

Памятка по профилактике дистанционных мошенничеств

В последние годы широкую популярность получили смс-рассылки или электронные письма с сообщениями о выигрыше автомобиля либо других ценных призов. Для получения «выигрыша» злоумышленники обычно просят перевести на электронные счета определенную сумму денег, мотивируя это необходимостью уплаты налогов, таможенных пошлин, транспортных расходов и т.д. После получения денежных средств они перестают выходить на связь либо просят перевести дополнительные суммы на оформление выигрыша.

Оградить себя от подобного рода преступлений предельно просто. Прежде всего необходимо быть благоразумным. Задумайтесь над тем, принимали ли вы участие в розыгрыше призов? Знакома ли вам организация, направившая уведомление о выигрыше? Откуда организаторам акции известны ваши контактные данные? Если вы не можете ответить хотя бы на один из этих вопросов, рекомендуем вам проигнорировать поступившее сообщение.

Если вы решили испытать счастье и выйти на связь с организаторами розыгрыша, постарайтесь получить от них максимально возможную информацию об акции, условиях участия в ней и правилах ее проведения. Помните, что упоминание вашего имени на Интернет-сайте не является подтверждением добропорядочности организаторов акции и гарантией вашего выигрыша.

Любая просьба перевести денежные средства для получения выигрыша должна насторожить вас. Помните, что выигрыш в лотерею влечет за собой налоговые обязательства, но порядок уплаты налогов регламентирован действующим законодательством и не осуществляется посредством перевода денежных средств на электронные счета граждан и организаций или т.н. «электронные кошельки».

Будьте бдительны и помните о том, что для того, чтобы что-то выиграть, необходимо принимать участие в розыгрыше. Все упоминания о том, что ваш номер является «счастливым» и оказался в списке участников лотереи, являются, как правило, лишь уловкой для привлечения вашего внимания.

Нередки случаи мошенничеств, связанных с деятельностью Интернет-магазинов и сайтов по продаже авиабилетов. Чем привлекают потенциальных жертв мошенники? Прежде всего - необоснованно низкими ценами. При заказе товаров вас попросят внести предоплату, зачастую путем внесения денежных средств на некий виртуальный кошелек посредством терминала экспресс-оплаты. Далее магазин в течение нескольких дней будет придумывать отговорки и обещать вам скорую доставку товара, а потом бесследно исчезнет либо пришлет некачественный товар.

Цель подобных сайтов – обмануть максимальное количество людей за короткий срок. Создать Интернет-сайт сегодня – дело нескольких минут, поэтому вскоре после прекращения работы сайт возродится по другому адресу, с другим дизайном и под другим названием.

Если вы хотите купить товар по предоплате помните, что серьезные Интернет-магазины не будут просить вас перечислить деньги на виртуальный кошелек или счет мобильного телефона. Поищите информацию о магазине в сети Интернет, посмотрите, как долго он находится на рынке. Если вы имеете дело с сайтом крупной или известной вам компании, убедитесь в правильности написания адреса ресурса в адресной строке вашего браузера. При необходимости потребуйте от администраторов магазина предоставить вам информацию о юридическом лице, проверьте ее, используя общедоступные базы данных налоговых органов и реестр юридических лиц. Убедитесь в том, что вы знаете адрес, по которому вы сможете направить претензию в случае, если вы будете недовольны покупкой.

Заметно участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Иногда подобные сообщения содержат призыв перевести деньги для разблокировки карты, иногда абонента просят позвонить или отправить смс на короткий номер.

Необходимо помнить о том, что единственная организация, которая сможет проинформировать вас о состоянии вашей карты – это банк, обслуживающий ее. Если у вас есть подозрения о том, что с вашей картой что-то не в порядке, если вы получили смс-уведомление о ее блокировке, немедленно обратитесь в банк. Телефон клиентской службы банка обычно указан на обороте карты. Не звоните и не отправляйте сообщения на номера, указанные в смс-уведомлении, за это может взиматься дополнительная плата.

