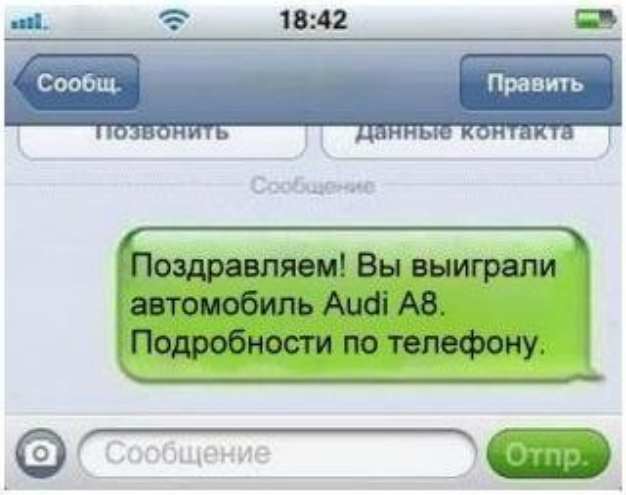
Памятка для граждан о мерах безопасности
«Как не стать жертвой мошенников?»

Ситуация 1.



Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза?

НИКОГДА не отправляйте деньги незнакомым лицам на их электронные счета.

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.

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.

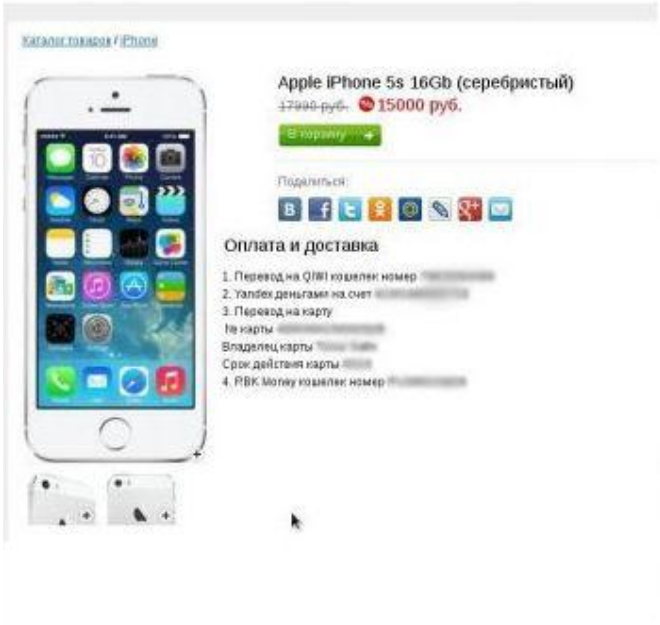
Любая просьба перевести денежные средства для получения выигрыша должна насторожить вас. Помните, что выигрыш в лотерею влечет за собой налоговые

обязательства, но порядок уплаты налогов регламентирован действующим законодательством и не осуществляется посредством перевода денежных средств на электронные счета граждан и организаций или так называемые «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.

Просьбы перейти по ссылке или поучаствовать в Интернет-опросе, различного рода Интернет-акциях, обещающих легкий доход, зачастую оказываются уловками мошенников. В ходе простого опроса потерпевшие, сами того не замечая, передают злоумышленникам номера банковских карт и прочие реквизиты. Итогом чаще всего становится не зачисление, а списание средств с карты.

Ситуация 2.



Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату?

НИКОГДА не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.

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.

Нередки случаи мошенничеств, связанных с деятельностью Интернет-магазинов и сайтов по продаже. 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.

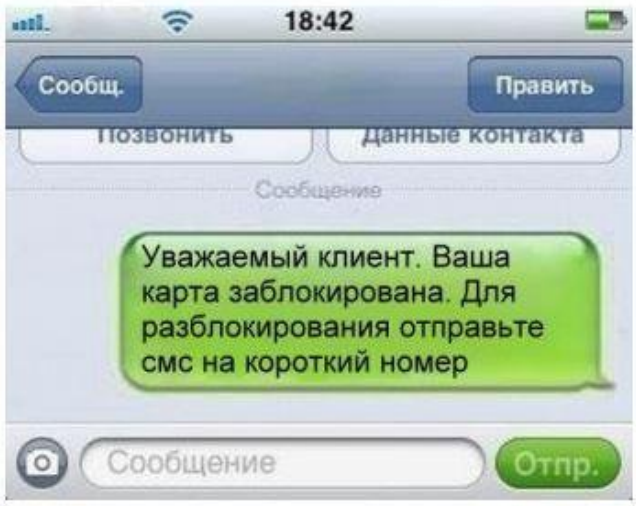
Цель подобных сайтов – обмануть максимальное количество людей за короткий срок. Создать Интернет-сайт сегодня – дело нескольких минут, поэтому вскоре после прекращения работы сайт возродится по другому адресу, с другим дизайном и под другим названием.

