ВНИМАНИЕ!!! Это важно знать.

Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет следует:

1. вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки, не переходя по ссылкам (зачастую торговые площадки блокируют возможность перехода на **поддельные ресурсы**);
2. ведя общение с пользователем стоит перейти к его профилю и обратить внимание на **дату создания** (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);
3. очень внимательно относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). **Самый надежный способ** уберечь свои средства - это **никому не сообщать реквизиты своей карты**;
4. уточнить у собеседника номер телефона если он не указан в объявлении, а потом позвонить на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку (очень часто злоумышленники используют номера телефонов, взятые в аренду на непродолжительное время и физического доступа к нему, не имеют);
5. использовать отдельную банковскую карту для осуществления покупок в сети Интернет (оформить в банке так называемую **«нереальную карту»** и класть на нее необходимое для покупки количество денег непосредственно перед совершением сделки), на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии;
6. избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки. Если Вам прислали такую ссылку, то, независимо от того, кто ее прислал, прежде чем по ней перейти, следует внимательно проверить доменное имя (адрес ресурса). Сделать это можно отыскав в интернете официальный сайт и сверив написание доменного имени. Отличие хотя-бы в одну букву или символ свидетельствует о том, что перед Вами ссылка на поддельный ресурс.

Если Вы все же ввели данные своей банковской карты на поддельном ресурсе или сообщили их постороннему лицу, ***необходимо в срочном порядке произвести блокировку карты, позвонив в банк либо самостоятельно в интернет-банкинге.***