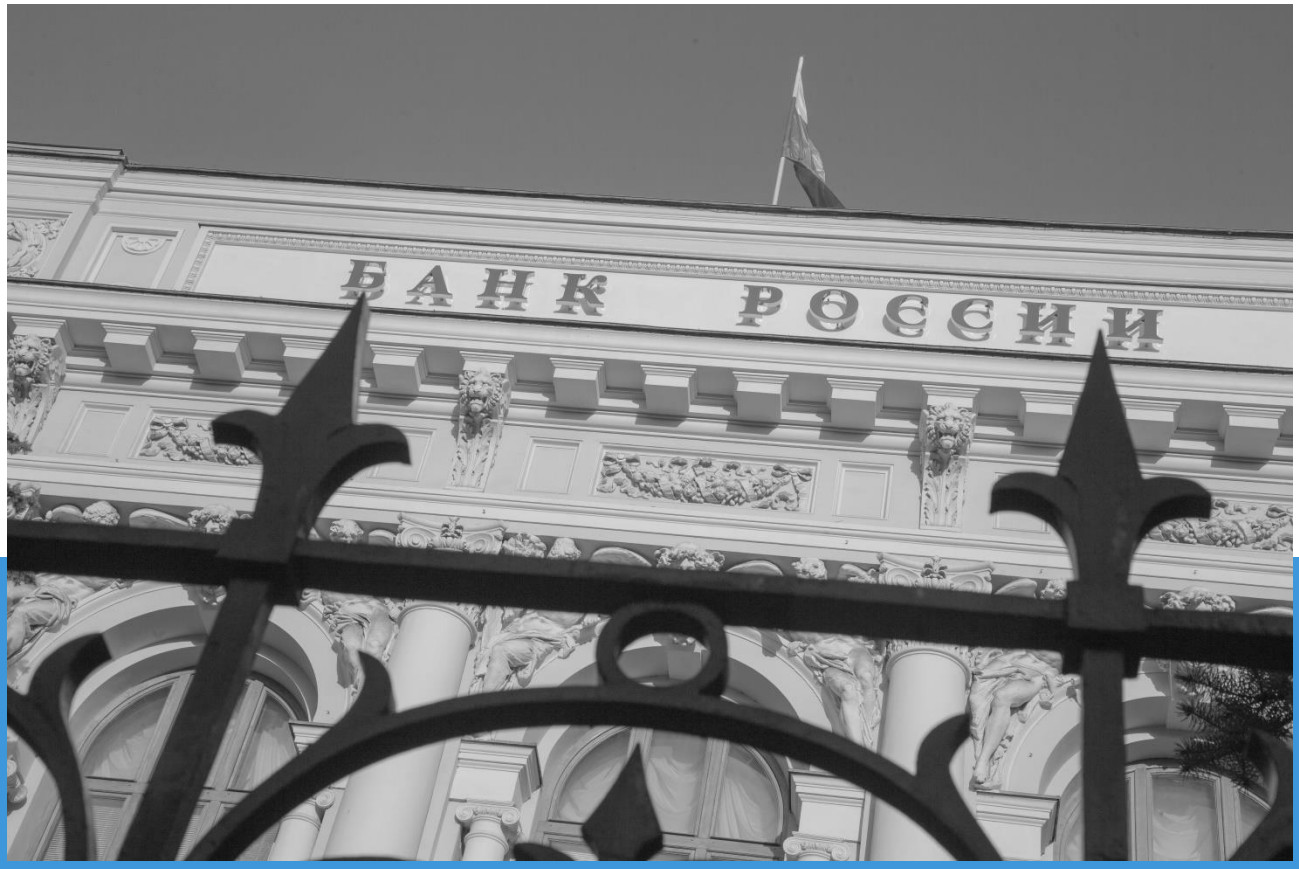
Банк России

Центральный банк Российской Федерации



Безопасность платежных услуг

Информационный материал

Москва

2015

Содержание

Безопасность при использовании платежных карт

Банк России рекомендует всем держателям платежных карт соблюдать основные меры по обеспечению безопасности при получении платежной карты в банке, при ее хранении, использовании в банкомате, предприятиях торговли и услуг, в том числе для оплаты товаров и услуг в сети Интернет.

