ПАМЯТКА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ
ПРИ РАБОТЕ В СИСТЕМЕ ДБО И СЕТИ ИНТЕРНЕТ

1. БАНК СЧИТАЕТ КРИТИЧЕСКИ ВАЖНЫМ ВЫПОЛНЕНИЕ КЛИЕНТАМИ СЛЕДУЮЩИХ ОСНОВНЫХ ТРЕБОВАНИЙ:

1.1. обеспечивать безопасность Ключевой информации;

1.2. соблюдать общие правила безопасного использования Системы ДБО;

1.3. использовать и оперативно обновлять лицензионное системное и прикладное программное обеспечение (ПО) только из доверенных источников, гарантирующих отсутствие вредоносных программ;

1.4. использовать и оперативно обновлять специализированное ПО для защиты информации – антивирусное ПО;

1.5. соблюдать правила безопасной работы в сети Интернет.

1.1. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КЛЮЧЕВОЙ ИНФОРМАЦИИ.

Владелец Ключевой информации должен хранить ее в условиях, исключающих доступ к ней третьих лиц, включая работников Банка и своих родственников.

Запрещается хранить Ключевую информацию на жестком диске компьютера, в памяти иного устройства, с использованием которого осуществляется выход в сеть «Интернет», а также иным способом, делающим данную информацию доступной для третьих лиц.

В случае потери Ключевой информации, необходимо немедленно сообщить об этом в Банк в соответствии с Договором ДБО. Только после этого доступ к Системе ДБО будет заблокирован и злоумышленник не сможет воспользоваться вашим Счетом в Банке!

Необходимо производить смену Ключевой информации не реже 1 (Одного) раза в два месяца или при возникновении подозрений о ее компрометации.

В случае утери телефона, номер которого зарегистрирован в Банке в качестве Номера телефона ДБО, необходимо немедленно сообщить об этом в Банк в соответствии с Договором ДБО. Только после этого доступ к Системе ДБО будет заблокирован и злоумышленник не сможет воспользоваться вашим Счетом в Банке!

Рекомендуется не использовать для получения Кодов подтверждения смартфоны или мобильные телефоны с возможностью установки программного обеспечения. Рекомендуется использовать простые мобильные телефоны с минимальными функциями.

1.2. СОБЛЮДЕНИЕ ОБЩИХ ПРАВИЛ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ДБО.

Не осуществлять вход в Систему ДБО и проведение Операций с использованием чужого персонального устройства (компьютер, смартфон, планшет, в том числе устройства, расположенного в общедоступных местах (интернет-кафе, киоски и т.д.)).

Не осуществлять вход в Систему ДБО и проведение операций в Системе ДБО с использованием недоверенных (публичных) беспроводных сетей.

До входа в Систему ДБО удостоверяться в том, что устройство (компьютер, смартфон, планшет, коммуникатор, телефон), с использованием которого осуществляется работа в Системе ДБО, не заражено вирусами, на нем установлено (не отключено) и настроено антивирусное программное обеспечение, регулярно обновляются антивирусные базы.

Использовать для доступа в Систему ДБО оригинальную учетную запись и Пароль.

Не оставлять устройство (компьютер, смартфон, планшет с активной Системой ДБО) без присмотра.

При каждом сеансе работы с Системой ДБО, проверить подлинность соединения, для чего убедиться, что:

- включен защищенный режим SSL, то есть в адресной строке браузера Web-адрес начинается с символов «https://» и в окне Web-браузера отражается символ «закрытый замок»;
- соединение установлено именно с сервером ООО «банк Раунд», то есть в адресной строке интернет-страницы указан точный адрес: https://dbo.round.ru (не допускается никаких отличий в написании Web-адреса, вплоть до любого знака);
- в сертификате сайта в строке «Кому выдан» указано точное значение «*.round.ru»;
- в сертификате сайта в строке «Кем выдан» указано точное значение «Local NetFlt CA 2».

Для всех учетных записей в операционной системе должны использоваться пароли, удовлетворяющие следующим требованиям: длина пароля не менее 6 символов; в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

При обнаружении признаков вредоносных программ при подключении к Системе ДБО, а также в случае получения сообщения из Банка Клиент должен срочно провести очистку компьютера от вредоносных программ посредством антивирусного ПО.

1.3. ИСПОЛЬЗОВАНИЕ И ОБНОВЛЕНИЕ СИСТЕМНОГО И ПРИКЛАДНОГО ПО.

Необходимо использовать только лицензионное программное обеспечение, регулярно обновлять операционную систему и прикладное программное обеспечение (браузер, программы для работы с документами и т.д.).

