Информационное сообщение о видах и способах совершения преступлений в отношении граждан путем обмана и злоупотребления доверием.

Злоумышленники при совершении преступлений используют сеть интернет, абонентские номера, как инструменты для их совершения. Звонят гражданам под различными предлогами, представляясь сотрудниками службы безопасности банка, сотрудниками иных государственных и негосударственных организаций, используя при совершении данных преступлений так называемую IP телефонию и подмену номеров, то есть могут позвонить с якобы официального номера банка и под предлогом той или иной операции по карте, завладеть реквизитами карт (номерами, подключиться к сервису «Банк Онлайн») и похитить с банковских счетов денежные средства. В данном случае важно понимать, что реальные сотрудники банка при совершении звонка клиентам, не выясняют полные номера карт и не просят назвать трехзначный код на оборотной стороне карт. Как правило сотрудники банка просят обратиться к специалистам в то или иное отделение банка для получения дополнительной информации и необходимой консультации.

Также злоумышленники звонят потерпевшим под видом покупателя товара, размещенного на интернет сайтах «Авито», «Юла» и других, после чего обманным путем добиваются от потерпевших сообщения номеров карт, трехзначного кода с оборотной стороны карты, просят назвать приходящие в смс сообщениях пароли, после чего похищают с банковских карт денежные средства. В некоторых случаях злоумышленники выступают в качестве продавца того или иного товара на интернет сайтах, интернет магазинах, зачастую используя созданные копии известных интернет магазинов, пользующихся популярностью. Однако отличить данный сайт от оригинала возможно по дате создания (как правило популярные интернет магазины функционируют не менее года). При общении с потерпевшими злоумышленники просят внести полную стоимость товара путем перевода денежных средств на банковскую карту либо абонентский номер, после чего перестают выходить на связь, не отправив товар в адрес покупателя, либо отправив иной товар по стоимости значительно меньшей оплаченному. В данном случае необходимо понимать, то передача товара и денежных средств должна происходить из рук в руки, либо заказ товара и его оплата должны производится на проверенных интернет сайтах и интернет магазинах с положительными отзывами и имеющими историю создания не менее 1 года.

Распространены также преступления совершаемые в социальных сетях под видом знакомого или родственника. Злоумышленники взламывают страницу в социальной сети и начинают массово писать однотипные сообщения пользователям сети, находящимся в списке друзей взломанной страницы с просьбой одолжить необходимую сумму денег путем перевода на банковскую карту. В данной ситуации необходимо позвонить лицу, с чьей страницы поступило сообщение с указанной просьбой и убедиться, что вам пишет действительно данное лицо.

Имеют место быть также преступления совершенные под предлогом освобождения сына, либо иного родственника, знакомого от уголовной ответственности за совершенное ДТП, иное преступление. Злоумышленники звонят на стационарные телефоны потерпевших, называют мамой, папой либо по имени, говорят тревожным голосом и сообщают о якобы совершенном преступлении, затем разговор прерывается и по телефону начинает общаться другой голос, как правило мужской. Злоумышленник представляется сотрудником правоохранительных

органов, либо адвокатом и просит перевести денежные средства на карту или абонентский номер для того, чтобы решить вопрос о не привлечении к уголовной ответственности. В данной ситуации необходимо позвонить на номер родственника (знакомого), либо в случае отсутствия связи с указанным лицом, позвонить иному лицу, находящемуся рядом с указанным и убедиться в том, что с ним все в порядке, либо есть какие-то проблемы. Необходимо знать, что фактически злоумышленник представляется сотрудником правоохранительных органов и просит дать ему взятку за освобождение лица от уголовной ответственности, и потерпевшая сторона в данном случае выступает, как лицо дающее взятку должностному лицу, что так же уголовно наказуемо, в случае, если звонивший и вправду окажется тем, кем он представился.

Зачастую преступники звонят престарелым гражданам, представляются сотрудниками центрального банка, судебными приставами, прокурорами и т. д. и предлагают выплату компенсации за ранее приобретенные биологически активные добавки, лекарственные препараты и за данную выплату просят перевести на банковский счет либо абонентский номер денежные средства в счет оплаты госпошлины, комиссии и т. д. В данном случае необходимо понимать, что выплатами компенсаций центральный банк и правоохранительные органы не занимаются. В случае признания какой — либо организации по продаже БАДов, медицинских препаратов, либо иной медицинской продукции мошеннической, лица пострадавшие от рук данных злоумышленников вызываются для дачи показаний в отдел полиции по месту жительства, либо по месту возбуждении уголовного дела.

Так же имеются случаи совершения преступлений под видом выплаты выигрыша, когда поступает сообщение на абонентский номер с другого номера и в сообщении указана ссылка для получения выигрыша, при переходе на которую появляется командное окно для ввода реквизитов карты, после заполнения необходимых полей с банковской карты происходит списание денежных средств. Не единичны случаи совершения указанного вида преступлений под видом брокеров игровых площадок. Злоумышленники просят ввести команду, как правило «Anydesk» на компьютере, планшете, ноутбуке после чего получают удаленный доступ к устройству, якобы обучают зарабатывать денежные средства на указанных площадках, получая в это время доступ к установленным на устройствах приложениям «Банк Онлайн», либо наблюдая за совершаемым потерпевшими действиями, в итоге просят ввести реквизиты банковских карт в том или ином поле, получая к ним отступ, после чего похищают денежные средства с карт потерпевших. В данной ситуации необходимо помнить, что «бесплатный сыр бывает только в мышеловке» и простых способов заработка денежных средств не существует. Киберпреступления совершенствуются каждый день, появляются новые способы их совершения. Однако службы безопасности банков также совершенствуют способы защиты карт и как правило по всем указанным выше преступлениям потерпевшие сами сообщают злоумышленникам все необходимые им данные для кражи денежных средств с их банковских счетов, игнорируя указанную в поступающих от банка смс сообщениях информацию о неразглашении паролей и кодов.