



*Типичные схемы дистанционных краж
безналичных денежных средств и
мошенничеств*

Брокерские операции, игра на бирже, инвестиции



1. Под предлогом получения высокой прибыли путем вложения денежных средств в брокерскую компанию, убеждают перевести денежные средства на различные указанные банковские карты.
2. Используя социальную сеть ВКонтакте и программу Skype, представившись сотрудником инвестиционной компании, убеждают внести денежные средства транзакциями на счета торговой площадки через КИВИ-кошелек, а также на банковские счета указанные данным лицом.

Лотереи, тотализатор, получение бонусов (ставки, получение выигрыша)



1. Используя никнейм в мессенджере «Viber», убеждают в том, что для получения выигрыша в лотерее необходимо по ссылке предоставленной данным лицом войти в онлайн-приложение, указать реквизиты банковской карты и произвести платеж 13% от суммы выигрыша.

БлаБлакар, Яндекс-такси

1. Используя абонентский номер телефона и сайт <https://www.blablacar.ru> под предлогом оказания услуг пассажирской перевозки, убеждают пройти по ссылке на непроверенный сайт и ввести реквизиты своей банковской карты. В последующем с банковской карты неизвестным лицом произведено списание средств.

Оформление денежных займов в микрофинансовых организациях



1. С банковской карты потрепевших производят списание денежных средств, в счет погашения задолженности по кредитным обязательствам перед микрофинансовой компанией. При этом займ в данной организации не оформлялся.

Шантаж, вымогательство

1. Используя в социальной сети никнейм, угрожая распространением личной информации о заявителе интимного содержания, принуждают перевести денежные средства на банковскую карту.

Продажа (покупка) товаров и услуг (вещи, проездные билеты, бронирование гостиниц и т.д.)



1. Используя мессенджер WhatsApp, под предлогом продажи товаров на сайте avito.ru убеждают пройти по ссылке на указанный «продавцом» сайт и ввести на нем реквизиты банковских карт. В последующем с данных банковских карт происходит списание средств.
2. Разместив объявление на сайте avito.ru убеждают потерпевшего перечислить предоплату на банковскую карту неизвестного лица. В последующем доставка товара не осуществляется.
3. Под предлогом продажи товара убеждают потерпевшего ввести на указанном неизвестным лицом сайте реквизиты своей банковской карты, в результате чего с нее были списывают денежные средства.

Банковские операции



1. По телефону представившись сотрудником службы безопасности банка, под предлогом пресечения несанкционированного списания денежных средств с банковского счета, завладевают реквизитами банковской карты, со счета которой затем похищают денежные средства переводя их на неустановленный счет.
2. По телефону представившись сотрудником службы безопасности банка, под предлогом пресечения несанкционированного списания денежных средств с банковского счета, убеждают оформить в банке кредиты и перевести данные средства на «резервные» счета.
3. Представившись сотрудником банка, под предлогом оказания помощи в использовании накопленных банковских бонусов, завладевают реквизитами и кодами банковской карты, в дальнейшем похищают с нее денежные средства.



Заём средств, просьба о помощи, оказание содействия в получении соц. выплат, компенсаций, благотворительность, вознаграждение за найденные вещи и т.д. (через соц.сети)

1. Используя взломанный аккаунт в социальной сети, под предлогом займа денежных средств, убеждают перевести денежные средства на указанную им банковскую карту.
2. Используя социальную сеть, под предлогом оказания содействия в оформлении социальной выплаты, вводят в заблуждение завладел реквизитами банковской карты с которой совершают хищение денежных средств.
3. Представившись сотрудником правоохранительных органов, вводят в заблуждение относительно полагающейся выплаты материальной компенсации за некачественные приобретенные лекарственные препараты, убеждают произвести переводы денежных средств на указанные неизвестным банковские счета.