ООО МКК «Выручай-Деньги»

ПРИКАЗ

«31» мая 2019 г. № 31-ПР

О размещении памятки на официальном сайте ООО МКК «Выручай-Деньги»

Во исполнении Положения Банка России от 17 апреля 2019 г. № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

ПРИКАЗЫВАЮ:

1.Администратору информационной безопасности выполнить работы по размещению на официальном сайте ООО МКК «Выручай-Деньги» памятку, содержащую информацию:

- о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода согласно Приложению 1.

2. Приказ вступает в силу с момента его подписания.

3.Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор Гажу Андриан

Приложение № 1 к приказу №31-ПД от 31.05.2019

ПАМЯТКА ДЛЯ КЛИЕНТОВ ООО МКК «ВЫРУЧАЙ-ДЕНЬГИ»

Выдача займов заемщику производится путем безналичного перечисления на расчетный счет заемщика, указанного в договоре займа. ООО МКК «Выручай-Деньги» информирует своих клиентов о том, что не имеет собственных платежных систем, через которые возможно производить погашение задолженности по займу.

Однако, многие из заемщиков пользуются онлайн-банком и могут быть подвергнуты угрозе получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Для обеспечения информирования о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления:

1. Не сообщайте посторонним лицам персональные данные или информацию о банковской карте или банковском счете через сеть Интернет, логины и пароли доступа к ресурсам Банка, историю операций, так как эти данные могут быть перехвачены Злоумышленниками и использованы для получения доступа к Вашим счетам.

2. Не записывайте логин и пароль на бумаге, не размещайте их на мониторе или клавиатуре вашего рабочего места или домашнего ПК.

3. Не используйте функцию запоминания логина и пароля в браузерах.

4. Не используйте одинаковые логин и пароль для доступа к различным системам.

5. Не пользуйтесь системами, требующими ввода логина и пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых Вы сомневаетесь.

6. Совершайте операции только со своего личного Средства доступа в целях сохранения конфиденциальности персональных данных и (или) информации о банковском счете.

6. Всегда завершайте сеанс работы с Системой, используя пункт меню «Выход».

7. В случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web-страницу). После возвращения к своему Средству доступа обязательно смените логин и пароль.

8. Если Вы получили на электронную почту письмо с просьбой обновить или подтвердить персональную и любую другую конфиденциальную информацию со ссылкой на какой-либо сайт (в том числе – сайт Банка), помните, что Банк никогда не просит передать данные по электронной почте.

9. Не открывайте приложения к письмам от незнакомых отправителей, так как они могут содержать вредоносное программное обеспечение, способное произвести кражу Ваших идентификационных данных для входа в Систему.

10. При регистрации на сторонних интернет-сайтах всегда изменяйте пароли, которые приходят Вам по электронной почте. Помните, что Банк никогда не направляет пароли по электронной почте.

11. Не реже одного раза в месяц, производите смену пароля.

12. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] < >. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

13. При использовании ЭП не позволяйте третьим лицам производить за Вас генерацию ключей.

14. При использовании ЭП присоединяйте ключевой носитель ЭП к компьютеру непосредственно перед началом работы с Системой. По окончании работы извлекайте ключевой носитель из компьютера.

15. Используйте лицензированное программное обеспечение.

16. Регулярно (не реже раза в неделю) проводите проверку на наличие новых версий программного обеспечения и обновляйте антивирусные базы. В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль в Системе.

17. Не запускайте на своем компьютере программы, полученные из незаслуживающих доверия источников.

18. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

19. Не храните незашифрованные личные данные на жестком диске, так как эти данные могут быть похищены Злоумышленниками и использованы для получения доступа к Вашим счетам.

20. Перед вводом своего логина и пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности, и информацию о Вашем последнем доступе в Систему.

21. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших счетах, необходимо подать заявление на временное отключение от Системы, подать заявление о преступлении в правоохранительные органы и прекратить использование (обесточить) персональный компьютер в целях сохранения доказательной базы. Если Вы пользуетесь аналогичными Системами других банков – заблокируйте их до выяснения обстоятельств происшествия. Эти учетные записи также могут оказаться скомпрометированными.

Еще раз напоминаем, что ООО МКК «Выручай-Деньги» не имеет собственных платежных систем, позволяющих осуществлять погашение займов.

Сотрудники ООО МКК «Выручай-Деньги» никогда не запрашивают пароли от входа в ваш онлайн-банк.

С информацией ***о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода*** ознакомьтесь на сайте онлайн-банка в котором производите денежные операции.