РЕКОМЕНДАЦИИ КЛИЕНТАМ ООО МФК «ВЭББАНКИР»
по соблюдению мер информационной безопасности
в целях противодействия незаконным финансовым операциям

1. Общие положения

1.1. Настоящие рекомендации разработаны Обществом с ограниченной ответственностью микрофинансовая компания «ВЭББАНКИР» (далее – Компания) в соответствии с требованиями Положения 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 (утв. Банком России 17.04. 2019 г. № 684-П).
Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, как на стороне Компании, так и на стороне её клиентов.

1.2. Возможные риски получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом на их осуществление, могут возникать путем реализации вирусных атак, таких как:
- «ФИШИНГ» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице злоумышленники предлагают потенциальной жертве ввести свои персональные данные, при этом потенциальная жертва может полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.
- «ПРЕТЕКСТИНГ» (англ. pretexting) — атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию вынуждает выдать конфиденциальную информацию. Эта атака подразумевает должную подготовку, наличие информации: день рождения, ИНН, номер паспорта либо последние цифры счета для того, чтобы не вызвать подозрений у жертвы. Обычно реализуется через телефон или электронную почту.
- «СМИШИНГ», « SMS -ФИШИНГ» (от «SMS» и «фишинг»). Рассылка SMS сообщений, содержащих ссылки на фишинговый сайт, входя на который и вводя свои персональные данные, жертва передаёт их злоумышленникам.
- «ТРОЯНСКИЙ КОНЬ» – вид вредоносного программного обеспечения, проникающего на устройство жертвы под видом легальных программ. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации банковских карт и её передачу злоумышленнику, её использование, удаление или злонамеренное изменение.

2. Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники в целях противодействия незаконным финансовым операциям.

2.1. Антивирусная защита осуществляется с целью исключения возможностей появления на устройствах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе паролей.
2.2. Рекомендуется установить и своевременно обновлять на устройстве антивирусное программное обеспечение, и установить в таком программном обеспечении по умолчанию максимальный уровень политики безопасности.
2.3. Не реже одного раза в неделю в автоматическом режиме рекомендуется осуществлять полную проверку устройства на предмет наличия вирусов и вредоносного программного кода.
2.4. Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы.
2.5. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам связи, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т.п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.
2.6. При подозрениях на наличие вирусов на устройстве (в частности, неожиданных «зависаниях», перезагрузках, повышенной сетевой активности), рекомендуется полностью воздержаться от использования систем денежных переводов и Личного кабинета заемщика на официальном сайте Компании в информационно-телекоммуникационной сети «Интернет» по адресу: https://glavpotrebcredit.ru (далее – Личный кабинет), до исправления ситуации.
2.7. Компания не несет ответственности в случае возникновения финансовых потерь, понесенных Клиентом в связи

с нарушением и/или ненадлежащим исполнением им требований по защите от вредоносного кода своих устройств для доступа к Личному кабинету.

3. Меры по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потери, хищении) устройства, с использованием которого совершались действия в целях осуществления финансовых операций, контролю конфигурации устройств и своевременному обнаружению воздействий вредоносного кода.

3.1. Рекомендуется использовать на устройствах только лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), и обеспечить регулярную своевременную установку обновлений операционной системы.

3.2. Рекомендуется своевременно обновлять установленное программное обеспечение и операционную систему (установка критичных обновлений), web-браузеры и иное прикладное программное обеспечение.

3.3. Не рекомендуется использовать средства удаленного администрирования на устройстве, предназначенного для доступа к Личному кабинету.

3.4. При работе в информационно-телекоммуникационной сети «Интернет» не рекомендуется устанавливать какие-либо сомнительных программы.

3.5. Рекомендуется ограничить информационный обмен в информационно-телекоммуникационной сети «Интернет» только надежными информационными порталами и проверенными корреспондентами электронной почты. Различные развлекательные сайты, сайты сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), могут послужить источником распространения вирусов.

3.6. Зачастую жертвам злоумышленников поступает вредоносная программа в виде «интересной ссылки» в письме от якобы знакомого. Вредоносная программа может скрываться под всплывающим окном рекламной ссылки на web-сайте.

3.7. При работе с электронной почтой не рекомендуется открывать письма и вложения к ним, полученные от неизвестных отправителей, и не переходить по содержащимся в таких письмах ссылкам.

3.8. Перед просмотром электронного письма необходимо всегда проверять адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса Компании.

3.9. Рекомендуется внимательно читать текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. В случае наличия в таких электронных письмах слов на иностранном языке, специальных символов и т.д., возможно, это – электронное письмо, отправленное мошенниками.

3.10. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить потенциальную жертву действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить потенциальную жертву в том, что её счету угрожает опасность, если потенциальная жертва немедленно не обновит критически важные данные.

3.11. Еще один вид мошенничества связан с созданием фальсифицированных web-сайтов – их доменные имена и стили оформления могут имитировать сайты Компании и содержать ложные реквизиты и контактную информацию. Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, т.е. разглашению персональных данных клиента.

