

Защитись от телефонных мошенников!

В настоящее время хищение электронных денежных средств является одним из распространенных преступлений.

В отличие от обычного хищения, кража с банковской карты (банковского счета), независимо от суммы похищенного является тяжким преступлением, так как вернуть похищенные деньги гораздо сложнее.

В соответствии со ст. 210 Гражданского кодекса РФ гражданин несёт бремя содержания своего имущества, а, следовательно, должен обеспечивать сохранность, в том числе своих денег, находящихся на банковской карте, и не допускать разглашения сведений о банковской карте.

Чтобы не поддаться на уловки злоумышленников, необходимо соблюдать правила безопасного поведения, в том числе при использовании мобильными телефонами и пластиковыми картами:

- пользоваться защищенными банкоматами, расположенными в безопасных местах и оборудованных системой видеонаблюдения;
- ни при каких обстоятельствах не сообщать посторонним номер своей банковской карты, который указан на ее лицевой и оборотной стороне, срок действия карты и CVC-код;
- не сообщать кому-либо по телефону сведения о персональных данных (ФИО владельца карты, серия и номер паспорта, адрес регистрации);
- никогда не называть и не показывать пин-код карты (4-х значный цифровой номер). Храните его отдельно от карты;
- при смене абонентского номера телефона, к которому был подключен «мобильный банк», необходимо обратиться в банк и написать заявление об отключении данной услуги от старого номера телефона;
- в случае утери (кражи) карты немедленно сообщите в банк о пропаже и напишите заявление о блокировании карты.

Устанавливая различные приложения на мобильный телефон, обращайтесь внимание на полномочия, которые в связи с этим запрашиваются. Будьте осторожны, если приложение запрашивает права на доступ к адресной книге к сети «Интернет» и отправку СМС-сообщений - вероятно, это мошенники.

При оплате услуг картой в сети «Интернет» (особенно если карта привязана к регулярным платежам или аккаунтам) необходимо учитывать высокую вероятность перехода на поддельный сайт. Поэтому необходимо использовать только проверенные сайты, внимательно читать тексты СМС-сообщений с кодами подтверждений, проверять реквизиты операции.

По всем возникающим вопросам необходимо позвонить в службу поддержки или обратиться лично в ближайшее отделение банка.

Проявляйте бдительность и обеспечивайте сохранность своего мобильного телефона и, банковских карт!