Рекомендации по обеспечению безопасности при использовании Интернет-Банка/банковской Карты и по снижению рисков повторного осуществления перевода денежных средств без согласия клиента

1. Исключить возможность неправомерного получения персональной информации пользователей систем ДБО (не передавать неуполномоченным лицам);
2. Осуществлять операции с использованием банкоматов, установленных в безопасных местах (в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.д.).
3. Не использовать банковские Карты в организациях торговли и обслуживания, не вызывающих доверия.
4. При совершении операций с банковской Картой без использования банкоматов не выпускать ее из поля зрения.
5. Не пользоваться устройствами, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.
6. Не использовать ПИН-код при заказе товаров либо услуг по телефону (факсу) или по Интернету;
7. Пользоваться услугой SMS-оповещения о проведенных операциях.
8. Осуществлять информационное взаимодействие с Банком только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные веб-сайты (порталы), обычная и электронная почта и др.), реквизиты которых оговорены в документах, получаемых в Банке.
9. Использовать на компьютере/мобильном телефоне/ином устройстве, с которого осуществляется работа с системой дистанционного банковского обслуживания, следующий комплекс мер безопасности, с которого осуществляется работа с системой ДБО, следующий комплекс мер безопасности:
   - Установите и своевременно обновляйте антивирусное программное обеспечение.
   - Проводите обновление операционной системы.
   - При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети интернет.
   - Используйте компьютер/мобильный телефон/иное устройство только для работы с доверенными сайтами и получения электронной почты.
   - Не открывайте письма и вложения, полученные от неизвестных Вам отправителей.
   - Настройте сервис SMS-уведомлений, об отправке/поступлении платежных документов в Банк, о движении по счету, а также обо всех Ваших входах в Интернет-Банк.
   - Систематически получайте из Банка и контролируйте выписки по счету.
   - Обращайте внимание на дату, время и ip-адреса последних входов в Интернет-Банк.
   - Храните в тайне пароль доступа к Интернет-Банку, исключите его запись на стикерах и т.п.
10. Незамедлительно обратиться в Банк при возникновении следующих ситуаций:
    - На компьютере/мобильном телефоне/ином устройстве, используемом для работы в Интернет-Банке, обнаружено вредоносное программное обеспечение (вирусы, «трояны» и т.д.).
    - В выписке обнаружены несанкционированные Вами расходные операции, либо Вы получили SMS -уведомление об операции, которую не совершали.
    - Вы получили SMS-уведомление об изменении номера мобильного телефона для отправки уведомлений, при этом изменения были совершены без Вашего ведома.

Телефон «Нацинвестпромбанк» (АО): +7(495)786-2152