



МВД России

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ЧЕЛЯБИНСКОЙ ОБЛАСТИ
(ГУ МВД России по Челябинской области)

ул. Елькина, 34, Челябинск 454091

28.04.2022 № 11/2021

на № _____ от _____

О профилактике безопасного
поведения при использовании
банковских карт

Экз. № _____

Министру образования и науки
Челябинской области

А.И. Кузнецову
454113, Челябинск, пл. Революции, 4,
minobr@gov74.ru

Уважаемый Александр Игоревич!

Направляю в Ваш адрес материалы для организации и проведения профилактических мероприятий с учащимися образовательных учреждений Челябинской области, а также их родителями направленных на информирование о безопасном использовании банковских карт (счетов).

Приложение: на 3 листах (только в адрес).

Заместитель начальника
- начальник полиции

С.В. Богдановский



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 предложениями 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.

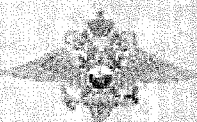
Характерными чертами интернет-сайтов злоумышленников являются:

- 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.



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.