Информация для граждан

Сведения о дебетовых и кредитных картах

ПИН-код карты – четырехзначная комбинация цифр, выдаваемая в конверте одновременно с изготовленной банковской картой. Его можно изменить, обратившись в отделение банка или позвонив на горячую линию.

Код безопасности **(CVV**2 или **CVC**2) – комбинация цифр, указанная на оборотной стороне карты, а именно: три крайние правые цифры, указанные после четырех последних цифр номера карты. Проверочный код необходим только для совершения платежей в интернете. При онлайн-оплате он вводится вместе с номером карты, именем держателя карты и сроком окончания действия карты.

Одноразовый пароль банка для подтверждения оплаты онлайн – комбинация цифр, отправляемых банком в смс-сообщении или push- уведомлении для подтверждения операций с денежными средствами.

Никому не сообщайте ПИН-код, код безопасности или одноразовый пароль третьим лицам!

Никто, в том числе сотрудники банка, не вправе требовать от держателя карты сообщить ПИН-код или код безопасности. А одноразовый пароль вводится при совершении онлайн-покупки на странице с защищенным соединением.

Кодовое слово держателя карты – информация, указанная клиентом банка при оформлении карты. Кодовое слово необходимо для идентификации клиента при звонке в контакт-центр банка. Рекомендуется использовать кодовые слова, которые злоумышленникам будет очень сложно узнать. Подумайте о том, что случилось с Вами в детстве или юности, вспомните место действия, объект, человека или событие – пусть оно будет Вашим кодовым словом.

Код клиента банка – комбинация цифр, используемая для сокращения времени на идентификацию клиента при обращении в контакт-центр.

Сообщать кодовое слово или код клиента банка можно только в том случае, если вы обратились в контакт-центр и разговариваете с сотрудником банка.

Как безопасно пользоваться интернет-банком?

1. Используйте сложный пароль блокировки экрана и качественную антивирусную программу. Не входите в банковские приложения, используя отпечаток пальца или функцию распознавания лица.

2. Ни в коем случае не храните в телефоне логин и пароль от входа в мобильный банкинг.

3. Не храните в телефоне реквизиты карты: номер, срок действия, проверочный код и ПИН-код карты.

4. Избегайте входа в систему мобильного банкинга с чужих устройств.

5. При утрате телефона немедленно обратитесь в банк для блокировки карты и в офис мобильного оператора для блокировки SIM-карты.

6. Не переходите по ссылкам из SMS-сообщений, даже если в сообщении утверждается, что оно из банка.

7. Отключите функцию отображения текста входящих SMS- уведомлений на экране заблокированного телефона.

ВАЖНО!

Довольно часто мошенники выдают себя за сотрудников банка. Под предлогом «сбоя в базе данных», «начисления бонусов» или «подключения к социальной программе» злоумышленники просят, а иногда даже требуют сообщить им реквизиты карты, код безопасности и одноразовый пароль. Получив необходимые сведения, мошенники списывают деньги со счета.

ПОМНИТЕ!

При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты карты и совершать какие-либо операции с картой.

Что делать, если вам позвонили из банка, и интересуются вашей платежной картой?

Разумнее всего прекратить разговор и перезвонить в банк по официальному номеру контактного центра банка (номер телефона службы поддержки клиента указывается на оборотной стороне карты).

Также можно обратиться в отделение банка лично. Помните, что самый распространенный способ совершения хищений денежных средств с карт граждан – побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

Как безопасно совершать платежи в интернете?

8. Используйте на устройстве антивирус с активной защитой онлайн- платежей.

9. Совершайте оплату только посредством использования защищенных соединений. Защищенное или зашифрованное подключение можно распознать по значку в виде замочка в начале адресной строки браузера и префиксу https:// (не просто http, а с буквой s на конце) перед адресом сайта.

10. Всегда завершайте сеанс в интернет-банке перед тем, как закроете вкладку браузера. Не проводите финансовые операции с общественного WI-FI в кафе, транспорте или гостиницах.

11. Не сохраняйте свои данные о карте в браузере.

Какими банкоматами пользоваться?

12. Отдавайте предпочтение банкоматам, установленным в защищенных местах (например, в офисах банков, госучреждениях, крупных торговых центрах).

13. Осмотрите банкомат перед использованием. Убедитесь, что на клавиатуре и в месте для приема карт нет дополнительных устройств, следов клея и механических повреждений.

14. При наборе ПИН-кода прикрывайте клавиатуру рукой.

15. Не используйте банкомат с признаками неисправности: устройство зависает, перезагружается или на экране появляются подозрительные изображения.

16. Не используйте банкомат в присутствии подозрительных лиц и не принимайте помощь от незнакомцев.

Банковские трояны

Банковские трояны – вредоносные программы, созданные для кражи денег через онлайн-банкинг. Подменяя страницу официальных банковских приложений, крупных онлайн-магазинов, программа похищает логины и пароли, а также данные банковских карт. Для обхода двухфакторной аутентификации программа способна перехватывать отправленные банком смс-сообщения и перенаправлять их.

Чаще всего под видом легального программного обеспечения: пользователь собственноручно скачивает на устройство вирусную программу, замаскированный под популярные бесплатные приложения (например, игры, фонарики, гороскопы и пр.). Также банковский троян автоматически скачивается на устройство при переходе по сомнительным ссылкам, присланным в смс-сообщениях или электронных письмах. Как правило, в сообщении ссылку на скачивание банковского трояна сопровождает текст о начале распродажи, предложении обменять товар или посмотреть фото/видео интригующего содержания.

Как защититься?

17. Установить на устройство надежную антивирусную защиту. Она блокирует попытку перехода на подозрительный сайт, а также остановит банковский троян при попытке проникнуть в устройство.

18. Не переходить по подозрительным ссылкам в смс-сообщениях и электронных письмах.

19. Скачивать приложения только из официальных магазинов Apple Store, Microsoft Store и Google Play. В настойках телефона установить запрет на скачивание приложений из непроверенных источников.

20. В ходе установки приложений обращать внимание на запросы разрешений (например, доступ к контактам и на отправку смс-сообщений).

21. Внимательно читать название сайта, на котором вводятся конфиденциальные данные. Зачастую названия сайтов-подделок от оригинальных отличаются лишь одним символом.

Безопасность учетных записей

Завладев логином и паролем от учетной записи электронной почты, социальной сети, портала госуслуг и других сервисов, мошенники получают возможности для извлечения материальной выгоды. И это не только списание средств с банковской карты. Войдя в чужую учетную запись, мошенники могут рассылать контактам пользователя сообщения с просьбой о переводе небольшой, как правило, суммы денег, или публиковать на странице информацию компрометирующего характера.

Как не оказаться в подобной ситуации?

22. Для каждой учетной записи использовать разные логины и пароли. Использовать сложные пароли, состоящие из букв и цифр. Создавать и хранить их поможет менеджер паролей.

23. Для максимальной защиты учетной записи рекомендуется использовать двухэтапную аутентификацию (для входа в аккаунт кроме логина и пароля необходимо ввести одноразовый код или подтвердить действие на электронных устройствах, подключенных к вашему аккаунту).