Необходимо помнить, что сайты, визуально напоминающие сайт с Личным кабинетом, создаются специально для незаконного получения информации. В случае обнаружения фальсифицированного сайта, копирующего дизайн официального сайта Компании или Личного кабинета, клиенту необходимо незамедлительно сообщить об этом Компании по всем возможным контактам, указанным на официальном сайте Компании в сети «Интернет» по адресу: https://glavpotrebcredit.ru.

Во избежание использования таких ресурсов необходимо удостовериться, что при подключении к Личному кабинету защищённое соединение было установлено исключительно с официальным сайтом Компании. Прежде чем ввести логин и пароль, необходимо проверить по информации из SSL-сертификата подлинность сайта.

3.12. Рекомендуется внимательно анализировать ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить потенциальную жертву злоумышленников на мошеннический web-сайт. Если ссылка выглядит подозрительно (ссылка с ошибками или заменой сходных по начертанию символов) или не соответствует требованиям безопасности (например, начинается с **http://** вместо **https://**), не рекомендуется переходить по этой ссылке.

3.13. Используемые в Личном кабинете логин и пароль, запрещается записывать и хранить в местах, доступных посторонним лицам. Пароль необходимо хранить в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых вводятся конфиденциальные данные.

3.14. В том случае, если клиент Компании обнаружил, что его пароль от Личного кабинета скомпрометирован, рекомендуется незамедлительно уведомить об этом Компанию и сменить пароль на новый.

3.15. Если в процессе работы клиент Компании столкнулся с тем, что ранее действующий пароль от его Личного кабинета не принимается информационной системой Компании, необходимо уведомить Компанию и как можно быстрее воспользоваться формой восстановления пароля.

3.16. Компания не рассылает электронных писем, SMS или других сообщений с просьбой уточнить

конфиденциальные данные клиентов (в т.ч. пароли, SMS-коды и т.п.).
3.17. Не рекомендуется пересылать файлы с конфиденциальной информацией для работы в Личном кабинете по открытым каналам связи, по электронной почте или через SMS-сообщения.
3.18. В том случае, если клиент Компании получил уведомление системы об операции, которую клиент не проводил - рекомендуется незамедлительно обратиться в Компанию.
3.19. Для безопасной работы в Личном кабинете на устройствах рекомендуется применять средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п., обеспечить регулярное автоматическое обновление программного обеспечения этих средств.
3.20. Не рекомендуется работать с Личным кабинетом на устройствах общего пользования («Интернет-кафе», вокзалы, аэропорты, библиотеки и т.п.). Работа с гостевых рабочих мест увеличивает риск неправомерного использования аутентификационной информации.
3.21. При работе с Личным кабинетом на устройствах рекомендуется использовать парольную защиту (PIN-код, графический ключ, разблокировка по отпечатку пальца, «FaceID» и пр.).
3.22. По завершении работы в Личном кабинете необходимо корректно произвести выход, используя для этого соответствующий пункт меню.
3.24. При потере(хищении) устройства, с использованием которого совершались действия в целях осуществления финансовых операций, необходимо в кратчайший срок обратиться к оператору сотовой связи и заблокировать SIM-карту.
3.25. При смене номера телефона, который зарегистрирован в информационной системе Компании необходимо указать эту информацию в Личном кабинете, либо сообщить об этом Компании посредством использования телефонной связи через оператора Компании.
Операторы сотовой связи могут передать номер телефона другому абоненту, если он будет неактивным длительное время.
3.26. Не рекомендуется оставлять свое устройство без присмотра, чтобы исключить несанкционированное использование финансовых услуг.
3.27. Не рекомендуется входить в Личный кабинет с устройств, которые не принадлежат клиенту, по просьбе третьих лиц, даже если к клиенту обратились от имени сотрудников Компании.
3.28. При установке на телефон дополнительных программ необходимо обращать внимание на полномочия, которые им необходимы. Необходимо обращать внимание на такие опасные разрешения: доступ и отправка SMS, доступ к «Интернет».
3.29. При внезапном прекращении работы SIM-карты необходимо обратиться к оператору сотовой связи за уточнением причин — возможно, проведение мошеннических действий третьими лицами.
3.30. Не рекомендуется устанавливать на устройство стороннее системное ПО, устанавливать на устройстве «root» доступ, так как это отключает защитные механизмы, заложенные производителем устройства. В результате устройство становится уязвимым к заражению вирусным ПО.
3.31. Загружать и устанавливать ПО Личного кабинета следует только с официальных сайтов – Google Play или Apple AppStore. Ссылки для загрузки размещены на официальном сайте Компании. Приложения Компании для разных платформ соответствуют требованиям безопасности и периодически обновляются.
3.32. Средства и методы защиты информации, применяемые в Компании, позволяют обеспечить необходимый уровень безопасности при работе в Личном кабинете и предотвратить мошеннические действия в отношении клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.