Общие рекомендации держателям платежных карт при получении в банке и хранении платежной карты

1. Вместе с платежной картой выдается запечатанный конверт (ПИН-конверт) с персональным идентификационным номером (ПИН–кодом), который необходим при проведении операций с использованием устройств самообслуживания (банкоматов) или терминалов в предприятиях торговли и услуг либо кредитных организациях через операционно-кассового работника. При получении платежной карты и конверта с ПИН-кодом проверьте отсутствие следов вскрытия конверта, сохраните его в недоступном для посторонних лиц месте.

2. Рекомендуется всегда иметь при себе номер платежной карты, а также контактные телефоны кредитной организации – эмитента карты, которые расположены на оборотной стороне карты.

3. Не записывайте ПИН-код на платежной карте, его рекомендуется запомнить либо хранить отдельно от карты в недоступном для посторонних лиц месте. Если кредитная организация – эмитент позволяет сменить ПИН-код, замените его на запоминающуюся комбинацию цифр.

4. Следует игнорировать электронные письма, в которых от имени кредитной организации – эмитента поступают просьбы сообщить любые данные о карте. Не рекомендуется переходить по ссылкам, в том числе по ссылкам на сайт кредитной организации, указанным в электронном письме, так как они могут привести Вас на мошеннические сайты – двойники.

5. Существует риск потерять все денежные средства с банковского счета в случае потери платежной карты, либо если карта была украдена, а также в случае кражи ПИН-кода и Ваших персональных данных. Необходимо немедленно сообщить в кредитную организацию о факте утраты платежной карты, либо о том, что ПИН-код и персональные данные узнали посторонние лица, и следовать инструкциям работника кредитной организации.

Рекомендации держателям платежных карт по использованию платежной карты в банкомате

1. Для совершения операций с использованием платежной карты, необходимо выбирать банкоматы, установленные в безопасных местах, а также в местах, в которых банкоматы находятся под видеонаблюдением (в подразделениях кредитных организаций, государственных учреждениях, аэропортах, крупных торговых комплексах и т.п.).

2. Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.

3. Прежде чем использовать платежную карту в банкомате, убедитесь в наличии на банкомате эмблемы платежной системы, соответствующей карте, а

также информации о банке, обслуживающем банкомат.

4. Прежде чем использовать банкомат, необходимо осмотреть его. Если обнаружены «посторонние» устройства, не соответствующие его конструкции, или дополнительные устройства на картоприемнике или клавиатуре для набора ПИН-кода, необходимо использовать другой банкомат. О банкомате, вызывающем подозрения, следует сообщить в кредитную организацию, обслуживающую банкомат.

5. При вводе ПИН-кода необходимо прикрывать клавиатуру рукой.

6. В случае если возникли сомнения в надлежащей работе банкомата (например, банкомат работает некорректно, долгое время находится в режиме ожидания, либо самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию по карте и дождаться возврата платежной карты.

7. Получив наличные денежные средства в банкомате, не забудьте взять платежную карту из картоприемника во избежание попадания ее в руки злоумышленника.

8. Нельзя доверять советам третьих лиц и прибегать к помощи посторонних при совершении операций по карте в банкомате, за исключением работников кредитной организации.

9. В случае если банкомат не возвращает карту, необходимо позвонить в кредитную организацию, чтобы сообщить о случившемся и следовать указаниям работника кредитной организации.

10. В случае если денежные средства не были выданы банкоматом, но были списаны с банковского счета, следует обратиться в кредитную организацию и написать заявление о несогласии с операцией.

Рекомендации держателям платежных карт по их использованию в предприятиях торговли и услуг

1. Не следует использовать платежную карту в предприятиях торговли и услуг, не вызывающих доверия.

2. Требуйте проведения операций с платежной картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения персональных данных, указанных на платежной карте.

3. При оплате товаров и услуг по карте кассир может попросить подписать чек, ввести ПИН-код или предоставить удостоверение личности. Перед тем, как ввести ПИН-код убедитесь в том, что находящиеся в непосредственной близости люди, не смогут его увидеть, либо прикрывайте ввод ПИН-кода рукой. Прежде чем подписывать чек, проверьте указанную в нем сумму.

4. Если оплата по платежной карте не прошла, сохраните чек, выданный терминалом, чтобы в дальнейшем проверить отсутствие этой операции в выписке по счету, а в случае ее наличия, заявить в кредитную организацию об этой операции.

