Совершение покупок в сети Интернет

Что делать, если при совершении сделок купли-продажи товаров через Интернет после их оплаты ни товаров, ни денег обратно получить не удается?

В случае, если вы стали жертвой интернет-мошенников, необходимо обращаться в правоохранительные органы по месту жительства для проведения необходимых проверок и возбуждения уголовного дела.

При обращении в полицию с заявлением необходимо сообщать как можно более полную информацию о злоумышленниках, в частности адрес сайта, расчетный счет, адрес электронной почты, номера телефонов, электронных кошельков и т.д.

Если вы все-таки решили приобрести товары в сети Интернет, не стоит торопиться предпринимать действия, навязываемые неизвестными продавцами, тем более, если они требуют перевода денежных средств каким-либо способом. Через Интернет вам могут предложить приобрести все что угодно, а распознать подделку при покупке через всемирную компьютерную сеть бывает сложно. Однако, соблюдая некоторые правила предосторожности, можно оградить себя от возможных неприятностей.

Прежде чем что-либо приобрести на неизвестном вам сайте, проверяйте полную информацию о нем, поищите отзывы, почитайте форумы. Наведите справки о продавце, изучите отзывы о его работе и только после этого принимайте решение.

Вас должна насторожить слишком низкая цена на товар, а также отсутствие фактического адреса или телефона продавца. В этом случае, скорее всего, вам предлагают приобрести подделку либо хотят присвоить ваши деньги.

Сегодня мошенничество в Интернете развито очень хорошо. Постоянно появляются новые способы обмана людей. В этой связи необходимо быть бдительными и осторожными.

Какие существуют мошеннические схемы, связанные с привлечением средств граждан под предлогом инвестирования и покупки товаров в интернет – магазинах с предоплатой?

Уважаемые граждане, обращаем Ваше внимание, что на протяжении последних лет увеличилось количество противоправных действий мошеннического характера с использованием сети Интернет путем вовлечения в сомнительные схемы, такие как доверительное управление денежными средствами, участие, в так называемых «бинарных аукционах» и покупки товаров в интернет – магазинах 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.

В связи с этим обращаем внимание, что интернет – ресурсы могут быть зарегистрированы с помощью зарубежных сайтов предоставляющих услуги анонимизации, что не позволит в ряде случаев пользователю установить достоверные сведения о лицах, которым он доверил денежные средства.

Совет гражданам: совершать покупки только на проверенных сайтах, о существовании которых можно узнать от друзей и знакомых, найти отзывы в сети Интернет и т.п. Поисковые системы (типа Яндекса) публикуют рейтинги Интернет-магазинов, которые тоже являются показателем надежности торговой площадки. Не нужно ничего покупать в социальных сетях. Не доверяйте брокерам, которые получают от граждан денежные средства для игры на бирже без заключения письменных контрактов.

Почему опасно вносить предоплату при покупках товаров в сети Интернет?

Мошенники привлекают потенциальных жертв низкими ценами на товары известных брендов. Покупателей просят внести предоплату, как правило, перевести денежные средства на электронный кошелек. В течение нескольких дней магазин обещает скорую доставку товара, после чего бесследно исчезает.

Схожий способ мошенничества используется при продаже товаров или услуг на электронных досках объявлений, интернет-аукционах, форумах, сервисах бронирования недвижимости. Как и в случае с интернет-магазинами, мошенники привлекают своих жертв низкими ценами и требуют перечисления предоплаты на электронный кошелек или банковскую карту.

Как действуют мошеннические схемы при оформлении полиса ОСАГО через Интернет, либо при покупке авиабилетов онлайн?

Мошенники регистрируют доменное имя, содержащее в названии слово «osago» или напоминающее доменное имя одной из известных страховых компаний. На этом домене размещается фишинговый сайт, страницы которого практически полностью копируют оформление оригинального веб-ресурса, принадлежащего страховой компании. Для расчета стоимости страхования пользователю необходимо заполнить небольшую анкету - указать имя, дату рождения, номер водительского удостоверения, данные об автомобиле, номер телефона и электронную почту для связи. После введения данных покупателю предлагают оплатить электронный полис ОСАГО с помощью банковской карты: указать номер карты, дату окончания ее действия и CVC/CVV-код. Мошенники перенаправляют пользователя на поддельную страницу подтверждения оплаты, где просят ввести полученный от банка код подтверждения оплаты. В случае успеха злоумышленники обходят двухфакторную аутентификацию и получают деньги.

Аналогичную схему обмана можно встретить при покупке авиабилетов онлайн.