Уважаемый Клиент!

В связи с тем, что в последнее время участились случаи получения злоумышленниками несанкционированного доступа к управлению счетами Клиентов и как следствие осуществления несанкционированных списаний со счета Клиента, уведомляем Вас о необходимости строгого соблюдения мер информационной безопасности при совершении операций в платежной системе «Мультисервисная платежная система» (далее – Платежная система), направленных на предотвращение хищений денежных средств Клиентов.

Реализация несанкционированного доступа к управлению счетами Клиентов, а также доступ к иной защищаемой информации может быть осуществлена злоумышленниками путем внедрения на рабочие станции Клиентов, подключенных к сети Интернет, с которых осуществляется доступ к системе удаленного доступа «Личный кабинет», вредоносного программного обеспечения.

На данный момент злоумышленники применяют различные способы для получения доступа к денежным средствам Клиентов:

- фишинг, т.е. использование вредоносного программного обеспечения в целях перенаправления Клиента на поддельный сайт для получения необходимой для доступа аутентификационной информации;
- скримминг, т.е. использование встроенных в платежные терминалы и устройства самообслуживания средств съема информации, а также средств видеонаблюдения для получения реквизитов платежной карты и аутентифкационной информации к ней;
- SMS- и e-mail-мошенничество, т.е. рассылка сообщений с целью использования доверия Клиентов и (или) внедрения вредоносного программного обеспечения для получения аутентификационных данных Клиента.

Современное вредоносное программное обеспечение, используемое для получения удаленного доступа к средствам управления счетами Клиента, способно предоставлять злоумышленнику не только возможность удаленного управления рабочей станцией Клиента, но и возможность сокрытия произведенных мошеннических действий.

Мы постоянно совершенствует меры, направленные на защиту денежных средств Клиентов при осуществлении переводов денежных средств в Платежной системе. Принимаемые меры основаны на современных методах и технологиях, однако их эффективность напрямую зависит от участия Клиентов.

В целях предотвращения мошеннических операций с денежными средствами рекомендуем Вам соблюдать все необходимые меры и рекомендации, указанные в настоящей «Памятке клиентам по соблюдению мер информационной безопасности в Платежной системе при использовании системы удаленного доступа «Личный кабинет» и (или) электронных терминалов»[1].

[1] Настоящая Памятка предназначена для Клиентов, осуществляющих в Платежной системе переводы денежных средств с использованием системы удаленного доступа «Личный кабинет» и (или) электронных терминалов.

ПАМЯТКА КЛИЕНТАМ

по соблюдению мер информационной безопасности в Платежной системе при использовании системы удаленного доступа «Личный кабинет» и (или) электронных терминалов

1. Общие меры информационной безопасности

1.1. Эксплуатацию системы удаленного доступа «Личный кабинет» следует осуществлять в соответствии с Инструкцией по использованию Интернет-портала ООО «Мультисервисная платежная система». При осуществлении переводов денежных средств с помощью электронных терминалов рекомендуется руководствоваться Инструкцией по использованию электронного терминала VERIFONE VX510.

1.2. В случае обновления документов по эксплуатации (использованию) средств и систем Платежной системы, актуальные версии данных документов публикуются на сайте. Клиент должен осуществлять контроль обновления версий документов по эксплуатации средств и систем Платежной системы и выполнять их положения.

1.3. Для корректной работы с системой удаленного доступа «Личный кабинет» эксплуатация программных, аппаратных, программно-аппаратных средств, в том числе средств защиты информации, включая криптографические, установленных на рабочих станциях пользователей[2], должна также осуществляться в соответствии с требованиями эксплуатационной и технической документации на данные средства.

1.4. Клиент должен незамедлительно информировать свой Банк и (или) оператора платежной системы обо всех выявленных в Платежной системе нарушениях работоспособности средств и систем, для принятия соответствующих мер по их устранению.

2. Меры по защите информации при осуществлении в Платежной системе переводов денежных средств с использованием системы удаленного доступа «Личный кабинет» и (или) платежных терминалов

2.1. Для защиты от несанкционированного доступа к счетам Клиентов рекомендуется ограничить круг пользователей лицами, доступ которых к средствам и системам Платежной системы необходим для выполнения прямых служебных обязанностей, а также осуществлять контроль и регистрацию действий лиц, которые допущены к работе с Платежной системой организационными и (или) техническими мерами.

2.2. Предоставление пользователям доступа к средствам и системам Платежной системы рекомендуется осуществлять только после их информирования о правилах работы в Платежной системе.

2.3. Клиенту рекомендуется минимизировать права пользователей в операционных системах рабочих станций, с которых осуществляется вход в систему удаленного доступа «Личный кабинет», обеспечив штатными средствами операционной системы и (или) дополнительными (наложенными) средствами защиты информации функционально-замкнутую среду для работы – учетные записи пользователей не должны иметь административных привилегий.

