Памятка владельцам банковских карт как защититься от мошенников

Всем владельцам пластиковых карт необходимо следовать правилам безопасности:

1. Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить.

Во избежание использования Вашей карты третьим лицом храните ПИН-код отдельно от карты, исключив одновременный доступ к ним, не пишите ПИН-код на карте, не сообщайте ПИНкод другим лицам (в том числе родственникам), не вводите ПИН-код при работе в сети Интернет.

2. Ни при каких обстоятельствах никому не сообщайте CVC- или CVV- коды банковской карты и одноразовые пароли, включая работников Банка.

Внимание! Если для входа в мобильное приложение Банка или личный кабинет на официальном сайте Банка, Вам предлагается ввести любую другую персональную информацию или дополнительные данные (номер мобильного телефона, контрольную информацию по банковским картам или другие данные), это указывает на мошенничество! В таких случаях необходимо немедленно прекратить сеанс работы в системе и срочно обратиться в Банк. Если Вам предлагается ввести пароль для отмены операции, в том числе и той, которую Вы не совершали, Вам необходимо прекратить сеанс работы в системе и срочно обратиться в Банк. При получении от Банка СМС-сообщения с одноразовым паролем внимательно ознакомьтесь с информацией в сообщении: все реквизиты операции в направленном Вам сообщении должны соответствовать той операции, которую Вы собираетесь совершить. Только после того как Вы убедились, что информация в этом СМС-сообщении корректна, можно вводить пароль.

Внимание! Если Вы получили СМС-сообщение от Банка по операции, которую Вы не совершали, необходимо срочно заблокировать карту с помощью онлайн-услуги или обратиться в Контактный центр Банка и следовать указаниям специалиста.

3. Используйте только официальные мобильные приложения Банка, доступные в официальных магазинах приложений производителей мобильных платформ. Обязательно убедитесь, что в поле «разработчик мобильного приложения» указан Банк, выдавший пластиковую карту.

4. Не позволяйте никому использовать Вашу пластиковую карту. В торговых точках, ресторанах и кафе и других общественных местах все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

5. Не доверяйте звонящему - банку, Центробанку, полиции и другим ведомствам. Мошенники могут представляться разными организациями и использовать скрытые или подменные номера - это значит, что на экране Вы можете увидеть номер банка, а звонит на самом деле мошенник. Не сообщайте никакие данные, даже если угрожают уголовным делом или другими последствиями. Даже если называют Вас по имени и отчеству и знают другую личную информацию, вы можете повесить трубку без предупреждения, не прощаясь, и сразу перезвонить в банк самостоятельно.

Во время разговора возьмите паузу. Вас будут торопить и говорить, что деньги могут украсть или заблокировать на счете в любой момент. Противостоять этому напору трудно: звонок от банка или госструктуры - стрессовая ситуация. Но перед тем как отвечать на вопросы мошенника, сделайте паузу, чтобы успокоиться. Не бывает ситуаций, в которых вам нужно быстро провести операцию, даже если это настоящий звонок из банка.

Внимание! Ни сотрудники банка, ни сотрудники полиции не просят взять гражданина кредит для поимки преступников с последующим помещением денежных средств на безопасный «резервный» счет.

Ни сотрудники банка, ни сотрудники полиции не станет предлагать установить какие-либо сторонние программы и приложения на ваш телефон.

Внимание! НИКТО, в том числе сотрудник Банка или представитель государственных органов не вправе требовать от держателя карты сообщить ПИН-код или код безопасности.

6. При пользовании банкоматом:

- прикрывайте клавиатуру при вводе ПИН-кода, вводите ПИН-код быстрыми отработанными движениями - это может помочь при установке мошенниками скрытых камер;

- выбирайте только те банкоматы, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д. Граждане, пользующиеся банкоматами без видеонаблюдения, могут подвергнуться нападениям злоумышленников;

- обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону;

- обращайте внимание на экран банкомата - дождитесь приветственных слов, обозначающих начало работы нового пользователя. В любых подозрительных случаях нажмите на клавишу ОТМЕНА 2-3 раза.

- В случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или самопроизвольно перезагружается - откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

Как защитить карту от злоумышленников?

- Установите услугу СМС-уведомлений, оповещающих о движении средств по счету.
- Никому не сообщайте пароль или CVV-код карты.
- Всегда выходите из аккаунтов интернет-банка и не сохраняйте пароль в браузере.
- Установите лимит на снятие наличных средств по карте.
- Подключите двухфакторную аутентификацию в финансовых приложениях, подтверждайте оплаты кодом из смс или пуш-уведомлений

Будьте бдительны!

- не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках.

- Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем звонит якобы растяпа, который по ошибке зачислил вам деньги и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС - не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.

- Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок опять же от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас код, чтобы списать с вашего счета деньги или подписать вас на ненужный платный сервис.

- Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.

Внимание! В случае если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка.

Внимание! В случае если Вы все же пострадали от мошенничества:

1. Необходимо немедленно обратиться (желательно лично) в Контактный Центр Банка для блокировки карты, реквизиты которой были сообщены посторонним или по которой были совершены несанкционированные операции, и следовать рекомендациям специалиста.

2. По факту мошенничества рекомендуется обратиться в правоохранительные органы по телефонам 02 или 102, а также подать заявление.