Способы защиты граждан от преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

 Век информационных технологий не мог не отложить отпечаток на существующие системы расчетов. Призванные к упрощению и унификации таких процедур электронные средства платежа стремительно вошли в жизнь практически каждого из нас, что способствовало и распространенности хищений в этой сфере.
 Среди наиболее распространенных способов хищений выделяет:
 - использование злоумышленниками индивидуальных данных банковских карт пострадавших для осуществления расчетов в преступных целях. Такие ситуации возможны при компрометации этих карт в результате раскрытия их данных третьим лицам;
 - двойное списание, характеризующееся тем, что потерпевший передает банковскую карту продавцу (оператору, официанту, заправщику), которую тот дважды проводит через платежный терминал под предлогом ошибки при первоначальном платеже;
 - хищение при бесконтактной оплате, в тех случаях, когда похитители оперируют собственными бесконтактными считывателями или терминалами, прислоняя их к карманам и сумкам;
 - хищение с использованием дубликата сим-карты мобильного телефона, которое осуществляются путем предварительного выяснения преступниками номера сим-карты, к которому привязаны банковские карты и изготовления ее фальшивого аналога с последующим списанием денежных средств;
 - хищения посредством использования информации о банковских картах, предоставленных похитителям самими пострадавшими для оплаты продаваемых ими товаров;
 - распространенный характер носят хищения, связанные с обманом доверчивых граждан, когда похитители, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившихся в их жизни неблагоприятных ситуаций;
 - отмечены случаи мошенничества, при которых похитители просят о перечислении денежных средств или оказании возмездных услуг под предлогом различных нужд органов государственной власти, а также правоохранительных органов.
 **Чтобы не оказаться жертвой мошенников необходимо знать следующее:**
 - сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;
 - ни при каких обстоятельствах не сообщать данные вашей банковской карты, а так же секретный код на оборотной стороне карты;
 - хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;
 - не сообщать пин-код третьим лицам;
 - остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;
 - лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;
 - внимательно читайте СМС сообщения приходящие от банка;
 - никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС сообщении от банка;
 - помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в СМС сообщении от банка;
 - сотрудники банка никогда не попросят вас пройти к банкомату;
 - если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;
 - не покупайте в интернет – магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;
 - никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;
 - в сети «Интернет» не переходите по ссылкам на неизвестные сайты;
 - действуйте обдуманно и не торопливо.

Заместитель прокурора Гурова Е.А.