---

[2] В настоящей Памятке под Клиентом понимается плательщик (юридическое лицо), осуществляющий в рамках Платежной системы операции по переводу денежных средств. Под пользователем понимается работник Клиента, непосредственно осуществляющий действия по переводу денежных средств с использованием электронного терминала или системы удаленного доступа «Личный кабинет».

2.4. При входе в операционную систему рабочей станции, используемой для осуществления доступа в систему удаленного доступа «Личный кабинет», должны применяться средства идентификации, аутентификации и авторизации, установленные Клиентом и способные предотвратить несанкционированный доступ к содержимому рабочей станции.

2.5. Информация, необходимая для аутентификации пользователя (пароль или ПИН-код) при использовании системы удаленного доступа «Личный кабинет» или электронных терминалов должна использоваться в соответствии со следующими рекомендациями:

- пароль для доступа к системе удаленного доступа «Личный кабинет» должен быть уникальным и отличаться от паролей для доступа к иным информационным ресурсам;
- пароли не должны состоять из легко вычисляемых сочетаний символов, слов на любом языке, общепринятых сокращений, а также из значимых сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- запрещается сообщать пароль/ПИН-код как посторонним, так и знакомым лицам, в том числе по телефону, электронной почте и т.д.;
- запрещается упоминать о содержимом пароля/ПИН-кода;
- запрещается указывать пароль/ПИН-код в анкетах или опросниках;
- запрещается хранить пароль/ПИН-код, в открытом виде на любых носителях информации;
- не рекомендуется осуществлять доступ к системе удаленного доступа «Личный кабинет» с недоверенных рабочих станций, в том числе с рабочих станций, находящихся в общедоступных местах;
- регулярно, но не реже, чем раз в два месяца рекомендуется осуществлять смену пароля;
- запрещается хранить ПИН-код совместно с платежной картой;
- при компрометации пароля/ПИН-кода необходимо незамедлительно предпринять действия по смене пароля или блокировке платежной карты соответственно.

2.6. При увольнении пользователей учетная запись и все реквизиты доступа пользователя к средствам управления счетом посредством системы удаленного доступа «Личный кабинет» или электронных терминалов должны быть заблокированы. Клиент должен незамедлительно предпринять действия по смене действующего пароля/блокировке карты.

2.7. Ввод учетных данных для доступа в систему удаленного доступа «Личный кабинет» должен осуществляться непосредственно уполномоченным на то пользователем.

3. Меры по защите от вредоносного программного обеспечения

3.1. На рабочих станциях, используемых для работы с системой удаленного доступа «Личный кабинет» необходимо обеспечивать постоянную защиту от вредоносного кода, а также контроль запуска программ и устройств, в связи с чем пользователям рекомендуется следующее:

- обеспечить выполнение предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на рабочих станциях, используемых для работы с системой удаленного доступа «Личный кабинет».
- исключить установку на рабочую станцию программного обеспечения, полученного из недоверенных источников, а также нелицензионного и свободно распространяемого программного обеспечения.

- Регулярно и в автоматическом режиме осуществлять обновление баз данных средств антивирусной защиты, установленных на рабочих станциях, используемых для работы с системой удаленного доступа «Личный кабинет».
- При обмене данными с недоверенными сетями передачи данных (включая сеть Интернет) обеспечить полную антивирусную защиту и контроль.
- При работе с электронной почтой крайне не рекомендуется открывать письма и вложения к ним, полученные от неизвестных отправителей, а также переходить по содержащимся в таких письмах ссылкам.
- периодически просматривать журнал событий операционной системы и реагировать на ошибки.
- не давать разрешения неизвестным программам осуществлять выход в сеть Интернет.

3.2. При обмене информацией между вычислительными сетями, в которых располагается рабочая станция, используемая для работы с системой удаленного доступа «Личный кабинет», и сетью Интернет, необходимо обеспечить фильтрацию сетевых пакетов, в том числе с применением средств межсетевого экранирования.

3.3. Во избежание попадания на фишинговые сайты (сайты-двойники) вход в систему удаленного доступа «Личный кабинет» необходимо осуществлять только с официального сайта ООО «Мультисервисная платежная система»: http://www.payhd.ru/, либо по прямой ссылке https://lk.payhd.ru:8008/ib/. Не рекомендуется входить в систему удаленного доступа «Личный кабинет» по ссылкам, размещенным во входящей корреспонденции или в источниках в сети Интернет. Адрес официального сайта рекомендуется набирать вручную.

3.4. При завершении работы с системой удаленного доступа «Личный кабинет» пользователь должен завершить сеанс работы посредством нажатия на кнопку «Выход» и только после этого закрыть Интернет-браузер.

4. Меры по защите ключевой информации

4.1. Средства электронной подписи (далее – ЭП), используемые для подтверждения операций по переводу денежных средств в Платежной системе с использованием системы удаленного доступа «Личный кабинет», следует использовать в соответствии с технической и эксплуатационной документацией на них. На Клиента возлагается обязанность по осуществлению контроля за соблюдением условий использования ЭП пользователями.

