ПАМЯТКА пользователю Системы «iBank2» для частных клиентов.

Требования по обеспечению информационной безопасности при работе с Системой

При работе в сети Интернет рекомендуем Вам соблюдать общие правила безопасности, применяющиеся для защиты любых данных, хранящиеся на компьютерах:

1. Используйте только доверенные компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным программным обеспечением (ПО) и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного ПО, своевременно обновляйте лицензионную операционную систему и браузеры.
2. Будьте внимательны: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в Банк с целью оперативного блокирования доступа!
3. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
4. Своевременно обновлять операционную систему (установка патчей, критичных обновлений).
5. Не использовать права администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора.
6. Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
7. Установить и своевременно обновлять на компьютере антивирусное ПО (NOD32, Kaspersky lab, Symantec AntiVirus и т.д.).
8. Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.
9. При выходе в Интернет использовать сетевые экраны (Kerio winroute, Outpost firewall и т.д.), разрешив доступ только к доверенным ресурсам Сети.
10. Запретить в межсетевом экране соединение с интернет по протоколам ftp, smtp. Разрешить соединения smtp только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики.
11. Не давать разрешения неизвестным программам выходить в Интернет.
12. При работе в Интернет не соглашаться на установку каких-либо дополнительных программ от недоверенных издателей.
13. При вводе личной информации, ПОМНИТЕ, что любой веб-адрес (URL) в адресной строке должен начинаться с "https". "S" означает "secure" (защищенный). Если в адресе не указано "https", это значит, что вы находитесь на незащищенном веб-сайте, и вводить данные нельзя.

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей финансовых интернет-систем файлов с секретными ключами Электронной подписи (ЭП) и пароли, вводимые с клавиатуры. Трояны распространяются через e-mail, по каналам ICQ, Skype, через принадлежащие преступникам сайты.

14. Безопасность работы в Системе «iBank2» обеспечена комплексом организационных и логических мер, направленных на предотвращение мошенничества и разглашения конфиденциальной информации.

Со стороны пользователей безопасность работы в Системе обеспечивается выполнением следующих рекомендаций:

1. Никогда и ни при каких обстоятельствах не сообщайте никому (в том числе родственникам) свои пароли для входа в Интернет-банк или для подтверждения платежей, а также номера ваших карт и CVV2/CVC2 коды.
2. Для входа в Систему вам требуется вводить только ваш логин и пароль. Не нужно вводить номер вашего мобильного телефона, номер вашей банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации в Системе. Используйте виртуальную клавиатуру для ввода пароля.
3. В случае утери мобильного телефона, на который приходят SMS-сообщения с разовым паролем, немедленно заблокируйте SIM-карту.
4. Регулярно контролировать состояние счёта (путем просмотра выписки).
5. Обращать внимание на дату и время последних входов в систему (данные фиксируются на первой странице после входа в Систему).
6. Устанавливайте мобильные приложения ООО КБ «РостФинанс» БИФИТ только из авторизованных магазинов App Store и Google Play. Перед установкой приложения убедитесь, что их разработчиком является БИФИТ. Используйте антивирусное программное обеспечение, в случае, если оно доступно для вашего электронного устройства.
7. Обязательно сверяйте текст SMS-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS указан пароль для платежа, который вы не совершали или вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по вашему счету платеж, ни в коем случае не вводите его в Интернет-банке и не называйте его, в том числе сотрудникам банка.
8. Запишите контактный телефон вашего Банка в адресную книгу или запомните его. В случае если в личном кабинете Интернет-банка вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в Банк по ранее записанному вами телефону. Также для этих целей подойдет телефон, указанный на вашей банковской карте.
9. Избегайте регистрации номера вашего мобильного телефона, на который приходят SMS-сообщения с разовым паролем, в социальных сетях и других открытых источниках.

При возникновении следующих ситуаций, просим незамедлительно обращаться в Банк, с целью оперативного блокирования доступа:

1. На компьютере или электронном устройстве, используемом для работы в Системе, обнаружено вредоносное ПО (вирусы, «трояны» и т.д.).
2. В «Журнале сеансов работы» обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).
3. В выписке обнаружены несанкционированные Вами расходные операции, либо Вы получили SMS уведомление об операции, которую не совершали.
4. Вы получили SMS или e-mail-уведомление об изменении адреса e-mail или номера мобильного телефона для отправки уведомлений, при этом изменения были совершены без Вашего ведома.

Перед началом использования Системы «iBank2» внимательно изучите информацию по обеспечению безопасности, размещенную на сайте http://rostfinance.ru.