Внимание ! Мошенники!

Ситуация 1

Вы получили СМС – сообщение о том, что ваша банковская карта заблокирована.
НИКОГДА НЕ ПЕРЕЗВАНИВАЙТЕ ПО НОМЕРУ, КОТОРЫЙ УКАЗАН В ТЕКСТЕ СООБЩЕНИЯ, НЕ ОТПРАВЛЯЙТЕ ОТВЕТНЫХ СМС. НЕ СООБЩАЙТЕ РЕКВИЗИТЫ СВОЕЙ БАНКОВСКОЙ КАРТЫ (СЧЕТА) И ЦИФРОВЫЕ КОДЫ ПОДТВЕРЖДЕНИЯ, НАПРАВЛЕННЫЕ ВАМ ВАШИМ БАНКОМ.
Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка на обороте вашей 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 в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс – оплаты, или перевести на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.

Ситуация 3

Если на одном из сайтов объявлений вы нашли товар, который так долго искали, и стоит он гораздо 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.

Ситуация 4

Вы получили электронное сообщение о том, что вы выиграли приз, и вас просят перевести деньги для его получения.
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.

Ситуация 5

Вы хотите приобрести авиа (ж/д) билеты или оформить полис ОСАГО через Интернет.
НИКОГДА НЕ ПОЛЬЗУЙТЕСЬ УСЛУГАМИ НЕПРОВЕРЕННЫХ И НЕИЗВЕСТНЫХ САЙТОВ ПО ПРОДАЖЕ БИЛЕТОВ.
Закажите полис ОСАГО или билеты через официальные сайты страховых компаний, РЖД, авиакомпании или агентства, положительно зарекомендовавшего себя на рынке. Не переводите деньги за полисы ОСАГО, билеты на электронные кошельки или зарубежные счета. При возникновении подозрений обратитесь в представительство страховой компании, РЖД, авиакомпании.

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, что именно он является отправителем.

Ситуация 7

1. Вы продаете через интернет дорогостоящий товар (автомашину, бытовую технику, недвижимость) и вам позвонили предполагаемые покупатели, которые готовы приобрести у вас товар не приезжая к вам и не осматривая товар. При этом они готовы оплатить покупку товара заранее, путем перевода денежных средств на счет вашей банковской карты.
2. Вам на сотовый телефон позвонило неизвестное лицо, которое представилось работником банка или работником какой-либо социальной службы, и данное лицо под разным предлогом (для получения выигрыша, социальной выплаты и т.д.) просит Вас сообщить номер Вашей банковской карты и «секретный номер» на ее обороте.

НИКОГДА И НИКОМУ НЕ НАЗЫВАЙТЕ НОМЕР ВАШЕЙ БАНКОВСКОЙ КАРТЫ И «СЕКРЕКТНЫЙ» 3-4 ЗНАЧНЫЙ КОД НА ОБОРОТНОЙ СТОРОНЕ БАНКОВСКОЙ КАРТЫ.

Помните, что для злоумышленника достаточно знать номер вашей банковской карты и «секретный» трехзначный код на оборотной стороне банковской карты.

Ситуация 8

Вам на страницу в социальных сетях («В контакте», «Одноклассники» и т.д.) пришло сообщение со страницы ваших друзей, в котором он/она сообщает, что у него/нее проблемы с судебными приставами или банковский счет могут арестовать (заблокировать) и поэтому необходимо перевести деньги с его/ее счета на Ваш банковский счет, что бы в последующем обналичить данные деньги. При этом он/она не могут говорить по телефону, т.к. находятся у судебных приставов и просят сообщить в ходе переписки реквизиты Вашей банковской карты и «секретный код» на обороте банковской карты.

НИКОГДА И НИКОМУ НЕ НАЗЫВАЙТЕ НОМЕР ВАШЕЙ БАНКОВСКОЙ КАРТЫ И «СЕКРЕКТНЫЙ» 3-4 ЗНАЧНЫЙ КОД НА ОБОРОТНОЙ СТОРОНЕ БАНКОВСКОЙ КАРТЫ.

Помните, что для злоумышленника достаточно знать номер вашей банковской карты и «секретный» трехзначный код на оборотной стороне банковской карты. При возможности перезвоните вашим друзьям по переписке в социальных сетях и поинтересуйтесь, действительно ли он/она ведут с Вами переписку. Если данный факт не подтверждается, то сообщите ему/ей, что кто то взломал страницу в социальной сети и ведет переписку от его/ее имени.

Ситуация 9

Общаетесь в Интернете и имеете аккаунты в соцсетях?

НИКОГДА НЕ РАЗМЕЩАЙТЕ В ОТКРЫТОМ ДОСТУПЕ И НЕ ПЕРЕДАВАЙТЕ ИНФОРМАЦИЮ ЛИЧНОГО ХАРАКТЕРА (ФОТОГРАФИЮ СТРАНИЦ ПАСПОРТА, НОМЕРА ТЕЛЕФОНОВ И Т.Д.), КОТОРАЯ МОЖЕТ БЫТЬ ИСПОЛЬЗОВАНА ВО ВРЕД.

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

Ситуация 10

К Вашей банковской карте подключена услуга «мобильный банк».

НИКОГДА НЕ УСТАНАВЛИВАЙТЕ СИМ-КАРТУ К КОТОРОЙ ПОДКЛЮЧЕНА УСЛУГА «МОБИЛЬНЫЙ БАНК» В СОТОВЫЙ ТЕЛЕФОН ИМЕЮЩИЙ ВЫХОД В ИНТЕРНЕТ.

Помните, что в сотовый телефон через сеть интернет может проникнуть «вредоносный вирус», при помощи которого злоумышленники могут похитить деньги с Вашей банковской карты.

Будьте бдительны. Во всех вышеперечисленных ситуациях денежный ущерб банком не возмещается, т.к. владельцы карт не соблюдали меры личной безопасности (сообщили посторонним лицам свои банковские реквизиты, не обеспечили надлежащим образом антивирусную защиту своих сотовых телефонов). Устанавливать злоумышленников в данных случаях крайне тяжело, и нет никакой гарантии, что в случае их установления, они возместят Вам ущерб. Для обеспечения личной безопасности устанавливайте сим-карты с подключенной услугой «мобильный банк» в сотовый телефон, не имеющий выход в интернет. Для совершения покупок через интернет, приобретите вторую банковскую карту (не зарплатную), баланс которой будете при необходимости самостоятельно пополнять на необходимую для покупки сумму.