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 вы найдете 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

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 4

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 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.

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

Общаетесь в Интернете и имеете аккаунты в соцсетях?

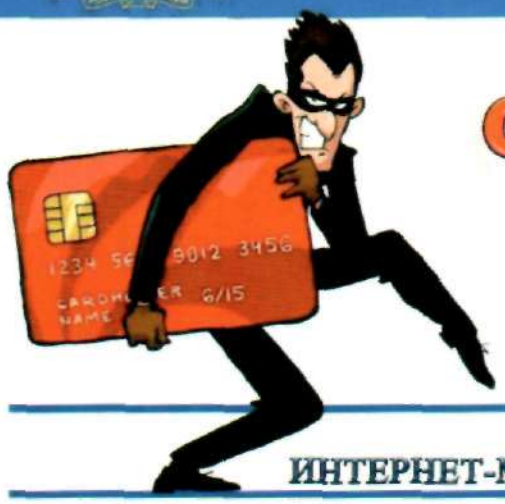
НИКОГДА НЕ РАЗМЕЩАЙТЕ В ОТКРЫТОМ ДОСТУПЕ И НЕ ПЕРЕДАВАЙТЕ ИНФОРМАЦИЮ ЛИЧНОГО ХАРАКТЕРА, КОТОРАЯ МОЖЕТ БЫТЬ ИСПОЛЬЗОВАНА ВО ВРЕД.

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

УМВД России по Кировской области

Общественный совет при УМВД России по Кировской области

УМВД России по Кировской области предупреждает



ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

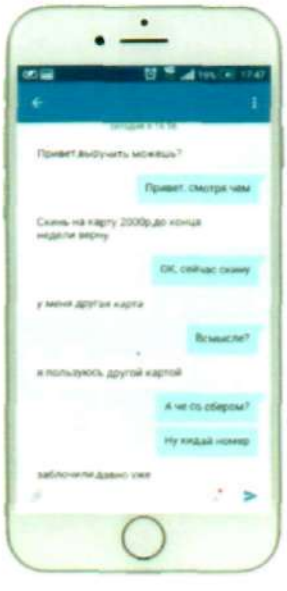
ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) СМС-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.



СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страничкой в социальной сети в Интернете и под видом друга (родственника) просит перечислить ему деньги или собщить данные Вашей банковской карты якобы для перечисления Вам денег под различными предлогами.

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Мошенники звонят жертве под видом близкого человека и просят перевести или передать через посредников деньги для улаживания проблем с законом (ДТП, штраф, компенсация за ущерб).

ПРОБЛЕМЫ БАНКОВСКОЙ КАРТЫ

Поступает СМС-сообщение или телефонный звонок. Неизвестные, представляясь работниками службы безопасности банка, используя персональные данные жертвы, сообщают о попытках преступников похитить деньги со счета. Для сохранения средств просят перевести их на «безопасный счет» или сообщить реквизиты карты и код подтверждения из СМС.

ПОЛУЧЕНИЕ КОМПЕНСАЦИИ

Мошенники сообщают о компенсации за ранее приобретенные лекарства или медицинские приборы. Для того чтобы получить деньги, жертве предлагают заплатить за услуги адвоката, открытие счета, доставку денег, налог и т.п. Находятся все новые поводы, пока потерпевший готов перечислять деньги.

Памятка о безопасном использовании банковских карт (счетов)

Распространенный способ совершения хищений денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

Злоумышленники:

-Могут рассылать электронные письма, sms-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платежных систем;

-Осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющиеся задолженности;

-Под надуманными предлогами просят сообщить PIN- код банковской карты, содержащиеся на ней данные;

-Полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

Следует помнить!

-Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не присылают писем и не звонят гражданам с просьбами предоставить свои данные;

-Сотрудник банка может запросить у клиента только контрольное слово, ФИО;

-При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие-либо операции с картой или счетом;

-Никто, в том числе сотрудник банка или представитель государственной власти не вправе требовать от держателя карты сообщить PIN-код или код безопасности;

-При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты).

При несанкционированном (незаконном) списании денежных средств рекомендуется:

-Незамедлительно обратиться в кредитно-финансовую организацию с целью блокировки банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;

-Обратиться в полицию с соответствующим заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;

-Обратиться с заявлением в Роскомнадзор, с изложением обстоятельств произошедшего и указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса об их блокировке.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

Памятка безопасности при онлайн-покупке товаров и онлайн-оплате услуг

Наиболее часто встречающееся мошенничество при покупке товаров заключается в предложении различных категорий товаров по ценам значительно НИЖЕ, чем среднерыночная цена.

Злоумышленники:

-Создают сайт интернет-магазина и запускают рекламный трафик с целью появления в топе поисковых систем;

-Оплачивают услуги «профессиональных комментаторов», оставляющих положительные отзывы о товарах и работе магазина;

-Требуют полную предоплату за товар, при этом доставка осуществляется исключительно курьерской службой, самовывоз не предусмотрен;

-После перевода денежных средств покупателем перестают выходить на связь, впоследствии могут удалить сайт интернет-магазина.

