Джей энд Ти Банк

О безопасном использовании интернет-технологий

Согласно рекомендациям Банка России (письмо от 25.06.2009 № 76-Т) сообщаем о появлении в российском сегменте сети Интернет web-сайтов, имитирующих интернет-представительства ряда российских кредитных организаций. Доменные имена и стиль оформления таких сайтов, как правило, сходны с именами подлинных web-сайтов банков, а содержание прямо указывает на их якобы принадлежность соответствующим кредитным организациям. При этом посетителям таких сайтов сообщаются заведомо ложные банковские реквизиты и контактная информация.

Использование подобных реквизитов, а также вступление в какие-либо деловые отношения с лицами, фактически представляющими ложные банки, связано с риском и может привести к нежелательным последствиям для клиентов кредитных организаций.

В связи с вышеизложенным,
приводим контакты Джей энд Ти Банка в сети Интернет:

Официальный сайт Джей энд Ти Банка: www.jtbank.ru

Администратор официального сайта: webmaster@jtbank.ru

В случае самостоятельного выявления клиентами ложных web-сайтов банка, а также получения информации о них по электронной почте или иным способом просим сообщать о полученных сведениях Администратору официального сайта по адресу: webmaster@jtbank.ru

→

Джей энд Ти Банк

Памятка по работе с системой интернет-банкинга iBank 2

Используемые определения:

- *iBank2* – система интернет-банкинга для юридических лиц
- *ЭЦП* – электронная цифровая подпись сотрудника организации
- *Ключ* – файл, хранимый на электронном носителе, содержащий аналог электронной цифровой подписи ответственного лица. Ключ формируется при регистрации клиента в системе iBank 2 на каждого сотрудника организации, указанного в банковской карточке клиента (генеральный директор, главный бухгалтер). В целях обеспечения профилактики безопасности системы, ключи выписываются сроком на один год. Действие ключей не подлежит продлению, далее следует сформировать новые ключи.

Система интернет-банкинга iBank 2 обеспечивает вас надежной системой безопасности для управления своими счетами. Однако вам так же необходимо побеспокоиться о конфиденциальность информации (паролей и ключей). Данная памятка поможет вам повысить уровень безопасности при работе с системой iBank 2.

Соединение и работа с системой iBank 2 осуществляется через общедоступную сеть интернет в защищенном режиме с помощью протокола SSL (Secure Sockets Layer).

При работе с iBank 2, для повышения безопасности, необходимо следовать следующим рекомендациям:

- Ни при каких условиях не сообщайте информацию о вашем пароле/ключе никому, включая сотрудников Банка.
- Проверяйте, что соединение действительно происходит в защищенном режиме SSL, в правом нижнем углу вашего вэб-браузера должен быть виден значок закрытого замка.
- Ни в коем случае не сохраняйте информацию о вашем пароле на любых носителях, включая компьютер, не осуществляйте отправку паролей, либо ключей по электронной почте. Если у вас возникли подозрения, что кто-либо владеет информацией о вашем ключе, вам необходимо с помощью обращения в Банк (по тел. (495) **662-45-45 /039**) заблокировать ключи ЭЦП.
- После окончания работы в iBank 2 обязательно закройте окно системы с помощью кнопки Выход.
- Убедитесь, что ваш компьютер не поражен какими-либо вирусами. Установите и активизируйте антивирусные программы. Старайтесь их постоянно обновлять. Обращаем внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о вашем ключе.
- Установите и используйте персональный брандмауэр (firewall) на вашем компьютере для входа в Интернет, это позволит предотвратить несанкционированный доступ к информации на вашем компьютере.
- Для подписи платежных документов, используются ключи электронной цифровой подписи (ЭЦП), хранимые в виде файла (ключа) на электронном носителе (дискета, компакт-диск, флеш-память и т.д.), необходимо обеспечить хранение этих данных в месте не доступном посторонним лицам. Также, не следует хранить эту информацию на жестком диске вашего компьютера.
- В случае порчи носителей, содержащих ключи ЭЦП, потребуется формирование новых ключей, т.к. они не могут быть восстановлены. Рекомендуется при получении новых ключей, создавать резервные копии и так же хранить их в месте не доступном посторонним лицам.