Рекомендации держателям платежных карт по совершению операций по карте в сети Интернет

1. Заказывая товары и услуги по телефону или при работе в сети Интернет, не следует сообщать и вводить ПИН-код. Если при оплате товаров и услуг в сети Интернет продавец запросил ПИН-код, в

таком случае следует сообщить об этом продавце в кредитную организацию.

2. С целью предотвращения неправомерного снятия всей суммы денежных средств с банковского счета, целесообразно установить суточный лимит на сумму операций по платежной карте. При совершении покупок в сети Интернет рекомендуется использовать отдельную карту, предназначенную для оплаты товаров и услуг через сеть Интернет.

3. Во избежание неправомерного использования Ваших персональных данных со стороны третьих лиц, рекомендуется делать покупки со своего компьютера. Если покупки осуществлялись на чужом компьютере, не сохраняйте на нем персональные данные.

4. Необходимо установить на свой компьютер антивирусное программное обеспечение, регулярно проводить его обновление и обновление других используемых программных продуктов (операционной системы и прикладных программ), это поможет защитить компьютер от проникновения вредоносного программного обеспечения.

5. Не используйте карту для покупок через web – сайты, которые не используют специальные средства для защиты информации о платежной карте. Безопасные web – сайты отмечены значком в виде закрытого замочка, адрес сайта должен начинаться с https://.

6. Рекомендуется делать покупки на Интернет–сайтах проверенных и надежных предприятий торговли и услуг, использующих технологию безопасного проведения операций по платежным картам в сети Интернет. На таких Интернет–сайтах указаны отметки платежных систем: «Verified by Visa», «MasterCard SecureCode».

7. Операции в сети Интернет в защищенном режиме рекомендуется проводить с использованием одноразовых паролей, которые можно получить в виде СМС-сообщения или списка в кредитной организации или банкомате кредитной организации.

Безопасность при использовании компьютеров и мобильных устройств для осуществления переводов денежных средств

Использование дистанционных методов оплаты товаров и услуг удобно для клиентов, при этом безопасность денежных средств связана с тем, насколько ответственно пользователь относится к безопасности устройства, используемого для осуществления переводов денежных средств (компьютера, ноутбука, мобильного телефона).

При осуществлении переводов денежных средств с использованием систем Интернет-банкинга злоумышленники зачастую действуют в целях хищения логинов и паролей, иной информации, позволяющей получить доступ в систему Интернет-банкинга.

Рекомендации для клиентов кредитных организаций при совершении платежей с использованием систем Интернет-банкинга

1. Рекомендуется ограничить доступ посторонних лиц к компьютеру (ноутбуку, планшету), используемому для работы с системой Интернет-банкинга, например,

установив пароль. Если не планируется использование системы в течение длительного времени, рекомендуется завершить работу и выйти из нее.

2. При возникновении подозрений о том, что логин или пароль для входа в систему Интернет-банкинга узнали посторонние лица, а также при осуществлении попытки несанкционированного доступа к системе Интернет-банкинга под Вашей учетной записью, необходимо незамедлительно информировать о случившемся кредитную организацию.

3. Не храните пароль на вход в систему Интернет-банкинга непосредственно на компьютере или около него. Не рекомендуется применять один и тот же пароль на сайтах, используемых для работы с системой Интернет-банкинга и иных сайтах. Если кредитная организация предоставляет такую возможность, обязательно смените пароль в систему Интернет-банкинга при первом входе и периодически его меняйте.

4. Внедрение на компьютер (ноутбук, планшет) вредоносного кода позволяет злоумышленнику собирать информацию о действиях в системе Интернет-банкинга и управлять удаленно компьютером. Поэтому необходимо устанавливать на компьютере (ноутбуке, планшете) современные средства обеспечения информационной безопасности при работе в сети Интернет. Основными из таких средств являются лицензионные средства антивирусной защиты и межсетевые экраны. Рекомендуется настроить автоматическое обновление антивирусных баз, а также регулярно проводить антивирусную проверку. Рекомендуется не отключать установленные средства защиты и периодически проверять их работу.

5. Не рекомендуется использовать открытые сети для доступа к системе Интернет-банк (точки доступа wi-fi, сети операторов мобильной связи). При использовании средств доступа к домашним сетям рекомендуется изменять установленные производителем пароли роутера, используемого для доступа в сеть, а также использовать шифрование.

