Дистанционные мошенничества

а) мошенничества при продаже товаров в сети Интернет по предоплате (распространенные виды : продажа Iphone, цифровой, бытовой техники, одежды, обуви, автомобилей, автозапчастей);

в) сайты «подделки» , а так же фишинговые сайты

Данный вид мошенничества предполагает, что жертва посчитает сайт знакомым и приобретет на нем товар, услугу, либо укажет данные своей банковской карты.

б) получение от интернет магазина, продавца товара не соответствующего заявленному;

г) сотовый телефон используется мошенниками для передачи СМС сообщения, сообщений через мессенджеры Viber, WhatsApp с вредоносной информацией. Типы сообщений: «здесь наши с тобой фото http:\\\\...», , «ваш акакунт, страница «вКонтате» взломаны, пройдите регистрацию http:\\\\...», «вы выиграли автомобиль, подробности http:\\\\...”

**Новый тип сообщений с вредоносной ссылкой:**

«я по вашему объявлению, согласны ли на обмен на это http:\\\\foto3.inc...»

в) сотовый телефон и ваше объявление в сети Интернет (сайт Avito) используется мошенником для получения от вас данных карты и привязки карты к мобильному телефону мошенника:

- « я по вашему объявлению на авито ( о продаже, о сдаче в аренду), сообщите мне данные с вашей карты и код на обратной стороне я вам отправлю деньги...»;

- « я хочу отправить деньги вам на карту за товар на авито, предоплату за аренду, у вас карта привязана к мобильному банку, если нет идите к банкомату я вас проинструктирую как подключить мобильный банк».

б) сотовый телефон используется для передачи СМС с ложной информацией:

-«мама, кинь мне на этот номер денег, потом все объясню»,

-«ваша карта заблокирована подробности по тел..»,

-«с вашего счета списано 5000 рублей, подробности по тел...»;

а) сотовый и проводной телефон используется как средство передачи голосовой информации, подвиды, типы:

- «ваш сын попал в аварию..»,

- «мама/папа у меня проблемы..»,

- «это из банка/соцзащиты и пр..»

**Мошенничества, совершаемые с использованием мобильной и проводной связи:**

**Мошенничества, совершаемые в сети Интернет и с помощью сети Интернет:**

Как не стать жертвой мошенничества

1. приобретать вещи за их реальную стоимость и не искать предложений с 30-50 % выгодой, так как это противоречит в целом принципам рынка, либо присланный товар окажется подделкой, неисправным, либо не удовлетворяющим запросам покупателя
2. Не стоит приобретать товары в интернет магазинах позиционирующих себя как российские, но имеющие сайты в доменных зонах .com .org .biz .net .info .tv .mobi
3. Особое внимание следует уделить отзывам в сети Интернет по данному интернет-магазину, продавцу. Проверить когда был создан магазин, сайт. Создан ли он год и более назад. Если сайт существует меньше месяца, то стоит отказаться от покупки
4. В ходе общения по телефону можно сообщить, что находитесь в городе продавца, магазина и предложите забрать товар самовывозом и оплатить наличными в офисе. В случае категоричного отказа следует отказаться от покупки.
5. Настоятельно рекомендуем не осуществлять «слепые» покупки в социальных сетях. Администрация соц.сетей исключила разделы объявлений с сайтов и не несет ответственность за совершаемые с использованием сети действия пользователей. В случае необходимости приобрести товар через социальную сеть необходимо тщательно проверить продавца, обязательно связаться с ним по телефону, расспросить подробности о товаре , потребовать фотографии товара в деталях, предложить отправить товар курьерской службой и наложенным платежом, обговорить возможность возврата товара, возможность самовывоза.
6. Если вы стали жертвой мошенников и заметили это после проведения операции, покупки, заблокируйте карту и обратитесь в банк в день проведения операции для её отмены и возврате денежных средств
7. не нужно перезванивать на указанные номера
8. необходимо прекратить разговор, даже если собеседник вселяет уверенность в своей правдивости
9. При сомнении в правдивости полученной информации следует перезвонить близким от имени кого пришло сообщение, позвонить в банк по указанному на карте, либо в договоре телефону, посетить ближайшее отделение банка (Банк никогда не запрашивает по телефону сведения о карте клиента её номер, код на обратной стороне, Ф.И.О. владельца карты и срок её действия, а тем более пин-код, если собеседник пытается получить от вас такую информацию, либо просит сообщить коды которые пришли на Ваш телефон от банка, прекратите с ним разговор.)
10. Если при мошенничестве, в ходе телефонного разговора преступником была получена информация о банковской карте, то необходимо позвонить по телефону указанному на карте и заблокировать карту. В день совершения мошенничества необходимо обратиться в банк с заявлением о возврате денежных средств на карту, так как банк обязан возвратить денежные средства если операция была оспорена владельцем карты в день операции.
11. не распространять в сети Интернет сведения о мобильных номерах с их привязкой к анкетным данным, не указывать мобильные номера на социальных страницах, в подаваемых в сети объявлениях не указывать рядом с номером сотового телефона Имя и Фамилию, адрес жительства и другую личную информацию. Не использовать в сети Интернет номера своих мобильных телефонов к которым привязаны банковские карты и номера мобильных телефонов, которые используются для работы в «Мобильном банке»
12. не распространять в сети Интернет сведения о мобильных номерах с их привязкой к анкетным данным, не указывать мобильные номера на социальных страницах, в подаваемых в сети объявлениях не указывать рядом с номером сотового телефона Имя и Фамилию, адрес жительства и другую личную информацию. Не использовать в сети Интернет номера своих мобильных телефонов к которым привязаны банковские карты и номера мобильных телефонов, которые используются для работы в «Мобильном банке»