4.2. Клиенту рекомендуется проводить обучение пользователей ЭП правилам работы с ними.

4.3. В случае выявления фактов нарушения правил использования ЭП, в том числе фактов утраты или недостачи носителей ключевой информации и других фактов, которые могут привести к разглашению защищаемой информации или к иным несанкционированном действиям, Клиенту необходимо незамедлительно провести разбирательство по данным фактам.

4.4. Рабочую станцию с подключенными носителями ключевой информации рекомендуется использовать в однопользовательском режиме.

4.5. Носители ключевой информации должны храниться в специально отведенных для этого местах.

4.6. Нельзя оставлять носители ключевой информации подключенными к рабочей станции после подписания платежных документов. Носители ключевой информации должны подключаться к рабочей станции только в момент подписания документов.

4.7. В целях предотвращения утери и (или) компрометации ключевой информации Клиенту рекомендуется обеспечивать поэкземплярный учет носителей ключевой информации, а также эксплуатационной и технической документации к ней.
4.8. Криптографические ключи, срок действия которых истек, выводятся из пользования и подлежат уничтожению способом, исключающим возможность восстановления содержащейся на них информации.
4.9. Пользователям криптографических ключей и ключевой информации запрещается:

- осуществлять несанкционированное копирование криптографических ключей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным;
- нарушать требования, предусмотренные эксплуатационной и технической документацией на ЭП;
- вносить какие-либо изменения в программное обеспечение ЭП.

4.10. При компрометации криптографического ключа Клиент обязан прекратить обмен электронными документами с его использованием, а также принять меры по его изъятию из обращения и замене на новый.
4.11. В случае прекращения использования ЭП (увольнение, смена обязанностей и т.п.) пользователи должны сдавать носители ключевой информации, эксплуатационную и техническую документацию к ЭП в соответствии с внутренним порядком.
4.12. При смене, увольнении лица, имеющего, даже потенциально, доступ к ключевому носителю (например, системного администратора) рекомендуется незамедлительно произвести смену криптографического ключа.

5. Меры по предотвращению несанкционированных списаний денежных средств

5.1. Клиент обязан предпринимать все возможные меры для предотвращения утраты (хищения) карты, ПИН-кода, логина, пароля, ключа ЭП или их незаконного использования.
5.2. Для отслеживания и контроля несанкционированных списаний пользователям рекомендуется регулярно осуществлять проверку входящих электронных документов, в том числе уведомлений о совершенных переводах денежных средств.
5.3. Пользователям следует регулярно контролировать состояние своих счетов и незамедлительно информировать Банк обо всех подозрительных или несанкционированных операциях (списаниях) в соответствии с положениями Договора.
5.4. В случае неожиданного выхода из строя рабочей станции, с использованием которой осуществлялся вход в систему удаленного доступа «Личный кабинет» рекомендуется прекратить работу с данной рабочей станцией, отключив ее от всех видов сетей, включая локальную корпоративную сеть, модемов и т.п., обесточить ее и срочно проверить счет, обратившись в службу клиентской поддержки ООО «Мультисервисная платежная система» по телефону: 8 800 550-10-20.
5.5. В случае обнаружения несанкционированных операций по счету, Клиенту необходимо написать заявление по факту таких действий в Банк с указанием даты, суммы платежа и других известных Клиенту обстоятельств.

6. Меры по поддержанию уровня информационной безопасности

6.1. Оператор платежной системы и Банк применяют все необходимые меры для обеспечения высокого уровня информационной безопасности в Платежной системе, однако для полного обеспечения и поддержания необходимого уровня информационной безопасности Клиенту крайне выполнять все предписанные требования и рекомендации, в том числе:

- Информировать пользователей системы удаленного доступа «Личный кабинет» о порядке использования средств электронной подписи и применения организационных мер защиты информации в Платежной системе.
- Осуществлять повышение осведомленности пользователей правилам работы и требованиям к защите информации в Платежной системе путем проведения инструктажей, обучения и т.д..
- Обеспечивать постоянный контроль соблюдения пользователями мер информационной безопасности, предусмотренных настоящей памяткой, а также документами по эксплуатации средств и систем Платежной системы.
- Незамедлительно обращаться в Банк при выявлении нарушений в Платежной системе, а также обеспечивать устранение и (или) контроль устранения выявленных нарушений.
- Проводить внутренние проверки соблюдения указанных в Памятке требований.
- Самостоятельно принимать меры, направленные на поддержание уровня информационной безопасности при выявлении недостатков в обеспечении защиты информации в ходе внутренних проверок.

6.2. Меры, направленные на поддержание уровня информационной безопасности, могут носить организационный и технический характер.

6.3. Для обеспечения надлежащего уровня информационной безопасности при эксплуатации средств и систем Платежной системы, а также для исполнения требований/рекомендаций, указанных в п.п. 6.1-6.7 настоящего раздела, Клиенту рекомендуется назначить лицо, ответственное за организацию и контроль обеспечения защиты информации и возложить на него соответствующие задачи (обязанности).