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.

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.

ВАМ ПОЗВОНИЛ ЧЕЛОВЕК И ПРЕДСТАВИЛСЯ СОТРУДНИКОМ КРЕДИТНОГО УЧРЕЖДЕНИЯ ИЛИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ?

ОН УТВЕРЖДАЕТ, ЧТО:

- ✕ по вашему счёту совершаются подозрительные переводы?
- ✕ необходимо спрочно получить зеркальный заём?
- ✕ нужно перевести деньги на безопасный счёт?

Не верьте! ЭТО МОШЕННИКИ!
ПРЕРВИТЕ РАЗГОВОР и позвоните в полицию!

ВЫ РЕШИЛИ СЭКОНОМИТЬ НА ПОКУПКЕ ДОРОГОСТОЯЩЕЙ ТЕХНИКИ И ВДРУГ НАТКНУЛИСЬ НА ПРЕДЛОЖЕНИЕ ПРИОБРЕСТИ ТОВАР С БОЛЬШОЙ СКИДКОЙ?

НО ДЛЯ ЭТОГО ПРОСЯТ:

- ! перейти в мессенджер для заказа?
- ! оплатить товар по сторонней ссылке?
- ! внести предоплату?

Остановитесь и всё обдумайте!
ВОЗМОЖНО, ВАС ОБМАНЫВАЮТ!

И ПОМНИТЕ:
бесплатный сыр только в мышеловке!

Вам предлагают взять кредит, который в будущем окупится и принесёт большую прибыль?

Нашли в сети заманчивое предложение дополнительного заработка на акциях известной компании?

Стали часто общаться с брокерами, звонящими с неизвестных номеров?

ОСТОРОЖНО!
ТАК ДЕЙСТВУЮТ МОШЕННИКИ!

1. Прервите разговор!
2. Не регистрируйтесь и не указывайте личные данные на подозрительных сайтах!
3. Не вкладывайте свои деньги в сомнительные проекты!
4. Не сообщайте персональные данные людям, которых вы не знаете лично!
5. Обратитесь в полицию!

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО!

МОШЕННИКИ!

Звонок ОТ МОШЕННИКА

ПРИЗНАКИ

1. Вам предлагают перевести свои денежные средства на БЕЗОПАСНЫЙ СЧЁТ;
2. Вас просят ПРОДИКТОВАТЬ реквизиты банковской карты или ВВЕСТИ их на сайте;
3. Вам предлагают ОТМЕНИТЬ (взять) заявку на КРЕДИТ или ЗАБЛОКИРОВАТЬ банковскую карту;
4. Вам предлагают получить БОНУСЫ и ПОДАРКИ от банка, а также различные КОМПЕНСАЦИИ;
5. Вам предлагают оформить БЕЗОПАСНУЮ СДЕЛКУ или ДОСТАВКУ, при ПОКУПКЕ/ПРОДАЖЕ ТОВАРОВ в сети Интернет, при этом скидывают Вам ссылку;

ЗАПОМНИТЕ!

НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ, поступившие с неизвестных номеров, особенно зарегистрированных в другом регионе;

НЕ ВЕРЬТЕ любой информации от незнакомца, **ДАЖЕ ЕСЛИ** звонок поступил с официального телефона горячей линии банка;

ПРЕРВИТЕ РАЗГОВОР и самостоятельно позвоните на телефон горячей линии банка, набрав номер **ВРУЧНУЮ**;

ПОМНИТЕ: код от вашей карты и пароли подтверждения операций **НЕ ИМЕЕТ ПРАВА** спрашивать даже сотрудник банка!

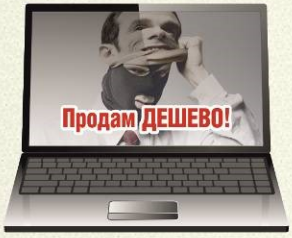
44.мвд.рф

ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

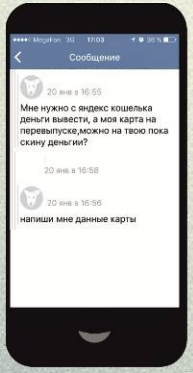
ОБЪЯВЛЕНИЕ О ПРОДАЖЕ



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.



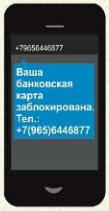
СООБЩЕНИЯ ОТ ДРУЗЕЙ

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

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

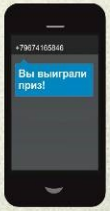
Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.



БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)



Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

ВИРУС В ТЕЛЕФОНЕ

Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.

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.