Венецбанк
основан в 1990 г.

Акционерное общество Банк «Венец»
432071, г. Ульяновск, ул. Марата, д.19; тел. / факс (8422) 32 62 84,
ИНН 7303024532, ОГРН 1027300000166, БИК 047308813
к/с № 30101810200000000813 в Отделении по Ульяновской
области Волго-Вятского главного управления ЦБ РФ
Многоканальная линия 8 800 707 55 99, www.venets-bank.ru,
e-mail: office@venets-bank.ru

ПРАВИЛА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ

В связи с участившимися попытками неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания (пароли, секретные ключи средств шифрования и аналогов собственноручной подписи, ПИН-коды и номера банковских карт, а также персональные данные их владельцев) Центральным Банком Российской Федерации для кредитных организаций распространено Письмо от 07.12.2007 года №197-Т «О рисках при дистанционном банковском обслуживании», которое содержит варианты попыток неправомерного получения информации персональной информации пользователей систем дистанционного банковского обслуживания, а именно:

1. По системам электронной почты направляются сообщения, в которых по каким-либо предлогам (техническое перевооружение организации, обновление или сверка баз данных кредитной организации и т.п.) предлагается ввести с клавиатуры компьютера указанные коды в поля экранных форм в ходе имитируемых сеансов информационного взаимодействия с кредитной организацией (к примеру, через созданный дубликат ее web-сайта). Одновременно на компьютер клиента с web-сайта могут передаваться вредоносные программы, являющиеся компьютерными вирусами или "закладками", выполняющими в фоновом режиме работы скрытые функции, связанные с неправомерным получением персональной информации пользователей систем дистанционного банковского обслуживания.
2. При проведении операций через банкоматы также наблюдаются случаи неправомерного получения реквизитов банковских карт. При этом используются накладные устройства на клавиатуру для ввода ПИН-кода или на устройство для приема карт в банкомат, а также специально приспособленные для этих целей "фальшивые" банкоматы, которые незаконно устанавливаются, как правило, в не контролируемых Банком местах и внешне не отличаются от банкоматов, используемых для дистанционного банковского обслуживания клиентов кредитных организаций.
3. При получении различными способами реквизитов банковских карт возможно изготовление поддельных банковских карт, частично (так называемый "белый пластик") или полностью имитирующих подлинные. При использовании в банкоматах поддельные банковские карты предоставляют их обладателям все возможности подлинных банковских карт.
4. В целях неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания используются также различные варианты телефонного мошенничества. В частности, отмечаются случаи направления мошенниками на мобильные телефоны клиентов Банка SMS-сообщений о необходимости позвонить по номерам телефонов, которые в действительности не принадлежат этим организациям. Также имеют место звонки клиентам с сообщением автоинформаторов о предоставлении продуктов и услуг банка с предложением нажать определенные клавиши на телефоне для подтверждения согласия в их приобретении и т.п. Тем самым клиенты банка провоцируются к вступлению в контакты с мошенниками, целью которых в том числе может являться получение конфиденциальной клиентской информации (например, номера банковской карты и ПИН-кода).

В связи с вышеизложенным, Банк распространяет рекомендации по безопасному использованию банковских карт, включающие в себя:

1. Общие рекомендации;
2. Рекомендации при совершении операций с банковской картой в банкомате;
3. Рекомендации при использовании банковской карты для безналичной оплаты товаров и

услуг;

4. Рекомендации при совершении операций с банковской картой через сеть Интернет;

1.1 Общие рекомендации

1.1.1 Никогда не сообщайте ПИН - код третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим вам в использовании банковской карты.

1.1.2 ПИН - код необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.

1.1.3 Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту.

1.1.4 При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без вашего согласия в случае ее утраты.

1.1.5 Будьте внимательны к условиям хранения и использования банковской карты. 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.

1.1.6 Телефон кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту) указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны кредитной организации - эмитента банковской карты и номер банковской карты на других носителях информации: в записной книжке, мобильном телефоне и (или) других носителях информации, но не рядом с записью о ПИН - коде.

1.1.7 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 или иным способом).

1.1.8 При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о банковской карте (в том числе ПИН - код) не сообщайте их. Перезвоните в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и сообщите о данном факте.

1.1.9 Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту)) 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.

1.1.10 В целях информационного взаимодействия с кредитной организацией - эмитентом банковской карты (кредитной организации, выдавшей банковскую карту) рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов (порталов), обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в кредитной организации - эмитенте банковской карты.

1.1.11 Помните, что в случае раскрытия ПИН – кода, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на вашем банковском счете со стороны третьих лиц.

В случае если имеются предположения о раскрытии ПИН - кода, персональных данных, позволяющих совершить неправомерные действия с вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и следовать указаниям сотрудника данной кредитной организации. До момента обращения в кредитную организацию - эмитент банковской карты вы несете риск, связанный с несанкционированным

списанием денежных средств с вашего банковского счета. Согласно условиям договора с кредитной организацией - эмитентом банковской карты денежные средства, списанные с вашего банковского счета в результате несанкционированного использования вашей банковской карты до момента уведомления об этом кредитной организации - эмитента банковской карты, не возмещаются.

1.2 Рекомендации при совершении операций с банковской картой в банкомате

1.2.1 Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

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

1.2.3 В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.

1.2.4 Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН - кода и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН – кода). В указанном случае воздержитесь от использования такого банкомата.

1.2.5 В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.

1.2.6 Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.

1.2.7 Набирайте ПИН - код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН - кода прикрывайте клавиатуру рукой.

1.2.8 В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку "Отмена", и дождаться возврата банковской карты.

1.2.9 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.

1.2.10 Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.

1.2.11 Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.

1.2.12 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 - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту), которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

1.3 Рекомендации при использовании банковской карты для безналичной оплаты товаров и услуг

1.3.1 Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.

1.3.2 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.

1.3.3 При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН - код. Перед набором ПИН - кода следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке. Подписывая данный документ, вы признаете правильность указанной суммы и тем самым даете указание Банку на перечисление со Счета данной суммы на счет обслужившей вас организации.

1.3.4 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.

1.4 Рекомендации при совершении операций с банковской картой через сеть Интернет

1.4.1 Не используйте ПИН -код при заказе товаров и услуг через сеть Интернет, а также по телефону (факсу).

1.4.2 Не сообщайте персональные данные или информацию о банковской карте или банковском счете через сеть Интернет, например, ПИН - код, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.

1.4.3 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.

1.4.4 Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.

1.4.5 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.

1.4.6 Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской карте или банковском счете.

В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).

1.4.7 Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых вами программных продуктов (операционной системы и прикладных программ), это может защитить вас от проникновения вредоносного программного обеспечения.