241035, Брянская обл., г. Брянск, ул. Бурова, д. 20, помещение I, офис 204

ООО МКК «Выручай-Деньги», ОГРН 1113256019469, ИНН 3255517143

# ПРИКАЗ № 01/01_D/2023/26_17

г. Брянск «16» октября 2023 г.

**«О размещении памятки для клиентов, о мерах по обеспечению информационной безопасности на официальном сайте ООО МКК «Выручай-Деньги»**

Во исполнении Положения Банка России от 20 апреля 2021 г. № 757-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. Приказ № 31-ПД от 31 мая 2019 г. считать утратившим силу.
2. Отделу маркетинга выполнить работу по размещению на официальном сайте ООО МКК «Выручай-Деньги» памятку для клиентов, о мерах по обеспечению информационной безопасности (Приложение №1).
5. Настоящий приказ вступает в силу с момента его подписания.
6. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор
ООО МКК «Выручай-Деньги» /Е.И. Шилинцева/

Приложение №1
УТВЕРЖДЕНО
приказом ООО МКК «Выручай-Деньги»
от «16» октября 2023 г. № 01/01_D/2023/26_17

**Памятка для клиентов**

**О мерах по обеспечению информационной безопасности**

**Уважаемые Клиенты!**

Выдача займов заемщику производится путем безналичного перечисления денежных средств 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.

Многие из заемщиков используют онлайн-доступ к своим банковским счетам (Интернет - банкинг) и могут быть подвергнуты угрозе несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

**Рекомендации по обеспечению информационной безопасности**:

1. Не сообщайте посторонним лицам персональные данные или информацию о банковской карте или банковском счете, логины и пароли доступа к системе дистанционного банковского обслуживания, историю операций по счетам, так как эти данные могут быть перехвачены злоумышленниками и использованы для получения доступа к Вашим счетам.
2. Не записывайте пароли там, где доступ к ним могут получить третьи лица.
3. Не используйте функцию запоминания логина и пароля в браузерах.
4. Не используйте одинаковые логин и пароль для доступа к различным системам.
5. Рекомендуется избегать работы в интернет-банке с «недоверенных» компьютеров (в Интернет-кафе или другие общедоступные компьютеры, а также «чужие» компьютеры, временно используемые вами и т.п.). Крайне нежелательно использование для работы в интернет-банке публичных беспроводных сетей (например, бесплатный Wi-Fi и т.п.).
6. Совершайте операции только со своего личного средства доступа в сеть интернет в целях сохранения конфиденциальности персональных данных и (или) информации о банковском счете.
7. Всегда завершайте сеанс работы с системой, используя пункт меню «Выход».
8. 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. После возвращения к своему личному средству доступа в сеть интернет обязательно смените пароль.
9. Если Вы получили на электронную почту письмо с просьбой обновить или подтвердить персональную и любую другую конфиденциальную информацию со ссылкой на какой-либо веб-сайт (в том числе – веб-сайт Банка), помните, что Банки никогда не просит клиентов передать данные по электронной почте (по незащищенным каналам связи).
10. Не открывайте приложения к письмам от незнакомых отправителей, так как они могут содержать вредоносное программное обеспечение, способное вызвать несанкционированный доступ к данным, блокировку данных и т.д.
11. При регистрации на интернет-сайтах всегда изменяйте пароли, которые приходят Вам по электронной почте. Помните, что Банк никогда не направляет пароли по электронной почте.

12. Во избежание раскрытия паролей входа в системы третьим лицам, рекомендуем изменять пароли один раз в три месяца.

13. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные специальные символы, например: ! / { } [ ] < > @. Не используйте в качестве пароля имена, памятные даты, номера телефонов. Рекомендуем составлять пароль не менее 12 символов.

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

15. При использовании ЭП подключайте ключевой носитель к компьютеру только на время подписи документов, ни в коем случае не храните ключи на жестком диске компьютера.

16. Используйте лицензированное программное обеспечение.

17. Регулярно проводите проверку на наличие новых версий программного обеспечения.

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

19. Рекомендуем постоянное использование системы антивирусного программного обеспечения на вашем компьютере. Необходимо использовать лицензионные программные продукты последних версий и постоянно обновлять антивирусные базы данных программных продуктов. Обновление антивирусных баз рекомендуется проводить в автоматическом режиме по мере их выпуска организацией-разработчиком.

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

21. Перед вводом своего логина и пароля убедитесь, что вы установили соединение с легальным веб-сайтом. Проверьте правильность адреса веб-сайта, наличие сертификата безопасности, и информацию о Вашем последнем доступе в систему.

22. 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, при оплате через Личный кабинет, Заемщику предоставляется возможность оплаты в адрес ООО МКК "Выручай-Деньги" через нашего партнера Банк СНГБ, с использованием Сервиса «Best2Pay»**. Подробно с Правилами наших партнеров по приему платежей можно ознакомиться на сайте https://www.sngb.ru , https://www.best2pay.net **позволяющих осуществлять погашение займов позволяющих осуществлять погашение займов.**

**Сотрудники ООО МКК «Выручай-Деньги» никогда не запрашивают пароли от личного кабинета 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.