Рекомендации по информационной безопасности

Уважаемые клиенты! Доводим до вашего сведения меры предосторожности необходимые для применения дистанционного банковского обслуживания и получения информации при пользовании Web-сайтами.

В связи с участившимися случаями неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания (далее - ДБО) о реквизитах банковских карт, пин-кодах и другой информации и в целях снижения рисков, возникающих при осуществлении кредитными организациями ДБО, в том числе с применением интернет-технологий, а так же В связи с появлением в российском сегменте сети Интернет Web-сайтов, имитирующих интернет-представительства ряда российских кредитных организаций. Банк России опубликовал Письмо от 7.12.2007г. № 197-Т «О рисках при дистанционном банковском обслуживании» и Письмо от 25.06.2009 № 76-Т "О рекомендациях по информированию клиентов о размещении на Web-сайте Банка России списка адресов Web-сайтов кредитных организаций". Начиная с 11.06.2009, он приступил к регулярному размещению на своем Web-сайте **http://www.cbr.ru/credit/CO_SitesFull.asp** списка адресов (доменных имен) официальных Web-сайтов кредитных организаций.

РЕКОМЕНДУЕМ:

1. Исключить возможность неправомерного получения персональной информации пользователей систем ДБО (не передавать неуполномоченным лицам);

2. Пользоваться услугой SMS-оповещения о проведенных операциях с применением ДБО (в случае возможности получения такой услуги);

3. Осуществлять информационное взаимодействие с кредитной организацией только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные web-сайты/порталы, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, получаемых непосредственно в кредитной организации;

4. При пользовании операционным сайтом перед предоставлением имени и пароля НЕОБХОДИМО проверять сертификат;

5. Сообщать кредитной организации об отсутствии возможности подключения к операционному WEB-сайту любым доступным способом;

6. Немедленно заменять ключи электронно-цифровой подписи в случае их компрометации или подозрения на компрометацию, а также по истечении срока действия ключа с периодичностью, установленной документацией на средство криптографической защиты и правилами работы в системе;

7. Немедленно заменять ключи электронно-цифровой подписи во всех случаях увольнения или смены лиц, допущенных к этим ключам, а также руководителей юридического лица, которые подписывали решение (доверенность) о допуске пользователей к ключам электронно-цифровой подписи;

8. Своевременно устанавливать на компьютеры, используемые пользователями систем дистанционного банковского обслуживания, обновления:

- систем дистанционного банковского обслуживания;

- операционной системы;

- Web-браузеров (Microsoft Internet Explorer, Mozilla FireFox, Opera и т.д.);

- антивирусного программного обеспечения.

9. Пользоваться сайтами, только указанными на сайте **http://www.cbr.ru/credit/CO_SitesFull.asp**

10. На информационном сайте Банка не требуется предоставления никакой информации о клиенте;

11. В случае обнаружения ложных Web-сайтов кредитных организаций передать всю информацию о них или о полученных сведениях подобного рода по электронной почте или иным способом.