


Интернет-мошенничество - памятка для граждан

СИТУАЦИЯ 1	
	<p>Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза?</p> <p>НИКОГДА не отправляйте деньги незнакомым лицам на их электронные счета.</p> <p><i>Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.</i></p>

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.

СИТУАЦИЯ 2	
	<p>Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату?</p> <p>НИКОГДА не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.</p> <p><i>Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.</i></p>

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.

СИТУАЦИЯ 3	
	<p>Вы получили sms-сообщение о том, что ваша банковская карта заблокирована?</p> <p>НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных sms.</p> <p><i>Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.</i></p>

Заметно участились случаи рассылки sms-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 sms 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 sms-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 sms-уведомлении, за это может взиматься дополнительная плата.

СИТУАЦИЯ 4



На электронной доске объявлений или в социальной сети вы нашли товар, который так долго искали, и стоит он намного дешевле чем в других местах?

НИКОГДА не перечисляйте деньги на электронные кошельки, не убедившись в благонадежности контрагента.

Внимательно посмотрите его рейтинг на доске объявлений, почитайте отзывы других покупателей, поищите информацию о нем в сети Интернет. Подумайте над тем, почему товар продается так дешево, узнайте какие гарантии может предоставить продавец.

Один из популярных способов мошенничества, 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.

СИТУАЦИЯ 5



Вы хотите приобрести авиабилеты через Интернет?

НИКОГДА не пользуйтесь услугами непроверенных и неизвестных сайтов по продаже билетов.

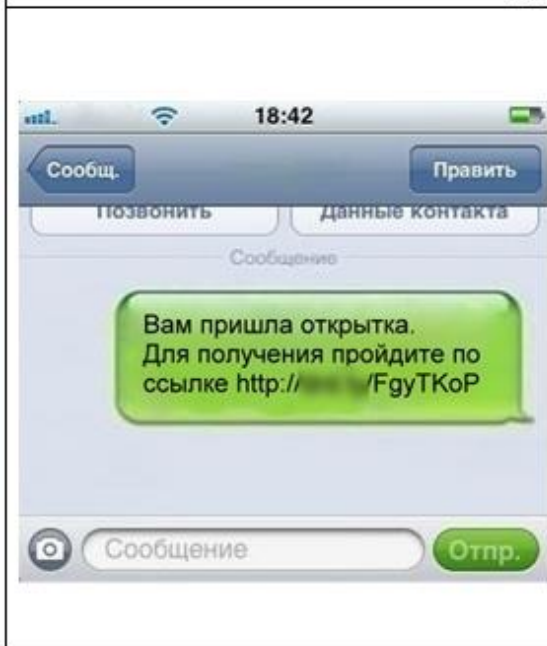
Закажите билеты через сайт авиакомпании или агентства, положительно зарекомендовавшего себя на рынке. Не переводите деньги за билеты на электронные кошельки или зарубежные счета. При возникновении подозрений обратитесь в представительство авиакомпании.

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.

СИТУАЦИЯ 6



Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы?

НИКОГДА не переходите по ссылке, указанной в сообщении.

Помните, что перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.

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.

СИТУАЦИЯ 7



Общаетесь в интернете и имеете аккаунты в соцсетях?

НИКОГДА не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред.

Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно. Помните о том, что видео и аудиотрансляции, равно как и логи вашей сетевой переписки, могут быть сохранены злоумышленниками и впоследствии использованы в противоправных целях.

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.

Советы по определению Интернет-ресурсов, несущих потенциальную угрозу финансовому благополучию пользователей



НЕ ОТКРЫВАЙТЕ ДВЕРЬ незнакомым людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиники, ЖКХ и т.д. Позвоните и уточните, направляли ли к Вам этого специалиста!



НЕ ДОВЕРЯЙТЕ, если Вам звонят и сообщают, что Ваш родственник или знакомый попал в аварию, за решетку, в больницу или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку, купить дорогие лекарства - в общем откупиться. **Это ОБМАН!**



**БУДЬТЕ
БДИТЕЛЬНЫ!**

Звоните в полицию

02/102

Бесплатная
"горячая линия МВД России"
8-800-222-74-47



Незнакомец сообщает о выигрыше, блокировке банковской карты, о пересчете квартплаты, срочном обмене денег на дому или предлагает приобрести товары и таблетки по низким "льготным" ценам?
НЕ ВЕРЬТЕ - ЭТО МОШЕННИЧЕСТВО!



КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ



Вам позвонили/прислали SMS с неизвестного номера с просьбой о помощи близкому человеку

- Не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей
- Задайте звонящему вопросы личного характера, помогающие отличить близкого Вам человека от мошенника
- Под любым предлогом постарайтесь прервать контакт с собеседником, перезвоните родным и узнайте, все ли у них в порядке



Вам позвонили/прислали SMS «из банка» с неизвестного номера

- Не торопитесь следовать инструкциям и отвечать на запрос
- Не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка
- Проверьте информацию, позвонив в контактный центр банка
- Незамедлительно обратитесь в правоохранительные органы



Вам прислали MMS или ссылку с неизвестного номера

- Не открывайте вложенные файлы, не переходите по ссылкам, удалите подозрительное сообщение
- Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков
- Защитите свой телефон, подключите БЕСПЛАТНУЮ услугу «Стоп-контент»



Вы заподозрили интернет-продавца в недобросовестности

- Необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки
- Встречаться с продавцом в общественном месте, так как это наиболее безопасный и гарантированный способ покупки. Следует передавать деньги продавцу лично в руки сразу после получения товара
- Никогда не переводить незнакомым лицам деньги в качестве предоплаты



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 "Western Union" 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, взятков 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.



Покупки через Интернет – это без сомнения очень удобно. Сфера Интернет-услуг расширяется, доходы сетевых ритейлеров растут, а люди все чаще предпочитают заказ товаров в сети походам по магазинам. Однако удобство Интернет-технологий распространяется не только на продавцов и покупателей. Мошенники также по достоинству оценили новые формы торговли и активно используют их своих целях.

Для того, чтобы радость онлайн-покупок не была омрачена получением некачественного товара или потерей денег мы рекомендуем вам обратить внимание на некоторые признаки потенциально опасных Интернет-магазинов.

1. Низкая цена. Если вы нашли объявление или магазин, предлагающий товары по ценам существенно ниже рыночных, имейте в виду, что мошенники часто используют данный прием для привлечения жертв.

На что следует обратить внимание? Посмотрите стоимость аналогичных товаров в других Интернет-магазинах, она не должна отличаться слишком сильно. Не поддавайтесь на слова «акция», «количество ограничено», «спешите купить», «реализация таможенного конфиската», «голландский аукцион».

2. Требование предоплаты. Если продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица, нужно понимать, что данная сделка является опасной.

На что следует обратить внимание? Учитывайте риски при совершении Интернет-покупок. Помните о том, что при переводе денег в счет предоплаты вы не имеете никаких гарантий их возврата или получения товара. Если вы решили совершить покупку по предоплате, проверьте рейтинги продавца в платежных системах.

3. Отсутствие возможности курьерской доставки и самовывоза товара. Данные факторы вынуждают покупателей пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату.

На что следует обратить внимание? Выбирая из нескольких магазинов, следует отдать предпочтение тому, в котором есть возможность забрать товар самостоятельно. Злоумышленники могут предоставить поддельные квитанции об отправке товара транспортной компанией.

4. Отсутствие контактной информации и сведений о продавце. Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном, такой магазин может представлять опасность.

На что следует обратить внимание? Внимательно изучите сведения о продавце. Помните о том, что вы собираетесь доверить деньги лицу или компании, о которой вы ничего не знаете. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем другие организации. Проверьте отзывы о магазине в открытых Интернет-рейтингах, пролистайте отзывы как можно дальше, злоумышленники могут прятать негативные отзывы за десятками фальшивых положительных оценок. В случае совершения покупок посредством электронных досок объявлений посмотрите историю сделок продавца и ознакомьтесь с его рейтингом, многие торговые площадки предлагают подобную услугу.

5. Отсутствие у продавца или магазина «истории». Если Интернет-магазин или учетная запись продавца зарегистрированы несколько дней назад, сделка с ними может быть опасной.

На что следует обратить внимание? Создание Интернет-магазина – дело нескольких часов, изменение его названия и переезд на другой адрес – дело нескольких минут. Будьте осторожны при совершении покупок в только что открывшихся Интернет-магазинах.

6. Неточности или несоответствия в описании товаров. Если в описании товара присутствуют явные несоответствия, следует осторожно отнестись к подобному объявлению.

На что следует обратить внимание? Внимательно прочитайте описание товара и сравните его с описаниями на других Интернет-ресурсах.

7. Излишняя настойчивость продавцов и менеджеров. Если в процессе совершения покупки менеджер магазина начинает торопить вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи, не поддавайтесь на уговоры и трезво оценивайте свои действия.

На что следует обратить внимание? Злоумышленники часто используют временной фактор для того, чтобы не дать жертве оценить все нюансы сделки. Тщательно проверяйте платежную информацию и при наличии любых сомнений откладывайте сделку.

8. Подтверждение личности продавца путем направления отсканированного изображения паспорта. Ожидая перевода денег, продавцы в социальных сетях часто направляют изображение своего паспорта покупателю с целью подкупить его доверие.

На что следует обратить внимание? Помните, что при современном развитии техники изготовить изображение паспорта на компьютере не представляет никакого труда. Данное изображение никаким образом не может подтверждать личность лица, направившего его вам.

ВЫВОД

Если Интернет-магазин или объявление соответствуют хотя бы одному из указанных признаков, это серьезный повод задуматься о целесообразности совершения сделки.

Если под их описание подходят два или более признака, мы настоятельно рекомендуем вам воздержаться от контактов с данным продавцом или магазином.