Установка и обновление системного и прикладного ПО (операционная система, браузеры, почтовые клиенты, офисные программы, бухгалтерские программы и пр.) на устройства (компьютер, смартфон, планшет) из ненадежных источников может привести к Компрометации ключевой информации и как следствие к незаконному списанию денежных средств.

Клиент должен использовать ПО только из надежных доверенных источников.

Если это коммерческое ПО, оно должно быть легально приобретено Клиентом и установлено с легального дистрибутива, гарантирующего отсутствие вредоносных программ. Если это свободно распространяемые программы, они должны быть получены из доверенного источника или загружены через Интернет с публичных сайтов разработчиков с использованием механизмов обеспечения целостности загружаемого ПО.

Необходимо строго придерживаться рекомендаций разработчиков о периодичности проверки появления новых версий и установки обновлений. Оперативное обновление системного и прикладного ПО на устройства (компьютер, смартфон, планшет) Клиента – это необходимое условие для снижения рисков заражения вредоносными программами, через новые выявленные уязвимости и ошибки в используемых клиентом программах.

1.4. ИСПОЛЬЗОВАНИЕ И ОБНОВЛЕНИЕ ПО ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ.

Для защиты от вредоносных программ Клиент должен использовать и оперативно обновлять на своих устройствах (компьютер, смартфон, планшет) Антивирусное ПО;

В настоящее время пользователям доступно достаточное количество специализированных программных средств защиты информации – как коммерческих, так и свободно распространяемых.

1.5. СОБЛЮДЕНИЕ ПРАВИЛ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ.

При использовании устройства (компьютер, смартфон, планшет) для работы в Системе ДБО, мы рекомендуем Клиентам неукоснительное соблюдение следующих правил безопасности:

Никогда не открывать сайт Системы ДБО по ссылкам (особенно баннерным или полученным через почту), поскольку существует множество способов фальсифицировать адрес. Необходимо всегда самостоятельно вводить в Web-браузере адрес Системы ДБО Банка.

Не отвечать на подозрительные письма с просьбой выслать Ключевую информацию. Подобное письмо, возможно, создано злоумышленниками. Никакой банк не позволяет себе запрашивать у клиентов конфиденциальную информацию по электронной почте.

Обращать особое внимание на отправителя почтовой корреспонденции при работе с электронной почтой, вне зависимости от того, выполняется работа с почтой через Web- интерфейс одной из известных почтовых систем mail.ru, yandex.ru и т.п., или в локально установленных программах типа Outlook, Outlook Express, The Bat! Не открывать вложение письма, что бы ни содержало данное сообщение, если отправитель почтового сообщения вам неизвестен.

Обращаем внимание: никакие обновления, патчи, апдейты для устройства (компьютер, смартфон, планшет) не распространяются по почте. При переписке со всеми адресатами необходимо помнить, что даже в письме известного Клиенту отправителя, в том числе отправителя, с которым ведется длительная переписка, может находится вредоносное вложение. Открывать вложения, полученные по электронной почте, необходимо только после предварительного сохранения их в специальной папке на жестком диске и проверки их на наличие вредоносных программ (антивирусной проверки).

Задать максимальный уровень безопасности Web-браузера по умолчанию (запрет языка Java, запрет сценариев, запрет загрузки элементов ActiveX) для снижения вероятности использования злоумышленником уязвимостей в Web-браузерах. Большинство случаев современных атак связаны с использованием данных уязвимостей, поскольку они обнаруживаются во всех Web-браузерах – Microsoft Internet Explorer, Firefox, Mozilla, Opera, Safari и т. п. Для тех сайтов, которые требуют разрешения исполнения соответствующих элементов необходимо индивидуально разрешить их исполнение, добавив сайты в список надежных.

При использовании служб мгновенного обмена сообщениями – WhatsApp, Viber, Telegram и т.д. необходимо соблюдать рекомендации аналогично работе с почтовыми клиентами – не принимать файлы из неизвестных источников, к файлам из известных источников относиться с осторожностью. Проверять все полученные файлы антивирусными программами.

Не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных Web-сайтов, присланные по электронной почте, полученные в телеконференциях. Такие файлы лучше немедленно удалять, а в случае необходимости загрузки такого файла следует убедиться, что он проверен антивирусом.

Не допускать использования устройства (компьютер, смартфон, планшет) для посещения сайтов сомнительного содержания (сайты эротической направленности, сайты бесплатных программ, хакерские сайты и т.п.). Зачастую такие сайты содержат вредоносные программы, загружаемые и запускаемые при входе на сайт.