БУДЬТЕ БДИТЕЛЬНЫ

«Приобретение товаров и услуг посредством сети Интернет»

Мы привыкли совершать покупки в интернет-магазинах и часто становимся невнимательными, чем пользуются мошенники.

Схема мошенничества выглядит так: создается сайт-одностраничник, на котором выкладываются товары одного визуального признака. Цена на товары обычно весьма привлекательная, ниже среднерыночной. Отсутствуют отзывы, минимален интерфейс, указаны скудные контактные данные. Чаще всего подобные интернет-магазины работают по 100%-ной предоплате. По договоренности с продавцом деньги, как правило, перечисляются за границу через «Western Union» на имя различных людей. Конечно же, псевдо-продавец после получения денег исчезает!

Интернет-мошенники

Объявление о продаже

«Мошенники-продавцы» просят перечислить деньги за товар или услугу со 100% предоплатой, после чего закрывают свои объявления и «покупатель» впоследствии, конечно же, свой заказ не получает.

Объявление о покупке

«Мошенники – покупатели» спрашивают реквизиты банковской карты и (или) смс-коды якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

Сообщения от друзей

Мошенники пользуются чужой страничкой в социальной сети в Интернете и под видом друга (родственника) просят перечислить средства или сообщить данные Вашей карты для перечисления Вам денег под различными предлогами.

Телефонные мошенники

Завладение реквизитами банковской карты

Мошенники под видом банковских работников звонят или присылают СМС с сообщением о блокировании банковской карты. Их цель – узнать ее секретный код.

Получение выигрыша (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.д. Жертве можно забрать его, заплатив якобы за сохранность денег.

Вирус в телефоне

Мошенники запускают вирус в телефон, предлагая перейти по № «зараженной ссылке». С помощью вируса получают доступ к банковской карте, привязанной к телефону.

Установите «антивирус» и не переходите по сомнительным ссылкам.

Памятка о безопасности при использовании банковских карт (счетов)

Злоумышленники:

- могут рассылать электронные письма, смс-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платежных систем;

- осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющуюся задолженность;

- под надуманными предлогами просят сообщить PIN-код банковской карты и содержащиеся на ней данные;

- полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

Следует помнить!

- Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не присылают писем и не звонят гражданам с просьбой предоставить свои данные;

- Сотрудник банка может запросить у клиента только контрольное слово и ФИО;

- При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие-либо операции с картой или счетом;

- Никто, в том числе сотрудник банка или представитель государственной власти, не вправе требовать от держателя карты сообщить PIN-код или код безопасности;

- При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты).

При несанкционированном (незаконном) списании денежных средств рекомендуется:

- незамедлительно обратиться в кредитно-финансовую организацию с целью блокирования банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;

- обратиться в полицию с соответствующем заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;

- обратиться с заявлением в Роскомнадзор с изложением обстоятельств произошедшего с указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса о блокировке таких ресурсов.

В последние время участились случаи совершения хищения денежных средств со счетов банковских карт

КАК ЭТО ПРОИСХОДИТ?

Вариант 1

Вам звонит злоумышленник, представляется сотрудником банка, клиентом которого Вы являетесь, и сообщает, что с Вашего счета неизвестные пытаются списать некую сумму денег. Звонок может быть осуществлен с номера, похожего на номер клиентской линии банка. Звонящий может рассказать Вам, сколько денег на Вашем счете и когда в последний раз была произведена операция по счету – НО ЭТО НЕ ГАРАНТИЯ ПОДЛИННОСТИ!

Вариант 2

Вам приходит смс-сообщение о блокировке Вашей карты с указанием номера контактного телефона для решения проблемы. Под предлогом защиты от незаконного списания денежных средств неизвестный просит Вас сообщить CVV (код на оборотной стороне карты) банковской карты, кодовое слово или код из смс-сообщения. В случае предоставления Вами этой конфиденциальной информации злоумышленниками будет осуществлен перевод Ваших денежных средств на счет третьих лиц.

Ни в коем случае не называйте:

- реквизиты карт

- пин-код

- cvv-код (напечатан на оборотной стороне карты)

Исключайте общение с «работниками банка по телефону» - помните, что в нашем городе все отделения банков находятся в шаговой доступности