6. На компьютере (ноутбуке, планшете), используемом для работы с системой Интернет-банкинга, необходимо исключить посещение сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения.

7. При использовании системы Интернет-банкинга проверяйте защищенность web–сайта. Безопасные web–сайты отмечены значком в виде закрытого замочка, адрес сайта должен начинаться с https://. В случае если сайт вызывает подозрения, обратитесь в кредитную организацию с использованием контактных данных, указанных на официальном сайте.

Рекомендации для клиентов банков при совершении платежей с использованием мобильных устройств

1. Необходимо устанавливать только официальные мобильные приложения кредитной организации, доступные в репозиториях (магазинах приложений) производителей мобильных платформ. При этом необходимо обязательно убедиться в том, что в качестве разработчика или автора приложения указана кредитная организация.

2. Рекомендуется использовать специализированное приложение кредитной организации, если оно доступно, поскольку мобильные браузеры более уязвимы по

сравнению с браузерами, используемыми на компьютерах и ноутбуках.

3. Рекомендуется своевременно устанавливать доступные обновления операционной системы и приложений на мобильный телефон.

4. Рекомендуется использовать антивирусное программное обеспечение для мобильного телефона и регулярно обновлять его базы.

5. Не переходите по ссылкам и не устанавливайте приложения и обновления программ, направленные по смс или электронной почте, в том числе от имени кредитной организации.

6. Не рекомендуется хранить в мобильном телефоне пароли и иную информацию, необходимую для доступа к мобильному банку.

7. Рекомендуется установить пароль на мобильном телефоне при наличии такой функции.

8. Никогда не передавайте мобильный телефон и SIM-карту третьим лицам.

9. Необходимо помнить, что подключение услуги мобильный банк к номеру телефона позволяет получить доступ к банковскому счету с использованием этого номера телефона.

10. Отправка сообщений на короткие номера позволяет списывать и переводить денежные средства как со счета в кредитной организации, так и со счета оператора мобильной связи.

11. В случае смены номера или утери телефона, в обязательном порядке следует обратиться в кредитную организацию для отключения услуги мобильный банк.

Общие рекомендации по обеспечению безопасности

1. Никогда не сообщайте третьим лицам, в том числе родственникам, знакомым, работникам кредитной организации, работникам предприятий торговли и услуг ПИН-код, CVV/CVC-код платежной карты, логины, пароли и иные коды, которые могут быть использованы для доступа к системе Интернет-банкинга, а также кодовое слово, паспортные данные. Не передавайте платежную карту и носители указанных выше сведений (скретч-карты, генераторы одноразовых паролей, средства электронной подписи и др.).

2. Если кто-нибудь попросил сообщить указанную выше информацию, необходимо позвонить в кредитную организацию и сообщить о случившемся.

3. Помните, что в случае разглашения персональных данных, ПИН-кода, утраты платежной карты возможно совершение злоумышленниками неправомерных действий с денежными средствами на банковском счете.

4. Кредитная организация не осуществляет рассылку программ для установления на компьютер, ноутбук, планшет и мобильный телефон, а также электронных писем с просьбой прислать персональные данные, пароли, данные счетов. Никогда не отвечайте на электронные письма, запрашивающие указанные сведения. Удаляйте любые полученные сообщения, содержащие ссылки на web-страницы и предлагающие ввести персональные данные.

5. Проверяйте все сообщения о платежах, обращая особое внимание на сумму и получателя.

Необходимо незамедлительно связаться с кредитной организацией, в случае

если уведомление поступило дважды или получено уведомление о платеже, который не был совершен.

Необходимо регулярно проверять состояние банковского счета и отслеживать выполненные операции по счету, в том числе с использованием систем Интернет-банкинга.

6. Следует осуществлять взаимодействие с кредитной организацией только с использованием контактов, указанных в документах, получаемых непосредственно от кредитной организации или иных официальных информационных источников кредитной организации (офисы, сайт и т.д.).

7. При смене контактных данных, в том числе в случае потери или смены номера телефона, который используется для получения услуг мобильного банкинга, необходимо обязательно сообщить об этом в кредитную организацию.

Подготовлено Управлением общественных коммуникаций совместно
с Департаментом национальной платежной системы Банка России

www.cbr.ru/fingramota