

Рекомендации по обеспечению безопасности при использовании Системы ДБО/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 публикуйте в социальных сетях фото банковской карты или сканы документов. Желательно даже не упоминать, клиентом какого банка вы являетесь
6. Не пользоваться устройствами, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.
7. Не использовать ПИН-код при заказе товаров либо услуг по телефону (факсу) или по Интернету.
8. Пользоваться услугой SMS-оповещения о проведенных операциях.
9. Контролируйте состояние счета (путем просмотра выписки) и при обнаружении подозрительных операций незамедлительно обращайтесь в Банк для их отмены и объявления сертификата ЭП скомпрометированным.
10. 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.
11. Использовать на компьютере/мобильном телефоне/ином устройстве, с которого осуществляется работа с системой дистанционного банковского обслуживания, 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.
 - Обращайте внимание на дату, время и ip-адреса последних входов в сервис «Интернет-Банк».
 - Храните в тайне пароль доступа к сервису «Интернет-Банк», исключите его запись на стикерах и т.п.
12. Незамедлительно обратиться в Банк при возникновении следующих ситуаций:
 - В выписке обнаружены несанкционированные Вами расходные операции, либо Вы получили SMS -уведомление об операции, которую не совершали.

Телефон АКБ «Форштадт» (АО): 8-800-100-2208.