Наиболее распространенным видом проявления киберпреступности является хищение денежных средств с карт-счетов граждан. Причем в большинстве случаев эти преступления становятся возможны в результате беспечных действий потерпевших, предоставивших реквизиты доступа к своим банковским счетам.

**1. Фишинг** (от англ. fishing – «рыбная ловля») - вид интернет-мошенничества, когда с помощью фейковых сайтов, почтовых рассылок или социальной инженерии (хакерства с использованием человеческого фактора) пытаются заполучить конфиденциальные данные пользователя (логины, пароли, учётные записи, банковские карты).–––

**2. Помощь другу.**Большинство онлайн-мошенников действуют по стандартной схеме: взламывают учетную запись пользователя в социальной сети и пишут его знакомым с какой-либо просьбой. Чаще всего преступники требуют отправить реквизиты банковской карты или же перевести им деньги. Причем предлоги бывают абсолютно разные. Злоумышленники утверждают, будто их собственная карта заблокирована, или же давят на жалость: мол, им срочно нужно оплатить операцию больному родст



**3. Вишинг** (от англ. voice fishing – «голосовой фишинг» или «голосовая рыбная ловля»). вид телефонного мошенничества, позволяющий красть у клиентов банков конфиденциальную информацию. Клиент получает звонок от автоинформатора, который сообщает, что с картой, например, производятся мошеннические действия, и дает инструкции — перезвонить по определенному номеру. Далее, следуя инструкциям автоответчика, клиент должен сообщить или ввести на телефонной клавиатуре реквизиты карты.

**4. Покупка с предоплатой.** Наиболее примитивной, но от этого не менее работающей формой интернет-мошенничества является размещение преступниками на виртуальных досках объявлений, тематических сайтах, в социальных сетях, группах интернет-мессенджеров объявлений о продаже каких-либо товаров по «бросовым» ценам. Однако для получения товара (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту или электронный кошелек. Правда, после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

   

**5. Шантаж.** В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства. К примеру, получив несанкционированный доступ к интернет-ресурсам (страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам) и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в сети Интернет. ****

**6. Иные мошенничества.**Также можно выделить еще несколько типов мошенничества, которые в недавнем прошлом часто успешно использовались на территории Республики Беларусь: просьбы пополнить счет определенного номера мобильного телефона или платежной карты в виде «Мама, пополни счет на 20 рублей. Мне не перезванивай – позже перезвоню. Нужно срочно!»; звонок с номера друга или родственника, в котором собеседник утверждает, что он сотрудник правоохранительных органов, просит вознаграждение, обещая предотвратить возбуждение уголовного дела в отношении близкого человека; когда мошенник звонит и сразу отменяет вызов, перезвонив на отобразившийся номер, абонент слышит автоответчик или гудки, в это время со счета его мобильного телефона списываются деньги, так как вызов совершается с применением переадресации на платный номер; когда приходит SMS-сообщение о некоем выигрыше, после чего абоненту предлагают отправить платное сообщение в ответ или отправить небольшую сумму на банковскую карту для получения «выигрыша»; когда приходит SMS-сообщение с гиперссылкой, пройдя по которой пользователь запускает процесс скачивания вируса; когда поступает звонок от «представителя сотового оператора», во время которого злоумышленники предлагают перерегистрировать SIM-карту, при этом пользователь вводит специальный код или отправляет SMS-сообщение, после чего с баланса его мобильного телефона списываются деньги; когда приходит SMS-сообщение или поступает звонок, в ходе которого сообщается, что абонент не оплатил штраф, после этого человеку предлагается произвести его оплату, перечислив деньги на «специальный» расчетный счет или пополнив банковский счет; когда приходит SMS-сообщение с информацией о том, что платежная карта заблокирована, и указывается номер, по которому можно получить справку или помощь; после звонка у абонента запрашивают PIN-код, CVV-код (трехзначный код на обратной стороне карты), номер карты и другие данные, необходимые для снятия денег с банковского счета.

**Алексей АНДРОСОВ, начальник Лиозненского РОВД**