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.

Нередко жертвами мошенников становятся и граждане, желающие продать через сеть «Интернет» принадлежащее им имущество. Чаще всего злоумышленники звонят продавцу и сообщают, что готовы незамедлительно приобрести товар. Обрадованный сделке продавец сообщает, по просьбе злоумышленников, номер своей банковской карты, а также пришедшие СМС-коды. В итоге вместо СМС о зачислении, к удивлению продавца, приходят сообщения о списании денежных средств.

Для безналичного перевода средств покупателю достаточно знать номер Вашей карты или номер телефона, в случае, если он привязан к мобильному банку. Пароли, пришедшие по СМС, а также три цифры, указанные на обороте карты нужны лишь для списания средств с карты! Для зачисления данные реквизиты не требуются!

Ситуация 3.



Вы получили смс-сообщение о том, что ваша банковская карта заблокирована?

НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.

Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.

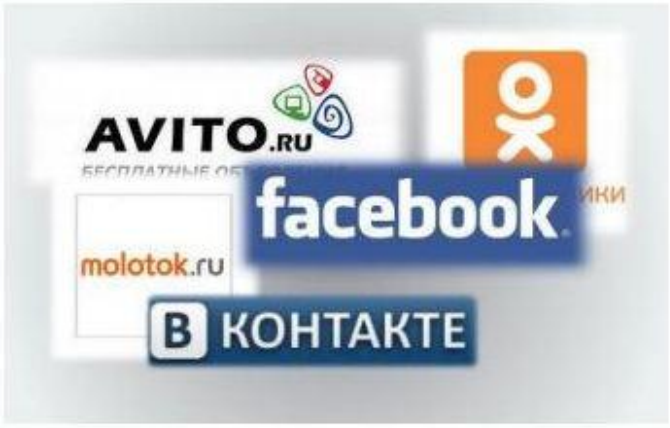
Заметно участились случаи рассылки СМС-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Иногда подобные сообщения содержат призыв перевести деньги для разблокировки карты, иногда абонента просят позвонить или отправить смс на короткий номер. Или злоумышленники звонят по телефону и, представившись сотрудниками банка, просят сообщить реквизиты банковской карты, паспортные данные, а также временные пароли, пришедшие по СМС.

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.

Доверяйте лишь СМС-рассылке, приходящей с номера Вашего банка! Для СМС-рассылок банки всегда используют один и тот же номер. Чаще всего это простые трехзначные номера. Участились случаи, когда мошенники используют зрительно схожие номера. Отвечая на незнакомый номер, будьте внимательны! Прежде чем сообщать какую-либо информацию, запрашиваемую у вас по телефону, хорошо подумайте! Если сомневаетесь, попросите Вам перезвонить. После чего позвоните на горячую линию Вашего банка и уточните, действительно и их сотрудник Вам звонил только что, а также может ли действительно понадобиться представителю банка запрашиваемая информация.

Не сообщайте никому временные пароли, полученные Вами при помощи СМС и Интернет-сообщений! Обратите внимание, каждое СМС с временным паролем, полученное из Банка, всегда содержит одну и ту же фразу: «Никому не сообщайте код». Эта информация только для Вас. Помните, люди, владеющие данной информацией, могут пользоваться Вашими средствами без Вашего участия. Чаще всего злоумышленники звонят по телефону и, представившись сотрудниками банка, просят сообщить реквизиты банковской карты, паспортные данные, а также временные пароли, пришедшие по СМС. Помните, действующим сотрудникам банка данная информация не нужна!

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 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.

