческие слабости – сострадание, обеспокоенность за близкого человека, жалось, алчность и т.д.

 Остановимся на самых распространенных схемах телефонного мошенничества.

«Родственник попал в беду (задержан сотрудниками полиции, совершил дорожно-транспортное происшествие)». В данной ситуации мошенники стремятся получить денежные средства путем внезапного сообщения о беде, не оставляя жертве время обдумать действия, т.к. близкий человек в беде и надо принимать решения быстро. Мошенники сообщают о том, что ситуацию можно урегулировать за определенную сумму денег, которую необходимо перевести на банковский счет или по номеру телефона.

«Розыгрыш призов». На телефон поступает СМС-сообщение, звонок о выигрыше, например, автомобиля. Но есть нюанс, для его получения необходимо перевести денежные средства за госпошлину, оформления документов, выполнить определенные действия с банковским счетом, результатом которых является списание денежных средств на счет мошенников.

«СМС-просьба». Абонент получает на мобильный телефон сообщение: «У меня проблемы, позвони по такому-то номеру, если номер не доступен, положи на него такую-то сумму и перезвони». Человек пополняет счет  и перезванивает. Телефон по-прежнему не доступен, а деньги вернуть уже невозможно.

«Продажа имущества на интернет-сайтах». При звонке на телефон, размещенный на Интернет-сайте (Авито, Дром и др.), правонарушитель просит сообщить данные карты для перевода денежных средств в качестве задатка за товар. После сообщения данных карты происходит списание денежных средств.

Это незначительная часть преступных схем. Чтобы уберечь себя от мошенников необходимо соблюдать несколько правил:

- не доверять звонкам и сообщениям о том, что родственник находится в беде. Как показывает практика, звонок этому родственнику помогает развеять все сомнения.

- не перечислять денежные средства при получении СМС-сообщений.

- не следует сообщать по телефону сведения личного характера.

Противостоять мошенникам возможно лишь повышенной внимательностью, здравомыслием и бдительностью. Помните, что ни одна организация, включая банк, не вправе требовать реквизиты Вашей карты включая CVV-код!