Почему важно знать какие банковские данные нужно хранить в тайне?

Важно знать, какие банковские данные нужно хранить в тайне, потому что это помогает предотвратить мошенничество и кражу личных данных. Если мошенники получат доступ к вашим банковским данным, они могут украсть ваши деньги, оформить кредиты на ваше имя или опустошить ваш банковский счёт. Знание, какие данные являются конфиденциальными, поможет вам принять меры для их защиты и сохранить свои средства и информацию.

Что такое реквизиты банковской карты?

Реквизиты банковской карты — это уникальные данные, которые указаны на самой карте и в договоре с банком. Они необходимы для использования карты, выполнения переводов, снятия наличных, оплаты товаров и услуг безналичным способом. Основные реквизиты включают:

- имя и фамилию владельца
- наименование банка
- срок действия карты
- номер карты
- номер счета
- код CVV/CVC — код из 3 или 4 цифр для совершения интернет-платежей, расположенный на обратной стороне
- ПИН-код (секретный четырёхзначный пароль)
- Смс-коды для подтверждения расходных операций

Какие реквизиты можно сообщать о карте

Можно сообщать следующие реквизиты карты:

- номер карты (целиком или частично);
- номер счёта, к которому выпущена карта;
- срок действия карты (месяц и год).

Эти данные можно сообщить знакомым, которые хотят перевести деньги, или при обращении в банк для блокировки или перевыпуска карты.

Почему нельзя сообщать 3-значный номер на обратной стороне банковской карты

Трёхзначный номер на обратной стороне банковской карты — это CVC2, который используется для проверки подлинности карты при совершении покупок в интернете. Этот номер содержит важную информацию о вашей карте и должен храниться в тайне.

Если у вас просят трёхзначный номер на обратной стороне банковской карты, это может быть признаком мошенничества. В этом случае рекомендуется немедленно заблокировать свою карту и обратиться в службу поддержки банка для консультации.

Реквизиты банковской карты, которые нельзя сообщать никому при любых условиях

Реквизиты банковской карты, которые нельзя сообщать никому:

1. Номер карты — мошенники могут использовать эту информацию для незаконных операций.
2. Срок действия — мошенники могут использовать эту информацию для подделки карты.
3. Имя владельца — мошенники могут использовать эту информацию для кражи личности.
4. CVV2/CVC — этот код используется для подтверждения платежей, и его передача может привести к несанкционированным операциям.
5. Сим-код нельзя сообщать при выполнении операции, потому что это конфиденциальная информация, которая может быть использована мошенниками для доступа к вашему мобильному банку и кражи денег с вашего счёта.

Эти данные должны быть известны только владельцу карты и сотрудникам банка. Что касаемо pin-кода от банковского приложения. Его нельзя сообщать никому, даже сотрудникам банка. Этот код предназначен исключительно для использования владельцем карты и служит для дополнительной защиты средств на счёте.

На что способны мошенники, зная реквизиты вашей банковской карты

Зная реквизиты банковской карты, мошенники могут:

- Совершать покупки от вашего имени в интернет-магазинах, используя номер карты, фамилию и имя владельца, срок действия и CVV-код.
- Оплачивать товары и услуги в некоторых приложениях, таких как Google Pay, используя номер карты, фамилию и имя владельца, срок действия и CVV-код.
- Переводить деньги на вашу карту с последующим требованием возврата, используя номер карты и ваше имя.
- Открывать вклады и брать кредиты на ваше имя, используя номер карты, фамилию и имя владельца, срок действия и CVV-код.
- Пополнять электронные кошельки, используя номер карты, фамилию и имя владельца, срок действия и CVV-код.

Мошенники также могут перевести деньги на вашу карту с пометкой «зачисление средств по кредитному договору» и потребовать возврата с процентами.

Как защитить реквизиты банковской карты

Для защиты реквизитов вашей банковской карты следуйте этим рекомендациям:

1. Не сообщайте секретные данные карты (CVV, PIN-код) посторонним лицам. Сотрудники банка могут спросить только кодовое слово.
2. Не публикуйте в социальных сетях фото банковской карты и сканы документов.
3. Установите двухфакторную аутентификацию для входа в онлайн-банк и проведения операций.
4. Обратитесь в отделение вашего сотового оператора, чтобы изменить процедуру смены сим-карты.
5. Не переходите по подозрительным ссылкам и скачивайте только официальные приложения банков из App Store, Google Play и RuStore.
6. Используйте сложные пароли и периодически меняйте их.
7. Расплачивайтесь в интернете отдельной картой или её цифровым аналогом.
8. При оплате в магазине используйте смартфон для подтверждения операции.
9. Отключите всплывающие уведомления на телефоне.

10. Если получаете странные сообщения от банка, сразу звоните по официальному номеру.