

Мошенничества с использованием банковских карт

Большинство людей для удобства подключают к своей банковской карте услугу «мобильный банк» и с помощью нее совершают различные операции: узнают текущий баланс на карте, переводят с нее денежные средства, получают информацию о списании денег и т.д.

В случае если мошенник имеет доступ к вышеуказанной услуге, то он может перевести ваши денежные средства на любой счет по всей России. Поэтому если к телефону подключена опция «мобильный банк», то ни в коем случае не давайте свой телефон неизвестным людям, даже если он просит у вас совершить звонок. Помните, мошеннику потребуется всего лишь несколько секунд, чтобы провести комбинации по переводу с вашей карточки денежных средств.

Кроме того, устанавливайте на ваш гаджет антивирусное программное обеспечение и периодически обновляйте его. При скачивании нужных вам интернет-программ, вместе с ними, в телефон может попасть и вредоносная программа (вирус), которая, находясь в вашем смартфоне, «обнаружит» всю информацию, касающуюся вашего счета и ваших паролей, и, используя услуги «мобильный банк», переведет денежные средства на счета мошенников.

Также не становится меньше случаев, когда звонит неизвестный человек, представляется сотрудником банка и говорит, что ваша банковская карта заблокирована и для разблокирования необходимо ввести какой-нибудь код или цифры и отправить по номеру. Человек, слыша в телефоне приятный и вежливый голос, думает, что карту действительно заблокировали и выполняет требования оппонента, даже не подозревая, что переводит свои денежные средства мошеннику.

Во избежание таких ситуаций нужно следовать простым правилам:

1. Никогда не передавайте незнакомым лицам свой сотовый телефон и не скачивайте с Интернета подозрительные или незнакомые программы, так как они могут оказаться вирусными.

2. Если вам позвонили и представились сотрудником банка, то не выполняйте никаких операций через телефон, лучше обратитесь в ближайший офис банка и узнайте там информацию по вашей банковской карте.

3. Никогда не отправляйте ответы на СМС - сообщения, в которых вам говорится, что вы выиграли что-либо.

4. Никогда не сообщайте код доступа, номер своей карты и пароль кому бы то ни было, даже если этот человек представился сотрудником банка.

5. Не вводите в Интернете каких-либо данные своей банковской карты, а если вы совершили какую-либо покупку, старайтесь искать более безопасные пути оплаты товара.