# Информация об основных видах мошенничества

В настоящее время наиболее распространенным способом совершения преступлений в данной сфере является хищение с банковских карт граждан, когда злоумышленники по телефону представляются сотрудниками служб безопасности различных банков и под различными предлогами получают от потерпевших номер банковской карты, код CVV (3 цифры на обратной стороне карты), а также пароли, приходившие по SMS, необходимые для проведения финансовых операций.

Зачастую потерпевшие, находясь под влиянием мошенников, сами снимают деньги, в том числе оформляют на себя кредиты, и переводят их на абонентскиеномера или счета, указанные злоумышленниками.

Также злоумышленники могут сообщить потерпевшим о необходимости установления на смартфон, компьютер или планшет различных программ

(«Anydesk», «Quick support», «Teamviever» и др.), выдавая их, в том числе, за антивирусные, позволяющих мошенникам дистанционно, т.е. удаленным доступом, управлять смартфоном, ноутбуком или планшетом и, как следствие, осуществлять онлайн переводы от имени потерпевших через их личный кабинет.

В ходе телефонных разговоров мошенники могут сообщить ваши персональные данные: ФИО, дату рождения, паспортные данные, а также даже последние операции по вашим счетам. Кроме того, преступники, используя возможности IP-телефонии, могут осуществлять звонки с абонентских номеров, схожих или идентичных официальным номерам банков, указанным на оборотнойстороне карт, или правоохранительных органов, в том числе полиции.

Чтобы не стать жертвой подобных преступлений необходимо помнить, что настоящие сотрудники банков никогда не звонят клиентам и не просят сообщить им какую-либо информацию, касающуюся как их персональных данных, так и банковской карты. Ни при каких обстоятельствах не разглашайте никому, включая сотрудников банков, пароли на проведение операций. Пароль для входа в систему «Банк Онлайн» это ваша личная конфиденциальная информация. Также, не в коем случае не стоит устанавливать по просьбе неизвестных лиц какие-либо приложения(программы).

Иные способы мошенничества, совершенные дистанционным способом.

С использованием сети Интернет:

1. Путем получения предоплаты в размере до 100% за товар или услугу с помощью создания «однодневных» интернет-магазинов и сайтов-двойников; с использованием Интернет-площадок по продаже товаров и услуг (сайты «Авито»,«Юла» и др.); в социальных сетях «В контакте», «Одноклассники» и т.д.Прежде чем заказать товар в Интернете почитайте отзывы на разных сайтах оданном интернет-магазине или виртуальном

продавце, в случае наличия вы сразуобнаружите отрицательные отзывы, отсутствие отзывов о выбранном вами интернет-магазине говорит о коротком периоде его существования.

Внимательно читайте названия Интернет-магазина или организации где вы планируете приобрести какие-либо товары, в том числе покупка билетов на все виды транспорта, оплата услуг и кредитов. Тем самым Вы избежите сайтов- клонов.

Старайтесь избегать покупки товара по предоплате. Если цена товара гораздо ниже цены в обычных розничных магазинах, так и в других интернет- магазинах, либо на рынке в целом (например, при продаже автомашины по заниженной стоимости), этоповод насторожиться.

2. Путем получения информации от лица, разместившего объявление о продаже какого-либо товара, о полных реквизитах его банковской карты (номер, срок действия, данные держателя, С VC-код), якобы, с целью внесения предоплаты,с последующим хищением с нее денежных средств, используя полученные данные.

Не сообщайте неизвестному какую-либо информацию, касающуюся банковской карты - для осуществления перевода требуется только номер карты, либо привязанный к ней абонентский номер. Ни при каких обстоятельствах несообщайте пароли на проведение операций. Пароль для входа в систему «Банк Онлайн» это ваша личная конфиденциальная информация.

3. С использованием ссылок в сети «Интернет», перенаправляющих на «фишинговые» (поддельные) сайты, предоставленных мошенниками потерпевшим при оплате товара, размещенного на сайтах «Авито», «Юла» и других, а также при покупке ж/д и авиабилетов, билетов в кинотеатры.

Не переходите по присланным незнакомыми лицами ссылкам и не вводите данные своих банковских карт.

4.Взлом страниц пользователей в социальных сетях, в основном «Вконтакте» и«Одноклассники», и рассылка сообщений «друзьям» от имени данного пользователя с просьбой одолжить денег, которые нужно перевести на указанные абонентские номера или банковские карты.

Прежде чем осуществить перевод позвоните своему другу, от которого пришло сообщение, и уточните информацию.

5. Путем получения денежных средств от потерпевших при, якобы, внесении ставок на фондовых и иных биржах.

Прежде чем вносить деньги почитайте отзывы на различных сайтах в Интернете, узнайте к юрисдикции какой страны относится деятельность данной организации, а также ознакомьтесь с правилами и условиями ее деятельности._