

Способы хищения денежных средств с банковских платёжных карт:

«Просьбы о помощи от знакомых и друзей»

потерпевшим в одной из социальных сетей («ВКонтакте», «Одноклассники», и др.) 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 её денежных средств или обналичивания интернет-денег с электронного кошелька, под предлогом того, что их банковская карта заблокирована либо с нею имеются другие проблемы. В таких случаях злоумышленники пользуются доверием близких и друзей человека. После того как потерпевший пересылает данные сведения о его карт-счёте (номер банковской карты, срок действия, и др.), злоумышленник воспользовавшись данными сведениями не санкционировано списывает денежные средства, которые, как правило, уходят на электронные кошельки или банковские карты зарегистрированные за пределами Республики Беларусь. В последующем устанавливается, что интернет-страница в социальной сети друга (знакомого) была взломана (либо создана страница копия оригинальной страницы) с территории иностранного государства.

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 номер телефона, по которому вы сможете связаться. Возможно, аккаунт взломали (либо создали копию страницы), и вам пишет мошенник. Если информация окажется достоверной, то можно связаться со знакомым посредством телефонной связи и подтвердить это.

«Звонок из банка»

клиенту банка поступает звонок на мобильный телефон, злоумышленник представляется 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-счёте, номере и реквизитах банковской карты, ФИО, паспортные данные клиента. Также иногда просят передать коды о подтверждении операции, которые будут поступать им в ближайшее время посредством смс-сообщений на мобильный телефон. Злоумышленники, получив реквизиты банковской карты переводят денежные средства с карт-счёта на счета иностранных банков и электронные кошельки.

«Звонок из банка»

клиенту банка поступает звонок на мобильный телефон, злоумышленник представляется 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 установить приложение скачать программу «AnyDesk» (программа удалённого

доступа). После чего просят ввести в интернет-банкинг данные (логин и пароль) с нажатием на кнопку в виде глазка, чтобы введённые данные были видны, а не скрыты. Злоумышленник получив реквизиты входа в интернет-банкинг, переводят денежные средства с карт-счёта на счета иностранных банков и электронные кошельки.

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

для осуществления своей преступной деятельности мошенники используют социальные сети, а также создают для этих целей интернет-магазины. Участие в подобных схемах подразумевает наличие всевозможных рисков и привлекает лиц, имеющих намерения на противоправное завладение денежными средствами граждан.

Сложность установления интернет-мошенников связана с тем, что интернет-ресурсы могут быть зарегистрированы с помощью зарубежных сайтов, предоставляющих услуги анонимизации.

Также в настоящее время участились случаи просьбы перевода денежных средств на расчётный счёт злоумышленника (электронный кошелёк) в счёт оплаты за приобретаемый автомобиль, мобильный телефон, бытовую технику, одежду и др. При этом лицо просит перевести часть суммы либо полностью и в последующем просто исчезает и не выполняет обязательств.

