Уважаемые клиенты!

Обращаем Ваше внимание на участившиеся случаи размещения в социальных сетях и иных информационных каналах мошеннических объявлений от имени банков Республики Беларусь. Наиболее распространенными методами реализации мошеннических операций со стороны злоумышленников являются:

- выманивание реквизитов банковских платежных карт с использованием взломанных аккаунтов в социальных сетях либо просьбы совершить определенные действия по переводу денежных средств;

- фишинг – вид мошенничества (часто с использованием электронных писем, текстовых сообщений или телефонных звонков), в ходе которого злоумышленник обманом вынуждает жертву раскрыть учетные данные, банковские реквизиты или другую персональную информацию, а затем использует их в преступных целях;

- метод с использованием смартфона – злоумышленник под предлогом совершения звонка незаметно устанавливает приложение, позволяющее получить доступ для совершения операций в системе с использованием электронных денег;

- распространение по электронной почте или мессенджеров под видом белорусских компаний ложной информации о проводимых акциях, опросах, распродажах и т.п. с целью введения в заблуждение граждан Республики Беларусь и завладения их денежными средствами.

Для проведения мошеннических операций, как правило используются методы социальной инженерии (психологическое манипулирование людьми с целью совершения ими определенных действий или разглашения конфиденциальной информации).

Для защиты себя и своей организации от мошеннических операций, следуйте следующим рекомендациям:

1. Не открывайте подозрительные файлы и не переходите по ссылкам в электронных письмах, полученных от неизвестных адресатов. ОАО «Банк развития Республики Беларусь» для обмена конфиденциальной информацией предварительно согласовывает с клиентами адреса электронной почты, используемые для переписки.
2. Не предоставляйте сведения, относящиеся к коммерческой тайне организации, персональным данным, банковскую тайну с использованием мессенджеров или адресов электронной почты, которые не были предварительно согласованы с банком для обмена информацией. ОАО «Банк развития Республики Беларусь» использует для переписки с клиентами корпоративный почтовый сервер, содержащий в адресе маску домена \*@brrb.by.
3. Не предоставляйте реквизитов доступа и иной информации, необходимой для доступа и совершения действий в системе дистанционного банковского обслуживания (далее – Cистема ДБО), в т.ч. друзьям, знакомым, родственникам, работникам ОАО «Банк развития Республики Беларусь». При обращении с указанными просьбами – просим информировать ОАО «Банк развития Республики Беларусь» по электронной почте на адрес: [sdbo@brrb.by](mailto:sdbo@brrb.by).
4. При использовании архивов с парольной защитой, работники ОАО «Банк развития Республики Беларусь» направляют пароль доступа к файлам по другим каналам передачи информации.
5. При переходе на страницы Интернет-сайтов банков, в особенности при использовании Систем ДБО или интернет-банкинга, проверяйте в адресной строке браузера наличие действующего сертификата организации, услугами которой планируете воспользоваться. Проверяйте правильность набора (копирования) ссылок (URL), по которым осуществляется переход на веб-страницы для проведения банковских операций. Используйте для проведения указанных операций двухфакторную аутентификацию (для онлайн-операций подключите услугу 3-D Secure).

ОАО «Банк развития Республики Беларусь» имеет один действующий официальный Интернет-сайт, размещаемый в сети Интернет по адресу: <https://brrb.by>.

При работе в Системе ДБО ОАО «Банк развития Республики Беларусь» убедитесь, что защищенное соединение установлено именно с официальным сайтом указанной системы <https://sdbo.brrb.by/>, настоятельно не рекомендуется переходить на данную страницу по ссылкам с Интернет-ресурсов (за исключением официальных ресурсов Банка, например, <https://brrb.by/>). Первоначальная страница доступа в личный кабинет Системы ДБО должна содержать только поля ввода логина и пароля.

1. Избегайте отправки конфиденциальной информации или осуществления финансовых операций через общественные Wi-Fi сети, так как они могут быть небезопасными и подвержены перехвату данных.

7. Не предоставляйте удаленный доступ к своему компьютеру для оказания технической поддержки или настройки операционной системы и/или доступа к платежным сервисам (сайтам), настройкам средств для работы с электронной цифровой подписью.