Один из популярных способов мошенничеств, основанных на доверии связан с размещением объявлений о продаже товаров на электронных досках объявлений и интернет-аукционах. Как правило, мошенники привлекают своих жертв заниженными ценами и выгодными предложениями и требуют перечисления предоплаты путем перевода денежных средств на электронный кошелек.

Благоразумие поможет и здесь. Внимательно изучите объявление, посмотрите информацию о лице, разместившем его. Если торговая площадка имеет систему рейтингов продавцов, изучите отзывы, оставленные другими покупателями, не забывая, однако, о том, что преступники могут оставлять положительные отзывы о себе, используя дополнительные учетные записи. Воспользуйтесь Интернет-поиском. Иногда достаточно ввести в форму поиска телефонный номер или сетевой псевдоним продавца для того, чтобы обнаружить, что эти данные уже использовались в целях хищения денежных средств и обмана покупателей.

Посмотрите среднюю стоимость аналогичных товаров. Чересчур низкая стоимость должна вызвать у вас подозрение. Если продавец требует перечислить ему полную или частичную предоплату за приобретаемый товар на электронный счет, подумайте, насколько вы готовы доверять незнакомому человеку. Помните, что перечисляя деньги незнакомым лицам посредством анонимных платежных систем, вы не имеете гарантий их возврата в случае, если сделка не состоится.

Покупать авиабилеты через Интернет удобно. Вам не нужно никуда ехать и стоять в очередях. Вы выбираете рейс, дату, оплачиваете билет и получаете его спустя несколько секунд. Сегодня многие люди выбирают именно такой способ приобретения билетов на самолет.

Естественно, мошенники не могут оставить данную сферу без внимания. За последний год существенно увеличилось количество жалоб на обман при покупке электронных билетов. Создать Интернет-сайт по продаже авиабилетов – дело нескольких часов, на смену его названия, адреса и внешнего оформления требуется еще меньше времени. Как правило, обман раскрывается не сразу, некоторые узнают о том, что их билетов не существует, лишь в аэропорту. Это дает мошенникам возможность перенести свой Интернет-ресурс на новое место и продолжать свою преступную деятельность под другим названием.

Чтобы не испортить себе отдых или деловую поездку стоит внимательно относиться к покупке авиабилетов через сеть Интернет. Воспользуйтесь услугами Интернет-сайта авиакомпании или агентства по продаже билетов, давно зарекомендовавшего себя на рынке. С осторожностью относитесь к деятельности неизвестных вам сайтов, особенно тех, которые привлекают ваше внимание специальными предложениями и низкими ценами. Не переводите деньги на электронные кошельки или счета в зарубежных банках. Не поленитесь позвонить в представительство авиакомпании, чтобы убедиться в том, что ваш рейс существует и билеты на него еще есть. Эти простые правила позволят вам сэкономить деньги и сберечь нервы.

Если вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или какой -нибудь программы, не спешите открывать её. Перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Посмотрите, с какого номера было отправлено вам сообщение. Даже если сообщение прислал кто -то из знакомых вам людей, будет не лишним

дополнительно убедиться в этом, ведь сообщение могло быть отправлено с зараженного телефона без его ведома. Если отправитель вам не знаком, не открывайте его.

Помните, что установка антивирусного программного обеспечения на мобильное устройство - это не прихоть, а мера позволяющая повысить вашу безопасность.

Многие люди сегодня пользуются различными программами для обмена сообщениями и имеют аккаунты в социальных сетях. Для многих общение в сети стало настолько привычным, что практически полностью заменило непосредственное живое общение.

Преступникам в наши дни не нужно проводить сложные технические мероприятия для получения доступа к персональным данным, люди охотно делятся ими сами. Размещая детальные сведения о себе в социальных сетях, пользователи доверяют их тысячам людей, далеко не все из которых заслуживают доверия.

Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно. Поэтому не следует раскрывать малознакомому человеку такие подробности вашей жизни, которые могут быть использованы во вред. Помните о том, что видео и аудиотрансляции, равно как и логи вашей сетевой переписки, могут быть сохранены злоумышленниками и впоследствии использованы в противоправных целях.

Не забывайте, что никто лучше вас самих не сможет позаботиться о сохранности той личной информации, которой вы не хотите делиться с общественностью.

Информация НЦБ Интерпола МВД России

о самых распространенных видах мошеннических действий с использованием компьютерных технологий.

Уважаемые граждане! Если Вы относитесь к активным пользователям Интернета, то рекомендуем Вам обязательно прочитать этот материал!

Мошенничество - это хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Подобная преступная деятельность преследуется законом независимо от места совершения - в реальной или виртуальной среде.

Мошенники постоянно изыскивают все новые и новые варианты хищения чужого имущества. Кратко остановимся на самых распространённых.

«Брачные мошенничества»

Типичный механизм: с использованием сети Интернет

преимущественно на сайтах знакомств преступники выбирают жертву, налаживают с ним электронную переписку от имени девушек, обещая приехать с целью создания в будущем семьи. Затем под различными предложениями «невесты» выманивают деньги (на лечение, покупку мобильного телефона, приобретение билетов, оплаты визы и т.д.). Переписка ведется главным образом студентами лингвистических ВУЗов. Направленные жертвами деньги преступники получают на подставных лиц. После получения средств переписка под различными предложениями прекращается.

«Приобретение товаров и услуг посредством сети Интернет»

Мы настолько привыкли покупать в интернет-магазинах, что часто становимся невнимательными, чем и пользуются мошенники. Обычно схема мошенничества выглядит так: создаётся 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 такие интернет-магазины работают по 100% предоплате. Переписка о приобретении товаров ведется с использованием электронных почтовых ящиков. По договоренности с продавцом деньги перечисляются, как правило,

за границу через "WesternUnion" на имена различных людей. Конечно же, псевдо-продавец после получения денег исчезает!

«Крик о помощи»

Один из самых отвратительных способов хищения денежных средств. В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

Мы не призываем отказывать в помощи всем кто просит! Но! Прежде чем переводить свои деньги, проверьте - имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

«Фишинг»

Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

Так, с помощью спам-рассылок потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на "сайт-двойник" такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы. Достаточно распространённым является предложение о работе за границей, уведомление о выигрыше в лотереи, а также сообщения о получении наследства.

«Нигерийские письма»

Один из самых распространённых видов мошенничества. Типичная схема: жертва получает на свою почту письмо о том, что является счастливым обладателем многомиллионного наследства. Затем мошенники просят у получателя письма помощи в многомиллионных денежных операциях (получение наследства, перевод денег из одной страны в другую), обещая процент от сделки. Если получатель согласится участвовать, то у него

постепенно выманиваются деньги якобы на оплату сборов, взяток чиновникам и т.п.

«Брокерские конторы»

С начала текущего года в НЦБ Интерпола МВД России наблюдается значительный рост количества обращений граждан, пострадавших от действий брокерских контор.

В распоряжении Бюро имеется информация о следующих недобросовестных брокерских компаниях: «MXTrade», «MMC1S» и «TeleTrade».

Для того, чтобы не потерять свои деньги при выборе брокерской компании необходимо обращать внимание на следующие признаки, которые характеризуют компанию-мошенника: обещание высоких процентов, отсутствие регистрации, обещание стабильной прибыли новичкам-трейдерам.

Перед тем, как доверить свой капитал, внимательно изучите не только интернет-ресурсы, но и официальную информацию о брокере и его регламент.

Важно! Помните, что инвестирование, предлагаемое на условиях брокерской компании, всегда является высоко рискованным даже при наличии безупречной репутации брокерской компании.