Наиболее популярные способы совершения преступления

- просьбы о помощи от знакомых и друзей

Потерпевшим в одной из социальных сетей приходит письмо от лица, с которыми ранее у него были контакты и, как правило, оно находится во вкладке «Друзья» на их странице данного сайта, с просьбой предоставить реквизиты банковской карты с целью перевода на ее денежных средств или обналичивания интернет-денег с электронного кошелька, под предлогом того, что их банковская карта заблокирована либо с нею имеются другие проблемы. После того как потерпевший пересылает данные сведения о его карт-счете, злоумышленник не санкционированно списывает денежные средства, которые, как правило, уходят на электронные кошельки или банковские карты, зарегистрированные за пределами РБ. Если знакомый просит перевести ему деньги или предоставить реквизиты банковской карты, позвоните ему и уточните достоверность информации. Если вы общаетесь редко с лицом, высказывающим указанную просьбу, попросите предоставить нотер телефон. Возможно, аккаунт взломали.

- "звонок из банка "

Клиенту банка поступает звонок на мобильный телефон, злоумышленник предоставляется сотрудником банка и сообщает, что с банковской картой клиента какие-то неполадки либо произошла несанкционированная попытка совершения операции и для предотвращения операции и устранения неполадок необходимо сообщить данные о карт-счете. Мошенники выманивают платежные данные карты (16-значный нотер, имя владельца, срок действия и трехзначный код на обратной стороне, а также код из СМС от банка). Получив реквизиты банковской карты переводят денежные средства с карт-счета на счета иностранных банков и электронные кошельки.

- Покупка товаров в интернет-магазинах либо у физических лиц с предоплатой

Мошенники используют социальные сети, создают для этих целей интернет-магазины. Мошенники рассылают поддельные письма от магазинов, предлагая скидки на различные товары, или создают копии сайтов известных брендов. Таким образом, они получают платежные данные карт, если клиент вводит их на мошенническом сайте. При переходе по ссылке в таком письме есть риск заразить устройство вирусом, который даст доступ ко всей информации на нем.

Мошенники обещают интернет-пользователям крупную сумму выигрыша или выплаты, но перед этим просят заплатить небольшую «комиссию» либо осуществить «закрепительный платеж» и в последующем просто исчезает и не выполняет обязательств.

- «доставка» (обман покупателя)

Злоумышленник размещает объявление на интернет-площадке о продаже товара по крайне выгодной цене. После того, как потенциальный покупатель начинает вести переписку во внутреннем чате площадки, злоумышленник под различными предлогами убеждает его продолжить общение в мессенджере или социальной сети. Во время общения мошенник уговаривает покупателя внести предоплату или оформить доставку, и чтобы развеять сомнения покупателя, сообщает о якобы новой услуге удержания (холдирования) средств, которая появилась на торговой площадке, т.е., если доставка не произойдет, то торговая площадка автоматически вернет средства на карту. При этом покупателю высылается ссылка на поддельную страницу, которая имитирует официальную страницу торговой площадки или интернет-банкинга, где нужно ввести данные карты (далее осуществляются действия по схеме обмана продавца).