Уважаемый клиент, обращаем Ваше внимание, что в последнее время существенно увеличилось количество мошеннических действий в отношении держателей платежных карт и пользователей систем дистанционного банковского обслуживания. Злоумышленниками активно применяются методы социальной инженерии, направленные на получение конфиденциальной информации и побуждении клиентов к совершению операций в их пользу. Широко используется вредоносное программное обеспечение, действие которого направлено для достижения тех же целей — хищение/несанкционированное копирование логинов, паролей доступа к системам дистанционного банковского обслуживания и иной конфиденциальной информации.

Основные риски получения несанкционированного доступа к устройствам клиента:

- риск совершения финансовых операций с Вашими активами, в том числе путем формирования и отправки от Вашего имени распоряжения на проведение финансовой операции, а также риск перехвата сообщений, отправляемых Банком на Ваш адрес электронной почты и/или абонентский номер, содержащих защищаемую информацию;
- риск совершения иных юридически значимых действий, в том числе включение и отключение услуг (включая платные услуги), внесение изменений в Ваши регистрационные данные, использование счетов и находящихся на них активов, прикрытие иных действий, носящих противоправный характер;
- риск повреждения Вашего программного обеспечения, а также риск искажения, изменения, уничтожения или шифрования информации о Ваших активах или Ваших данных;
- риск разглашения конфиденциальной информации.

В работе информационных систем «ИНТЕРПРОГРЕССБАНК» (Акционерное общество), системе карточных переводов, системах дистанционного банковского обслуживания используются самые современные технологии и механизмы, обеспечивающие высокий уровень безопасности и удобство пользования услугами.

Наряду с этим, эффективность использования данных технологий и механизмов напрямую зависит от соблюдения Вами необходимых мер безопасности.

В целях минимизации рисков совершения в отношении Вас противоправных действий, настоятельно рекомендуем Вам соблюдать следующие меры безопасности:

- не передавайте никому, не оставляйте в легкодоступных местах Вашу платежную карту и ее фотографию;
- регулярно контролируйте состояние Вашего счёта;
- по возможности не подключайтесь к открытым сетям общего пользования (кафе, гостиницы, офисные центры и т.д.);
- ПИН-код, код CVV (на обратной стороне карты), логин и пароль к системе дистанционного банковского обслуживания – это Ваша конфиденциальная информация. Не сообщайте их никому, включая сотрудников Банка;
- при необходимости передать кому-либо (продать) Ваше электронное устройство (флеш-накопитель, смартфон, планшет, компьютер и т.д.) убедитесь, что вся Ваша конфиденциальная информация, а также платежные приложения надежно удалены с устройства;
- не передавайте никому, не оставляйте без присмотра Ваши электронные устройства (смартфоны, телефоны и т.д.), на которые приходят одноразовые пароли;

- не сохраняйте и не храните Ваши ПИН-код, код CVV (на обратной стороне карты), логин и пароль к системе дистанционного банковского обслуживания на мобильных устройствах, флешках или на любых других, не предназначенных для секретного (зашифрованного) хранения носителях информации;
- не оставляйте записанные на бумаге и т.п. носителях информации Ваши ПИН-код, код CVV, логин и пароль к системе дистанционного банковского обслуживания в легкодоступных местах (напр. на рабочем столе), не передавайте эти данные третьим лицам;
- ограничьте доступ посторонних лиц к Вашим электронным устройствам, с помощью которых осуществляется работа с системой ИПБ-онлайн;
- не используйте устройства третьих лиц для подключения к системам для совершения финансовых операций;
- поставьте пароль на вход в Ваш профиль на компьютере и обязательное условие ввода пароля для входа после отключения «спящего режима» / используйте функцию блокировки смартфона (планшета). Наиболее надежным методом блокировки мобильных устройств является сканер отпечатков пальцев. Если на устройстве нет такой возможности, обязательно используйте защиту с помощью пароля или графического ключа.
- блокируйте экран компьютера, если покидаете рабочее место;
- регулярно обновляйте операционную систему как на компьютерах (Windows, MacOS), так и мобильных устройствах (Android, iOS);
- используете парольную или иную защиту для доступа к устройству;
- регулярно меняйте пароли для работы со своими учетными данными в различных системах. Длина пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов;
- не используйте нелицензионное (пиратское) программное обеспечение;
- рекомендуем отключить возможность удаленного подключения к вашему компьютеру;
- входите в систему ИПБ-онлайн через официальный сайт Банка, убедитесь, что используется безопасное соединение HTTPS (в адресной строке присутствует «замок»);
- регулярно выполняйте антивирусную проверку, используйте современное антивирусное программное обеспечение и регулярно его обновляйте;
- следите за тем, чтобы антивирусная защита, а также брандмауэр Windows или альтернативное решение типа firewall были всегда включены;
- в целях избежание заражения вредоносным программным обеспечением не посещайте интернет-сайты сомнительного содержания;
- не устанавливайте программы, скачанные из недоверенных источников. Для мобильных устройств настоятельно рекомендуем использовать только официальные магазины Google Play и App Store;
- не открывайте неизвестные файлы, присланные на email, в сообщениях социальных сетей, мессенджерах или других мобильных приложений;
- не переходите по ссылкам на неизвестные источники;
- если в процессе работы Вы столкнулись с тем, что ранее действующий ПИН-код, логин/пароль, или токен не позволят Вам войти в систему дистанционного обслуживания - незамедлительно позвоните в Контакт-центр Банка и попросите заблокировать Вашу карту и (или) аккаунт в сервисе дистанционном обслуживании;
- в случае утраты Вашей конфиденциальной информации, подозрениях на её компрометацию незамедлительно позвоните в Контакт-центр Банка и

попросите заблокировать Вашу карту и (или) аккаунт в сервисе дистанционном обслуживании.