Будьте бдительны!
Мошенничество с банковскими пластиковыми картами

Банковские пластиковые карты – способ совершения преступления

Банковские пластиковые карты каждый из нас использует в повседневной жизни.

Они упрощают процесс оплаты, а главное – являются дополнительной защитой для денежных средств, ведь украденная карта бесполезна, если не знать PIN-код.

Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от того, соблюдает владелец правила пользования картой или нет.

Небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана владельцев карт.

Самое трудное для мошенников – узнать PIN-код. Для этого могут использоваться различные способы.

В первую очередь, это оглашение сведений о PIN-коде самим держателем карты. Имеется в виду, например, его запись на карте или каком-либо другом носителе (лист бумаги, записная книжка и др.), хранимая вместе с картой.

Также карты могут быть использованы людьми с предварительной осведомленностью о PIN-коде: членами семьи, близкими друзьями, коллегами по работе - то есть теми, кто имеет доступ к хранению карты.

Помимо этого, мошенник может узнать PIN-код держателя банковской карты, подглядывая из-за его плеча, пока тот вводит код в банкомате, либо во время оплаты покупки в магазине.

Последние годы злоумышленники чаще всего звонят гражданам, представляясь сотрудниками банков, называя по имени – отчеству, и просят сообщить данные карт. При этом могут быть использованы программы подмены телефонных номеров, входящий звонок может определяться у клиента как номер банка.

Для совершения мошенничества с кредитными картами могут использоваться фальшивые банкоматы либо переделанные старые банкоматы. Размещаются они в наиболее оживленных местах. После введения карты и PIN-кода на дисплее такого банкомата появляется надпись, что денег в банкомате нет или что банкомат неисправен.

Также преступники могут использовать особые устройства, считывающие информацию с магнитных полос карты (скимминг). Как правило, это специально изготовленные клавиатуры, которыми накрывают существующие.

Нередко мошенники для кражи денег пользуются психологическими приемами для управления действиями человека. Они изображают покупателей автомобилей, земельных участков, животных, мебели, одежды и др. на сайтах бесплатных объявлений или в социальных сетях. При этом они все находятся где-то далеко, но для того чтобы вожделенный товар не приобрел кто-то другой, они готовы перевести часть стоимости или даже полную стоимость немедленно на банковскую карту продавца.

Основные правила безопасности для владельцев пластиковых карт

1. Никогда и никому не сообщаете PIN-код карты, не пишите его на карте или другом носителе, не храните его рядом с картой. **Выучите** PIN-код**.**
2. Для оперативного получения информации об операциях по расчетному счету подключите на телефоне услугу «СМС-оповещение».
3. Обратившись в обслуживающий Вас банк, установите лимит (дневной) снятия наличных денежных средств с карты.
4. Не стесняйтесь закрывать от посторонних **клавиатуру банкомата** во время ввода PIN-кода.
5. Снимайте денежные средства и производите операции по карте в банкоматах, которые расположены в офисах банка, рядом с ними, или находящимися в государственных учреждениях, крупных торговых центрах и т.д.

Банкомат не должен выглядеть подозрительно. Обратите внимание на то, не прикреплены ли к нему какие – либо дополнительные устройства, не имеются ли на экране дополнительные инструкции, надписи и др.

6. Не пользуйтесь советами третьих лиц и не прибегайте к помощи незнакомцев при возникновении проблем в работе с банкоматом. В таком случае необходимо сразу же позвонить в службу поддержки клиентов банка, телефоны которой, как правило, указаны на банкомате.

7. Не передавать карту другим лицам, все операции с картой должны проводиться на Ваших глазах. В торговых точках, ресторанах и кафе все действия с пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты карты и при помощи специальных устройств использовать их в дальнейшем для изготовления подделки.

8. Пользуясь картой в сети «Интернет», внимательно относитесь к своевременному обновлению антивирусной программы. Не совершайте покупки на подозрительных сайтах, обращайте внимание на поддержку сайтами технологии 3D-Secure.

Не держите на карте, которую используете для платежей в сети «Интернет», крупную сумму. Для совершения покупки дистанционно лучше оформить отдельную карту или выпустить «виртуальную карту».

9. Если карта утрачена или есть подозрения, что данные карты стали известны третьему лицу, незамедлительно позвоните в банк и заблокируйте карту. Если Вы подключены к сервису «Мобильный банк», то блокировку можно сделать при помощи направления SMS-уведомления.

10. Не сообщайте данные карты, персональные данные, коды, сведения, содержащиеся в SMS-уведомлениях, посторонним лицам. Не давайте никому доступ к Вашей карте через онлайн-банкинг.

11. Регулярно меняйте PIN-код Вашей карты. Особенно после заграничных поездок или снятия денег в подозрительных местах.

Только Ваша бдительность и внимательность поможет Вам не стать жертвой преступления!

Информационный материал подготовлен прокуратурой Кировской области совместно с Общероссийской общественной организацией «Ассоциация юристов России»

Прокуратура Кировской области
610000 г. Киров, ул. Володарского, д. 98
«Телефон доверия»: 8(8332) 38-11-53
E-mail: prokuror@oblast.kirov.ru

Общероссийская
общественная организация
АССОЦИАЦИЯ ЮРИСТОВ РОССИИ
Кировское региональное отделение
г. Киров, ул. Дерендяева, 23, к.108
тел./факс (8332) 64-98-11
E-mail:info@alrf43.ru