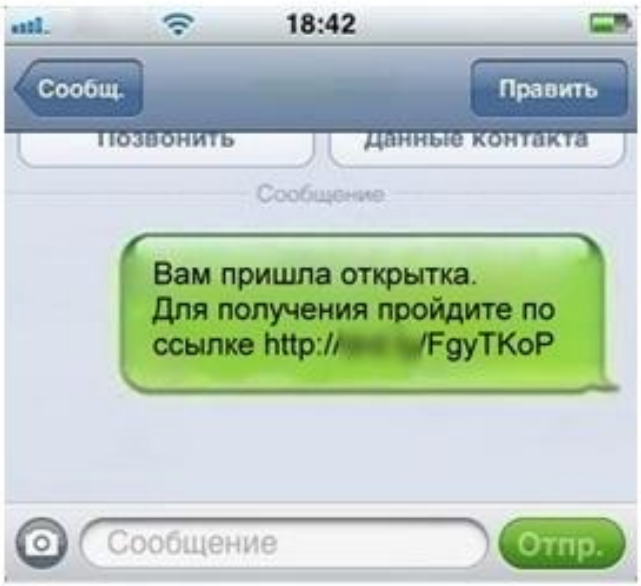
Посмотрите среднюю стоимость аналогичных товаров. Чересчур низкая стоимость должна вызвать у вас подозрение. Если продавец требует перечислить ему полную или частичную предоплату за приобретаемый товар на электронный счет, подумайте, насколько вы готовы доверять незнакомому человеку. Помните, что перечисляя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

Нередко жертвами мошенников становятся и граждане, желающие продать через сеть «Интернет» принадлежащее им имущество. Чаще всего злоумышленники звонят

продавцу и сообщают, что готовы незамедлительно приобрести товар. Обрадованный сделке продавец сообщает, по просьбе злоумышленников, номер своей банковской карты, а также пришедшие СМС-коды. В итоге вместо СМС о зачислении, к удивлению продавца, приходят сообщения о списании денежных средств.

Помните, что для безналичного перевода средств покупателю достаточно знать номер Вашей карты или номер телефона, в случае, если он привязан к мобильному банку. Пароли, пришедшие по СМС, а также три цифры, указанные на обороте карты нужны лишь для списания средств с карты! Для зачисления данные реквизиты не требуются!

Ситуация 5.



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.

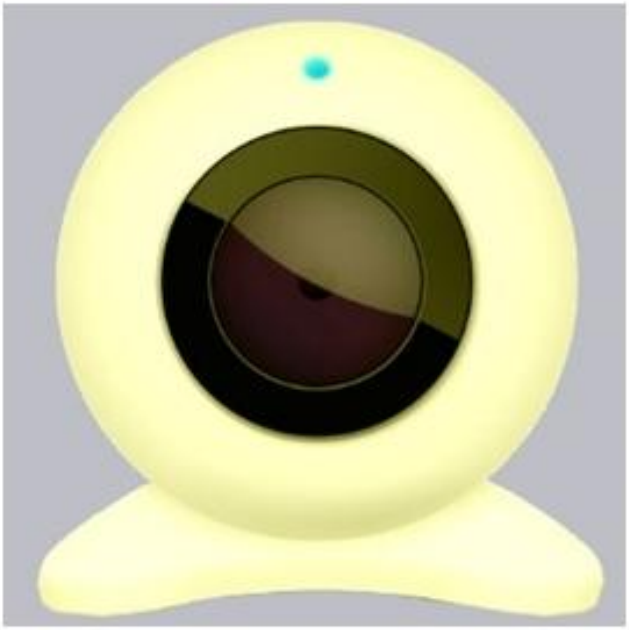
Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.

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 6.



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.

Если Ваши близкие просят Вас о помощи посредством соц.сетей, сообщений или от их лица звонят незнакомцы, не верьте им, скорее всего это мошенники! Не исключением становятся мошеннические действия при помощи соц.сетей, когда злоумышленники, взломав чужую страницу, от имени Ваших друзей просят Вас о помощи. Самый простой способ не попасться на удочку мошенников, пообщаться со знакомым лично, позвонить ему. Очень часто люди с удивлением встречают подобного рода информацию, даже не догадываясь о том, что кто-то от их лица шлет сообщения с просьбой о помощи.

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