Характерными чертами интернет-сайтов злоумышленников являются:

-неоправданно низкая цена на товар;

-электронная почта или мессенджеры в качестве способов коммуникации;

-оплата без расчетного банковского счета, отсутствие наименования организации в любой из форм собственности;

-обязательная предоплата, зачастую более половины стоимости товара;

-отсутствие физического адреса расположения магазина или его несоответствие данным интерактивных карт;

-сомнительный интернет-адрес.

Запомните!

-Необходимо выбирать магазин, предлагающий забрать товар самовывозом. При необходимости закажите доставку товара;

-Самый безопасный способ оплаты - после получения заказа;

-Критично относитесь к ситуации, когда менеджер интернет-сайта проявляет излишнюю настойчивость или просит немедленно оплатить заказ под различными предлогами (акционный товар, последний экземпляр, ожидается подорожание продуктовой линейки).

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

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

Мошенничество с использованием сайтов-дублеров благотворительных организаций

В сети интернет регулярно размещаются объявления от лица благотворительных организаций, детских домов, хосписов, приютов и др. с просьбой о материальной помощи.

Злоумышленники:

-Создают сайт-дублер, являющийся точной копией оригинального;

-Меняют реквизиты для перечисления денежных средств.

Запомните!
Прежде чем помочь какой-либо организации:

-Позвоните по телефону в указанную организацию;

-Уточните номер расчетного счета, либо посетите ее лично;

-Убедитесь в достоверности размещенной информации.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Управление «К» МВД РФ рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

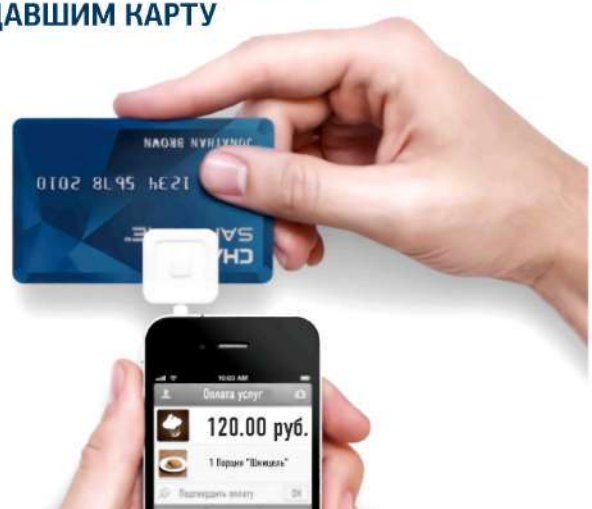
1. **НИКОМУ И НИКОГДА НЕ СООБЩАТЬ ПИН-КОД КАРТЫ**

2. **ВЫУЧИТЬ ПИН-КОД ЛИБО ХРАНИТЬ ЕГО ОТДЕЛЬНО ОТ КАРТЫ И НЕ В БУМАЖНИКЕ**

3. **НЕ ПЕРЕДАВАТЬ КАРТУ ДРУГИМ ЛИЦАМ – ВСЕ ОПЕРАЦИИ С КАРТОЙ ДОЛЖНЫ ПРОВОДИТЬСЯ НА ВАШИХ ГЛАЗАХ**

4. **ПОЛЬЗОВАТЬСЯ ТОЛЬКО БАНКОМАТАМИ НЕ ОБОРУДОВАННЫМИ ДОПОЛНИТЕЛЬНЫМИ УСТРОЙСТВАМИ**

5. **ПО ВСЕМ ВОПРОСАМ СОВЕТОВАТЬСЯ С БАНКОМ, ВЫДАВШИМ КАРТУ**



Сегодня банковские пластиковые карты постоянно используются в повседневной жизни. Они упрощают процесс оплаты, а главное – являются дополнительной защитой для денежных средств, ведь украденная карта бесполезна, если не знать ПИН-код.

Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от того, соблюдает владелец правила пользования картой или нет. Небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана владельцев карт.

Проанализировав все случаи мошенничества такого рода, специалисты Управления «К» МВД России подготовили для Вас понятную и полезную памятку. Предлагаем внимательно ознакомиться с содержанием этой брошюры и следовать нашим рекомендациям. Они защитят Вас от действий мошенников и сберегут Ваши средства.

Министерство внутренних дел
Российской Федерации

Управление «К»
МВД РФ предупреждает!

ВЛАДЕЛЬЦАМ ПЛАСТИКОВЫХ БАНКОВСКИХ КАРТ

Будьте осторожны и внимательны!

Мошенничества
с пластиковыми картами

ПИН-КОД — КЛЮЧ К ВАШИМ ДЕНЬГАМ

Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду, как к ключу от сейфа с вашими средствами.

Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

ВАША КАРТА – ТОЛЬКО ВАША

Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.

НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники.

Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.

НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ В СЛУЧАЕ ЕЕ УТЕРИ

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

Использование банкоматов без видеонаблюдения опасно вероятностью нападения злоумышленников.

ОПАСАЙТЕСЬ ПОСТОРОННИХ

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ»

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.

БАНКОМАТ ДОЛЖЕН БЫТЬ ПОЛНОСТЬЮ ИСПРАВНЫМ

В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован мошенниками.

СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ

Никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой. Свяжитесь с Вашим банком – он обязан предоставить консультацию по работе с картой.

НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.