Безопасное пользование банковскими картами.

Трудно на сегодняшний день представить жизнь без ежедневного использования банковских карт и различных онлайн платежей. Банковская карта дает возможность приобретать необходимое, не имея при этом с собой денег как таковых. Но, тем не менее, владельца карты постоянно подстерегает опасность – при использовании банкомата, при совершении покупок, просто на улице и даже в банке при общении с операционистом.



**Общие правила безопасного использования банковской карты:**

* Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании карты.
* ПИН необходимо запомнить или хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.
* Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам.
* При получении банковской карты распишитесь на ее оборотной стороне. Это снизит риск использования карты без Вашего согласия в случае ее утраты.
* Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.
* Телефон кредитной организации указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны кредитной организации.
* С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по банковской карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений).
* При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о банковской карте (в том числе ПИН) не сообщайте их.
* Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации предлагается предоставить персональные данные. Не следуйте по “ссылкам”, указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.
* В целях информационного взаимодействия с кредитной организацией рекомендуется использовать только реквизиты средств связи которые указаны в документах, полученных непосредственно в кредитной организации — эмитенте банковской карты.
* В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию следовать указаниям сотрудника данной кредитной организации.

**Операции с банковской картой в банкомате:**

* Осуществляйте операции с использованием банкоматов, установленных в безопасных местах.
* Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.
* В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.
* Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт.
* В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.
* Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.
* Набирайте ПИН таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть.
* В случае если банкомат работает некорректно, следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку “Отмена”, и дождаться возврата банковской карты.
* После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что банковская карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.
* Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
* Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
* Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию, которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

**Безналичная оплаты товаров и услуг:**

* Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
* Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.
* При использовании карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН.
* В случае если при попытке оплаты банковской картой имела место “неуспешная” операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

**Оплата картой в Интернете:**

* Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
* Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет.
* С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.
* Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.
* Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.
* Рекомендуется совершать покупки только со своего компьютера.
* Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление.

Что такое CVC/CVV код на карте и как он защищает деньги

***Каждый кто хоть раз оплачивал онлайн-покупки банковской картой вводил CVC/CVV код, который расположен с обратной стороны банковской карты. Этот код является защитой вашей банковской карты, его цель – проверка подлинности карты. Эксперты Регионального центра финансовой грамотности Калининградской области рассказали о работе этого кода и основной его цели.***

**Что такое CVC/CVV-код**

При оплате покупок в магазинах на сумму более 1 тыс. рублей терминалы, как правило, просят ввести ПИН-код — пароль от банковской карты. В интернете же безопасность платежей гарантирует security code — это три цифры, которые есть на обратной стороне каждой банковской карты.

У разных платежных систем этот код называется по-разному:

* CVV2 (card verification value 2, англ.) — трехзначный код проверки подлинности карты платежной системы Visa.
* CVC2 (card validation code 2, англ.) — защитный код для карт Mastercard.
* CVP2 (card verification parameter 2, англ.) — код подлинности карт платежной системы «Мир».

Цифра 2 в названии говорит о том, что существует и первый защитный код — CVV/CVC-код. Он, как правило, записан непосредственно на магнитную полосу карты и служит для проверки подлинности пластиковой карты при офлайн-покупках. Код считывается терминалами автоматически, поэтому на карте его найти не получится и в жизни CVV2/CVC2-коды называют CVV/CVC-кодами.

**Зачем нужен код?**

Три цифры нудны для защиты от аферистов. Как и ПИН-код, CVV2/CVC2-коды являются конфиденциальной информацией, которые по правилам использования банковской карты – нельзя передавать третьим лицам. Операцию с вводом CVV2/CVC2-кода может совершить любой человек, получивший доступ к карточке.

CVV/CVC код, в отличие от ПИН-кода, указан на самой карте, поэтому обеспечить его конфиденциальность сложнее. В этой связи важно помнить, что передавать банковскую карту посторонним лицам нельзя!

**Защита от мошенников**

При оплате онлайн-покупок банковской картой, как правило, магазины требуют ввести платежную информацию: номер банковской карты, срок ее действия, имя и фамилию держателя и трехзначный код безопасности. Код как раз таки и нужен для подтверждения того, что покупку совершает законный владелец карточки. Если ошибиться с вводом кода – покупку совершить не получится. Очевидно, что код безопасности — это еще один барьер для защиты от мошенников.



Для повышения безопасности онлайн-платежей, многие банки уже давно применяют двухфакторную идентификацию покупателей (технология 3D-Secure). Для совершения оплаты требуется ввести одноразовый пароль из СМС или push-уведомления, который направляется на привязанный к карте номер телефона. На сайтах, поддерживающих 3D-Secure, есть специальные значки Mastercard SecureCode и Visa Secure.

У национальной платежной системы «Мир» есть собственная технология — MirAccept (на основе 3D-Secure). Крупные банки, активно переходят на новую версию этой технологии, MirAccept 2.0. Ее принципиальной особенностью является наличие анализа совокупности факторов, помогающих идентифицировать пользователя (платежное поведение, параметры устройств, геолокация и пр.). В отличие от двухфакторной аутентификации с использованием СМС-кода, такой способ проверки подлинности плательщика является более надежным, позволяет ускорить процесс оплаты и увеличить количество успешных платежей.

**Памятка для безопасного использования банковских карт**

⚠️ не передавать карту посторонним (кассирам, официантам и даже сотрудникам банка);

⚠️не сообщать код безопасности и иную конфиденциальную информацию о карте по телефону, даже если звонящий представляется работником банка или правоохранительных органов;

⚠️ не выкладывать фото карты в сети интернет;

⚠️ расплачиваться картой только с проверенного устройства;

⚠️ устанавливать на все гаджеты, с которых расплачиваетесь в интернете лицензионный антивирус;

⚠️ не пользоваться бесплатным, общественным Wi-Fi для денежных операций в интернете;

⚠️ не расплачиваться картой в сомнительных интернет-магазинах, на игровых или лотерейных сайтах — такие сервисы часто являются мошенническими;

⚠️ незамедлительно блокировать карту при ее утере или краже.

Нелишним будет иметь отдельную карту для онлайн-платежей и пополнять ее только на сумму, необходимую для покупки.

Использованные ресурсы:

1. <https://stopmoshennik.com/russia/>

2. Banki.ru <https://www.banki.ru/news/daytheme/?id=10985509>

3. <https://ru.wikipedia.org/>

4. <https://cbr.ru/>

5. <https://openbudget.irkobl.ru/sodeystvie/federalnyy-uroven/>

Информацию подготовил:

ведущий специалист ФУА МО Куйтунский район А.А. Кошкарева