Памятка по обеспечению безопасности при использовании Системы ДБО

Уважаемые Клиенты!

Общие рекомендации:

1) Пароль для входа в систему дистанционного банковского обслуживания «iBank 2» это личная конфиденциальная информация Клиента, ни при каких обстоятельствах не раскрывайте свой пароль никому, включая сотрудников Банка. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбами сообщить конфиденциальную информацию (пароли, кодовые слова, и пр.) ни при каких обстоятельствах не сообщайте данную информацию.
2) Первоначальная страница доступа в личный кабинет содержит только поля ввода логина и пароля. В случае если на данной странице от Клиента требуется ввод любой другой персональной информации (номеров банковских карт, мобильного телефона, других личных данных), следует прекратить пользование услугой и связаться с сотрудниками Банка.
3) Не сохраняйте пароль в текстовых файлах на компьютере либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.
4) При любых подозрениях на компрометацию пароля посторонними лицами (в т.ч. представившимися сотрудниками Банка), следует незамедлительно остановить работу и обратиться в Банк по телефонам: 98-04-39, 8-800-100-22-08.
5) Используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением.
6) Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ.
7) Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей.
8) Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты своего компьютера – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам»-рассылок и пр.
9) Завершение работы с системой выполняйте путем выбора соответствующего пункта меню.
10) Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.
11) По возможности, исключите работу в Системе «iBank 2» и подготовку платежных документов на персональном компьютере с общедоступным доступом (в т.ч. Интернет-кафе, бесплатный Wi-Fi и пр.).
12) Исключайте на персональном компьютере, на котором осуществляется подготовка и отправка документов в Банк, использование систем удаленного управления персональным компьютером. Не привлекайте для администрирования и обслуживания данного персонального компьютера ИТ-персонал на условиях предоставления ему удаленного доступа.
13) Исключайте посещение с персонального компьютера, на которых осуществляется подготовка и отправка документов в Банк, сайтов сомнительного содержания и любых других Интернет-ресурсов непроизводственного характера (социальные и пиринговые сети, конференции и чаты, телефонные сервисы и т.п.), чтение почты и открытие почтовых вложений от недоверенных источников (неизвестных отправителей), установку и обновление любого программного обеспечения не с сайтов производителей. Настройками сетевого оборудования, корпоративных и персональных сетевых экранов выход в сеть Интернет ограничивайте «белым списком» со всех рабочих мест, на которых осуществляется подготовка, подписание и отправка платежных документов. В «белый список» должны включаться исключительно доверенные сайты и хосты самой организации, банков, налоговой службы, других государственных органов, необходимых в производственном процессе, сервера обновлений системного и антивирусного программного обеспечения.
14) Обращайте внимание на дату, время и ip-адреса последних входов в Систему «iBank 2».
15) Храните носитель ключей (USB-токен) в месте, недоступном посторонним лицам. Исключите хранение ключей на жёстком диске, в сетевых каталогах и прочих общедоступных ресурсах.
16) При наличии проблемы с подключением к Системе «iBank 2» следует немедленно обратиться в службу поддержки Банка.

Рекомендации для клиентов с SMS-паролем:

1) При подтверждении операций одноразовым SMS-паролем необходимо контролировать соответствие реквизитов операции и реквизитов в полученном SMS-сообщении.
2) Не пользуйтесь Системой «iBank 2» с того же мобильного телефона, иного устройства, на который приходят SMS-сообщения с подтверждающим одноразовым паролем.
3) При утрате мобильного телефона, на который Банк отправляет SMS-сообщения с подтверждающим одноразовым паролем, а также в случае, если у Клиента неожиданно перестала работать телефонная sim-карта, следует оперативно обратиться к своему оператору мобильной связи для блокировки абонентского номера и замены sim-карты, а также обратиться в Банк для выявления возможных несанкционированных операций.
4) Не устанавливайте на мобильный телефон, на который Банк отправляет SMS-сообщения с подтверждающим одноразовым паролем, приложения, полученные от неизвестных Клиенту источников. Помните, что банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/Email - сообщения.

Просим Вас незамедлительно обращаться в Банк при возникновении следующих ситуаций:

1) На персональном компьютере, используемом для работы в Системе «iBank 2», обнаружено вредоносное программное обеспечение (вирусы, «трояны» и т.д.).
2) В «Журнале сеансов работы» обнаружены факты проникновения в Систему «iBank 2», посторонних лиц (вход в Систему «iBank 2», с нетипичного IP-адреса либо в нетипичное для Клиента время).
3) В выписке обнаружены несанкционированные Клиентом расходные операции, либо Клиент получил SMS или E-mail-уведомление об операции, которую не совершали.
4) Клиент получил SMS или E-mail-уведомление об изменении адреса E-mail или номера мобильного телефона для отправки уведомлений, при этом изменения были совершены без ведома Клиента.

Телефон АКБ «Форштадт» (АО): 98-04-39, 8-800-100-22-08

Справочный центр Системы «I Bank2»: 8 -495-797-88-89.