О мерах информационной безопасности при использовании систем дистанционного обслуживания

1. Работа на компьютере:

- Рекомендуем Вам использовать для работы в системе дистанционного обслуживания защищенный паролем персональный компьютер. Вход в систему с чужого компьютера, а также с компьютеров в интернет-кафе не является безопасным;
- Работайте на компьютере, на котором Вы входите в систему дистанционного обслуживания, под учетной записью без прав локального администратора;
- Используйте только лицензионное программное обеспечение. Помните, использование нелицензионного программного обеспечения это не только правонарушение, но и лазейка в системе Вашей безопасности, которой могут воспользоваться злоумышленники.

2. Защита от вредоносного программного обеспечения:

- Установите на компьютере, который Вы используете для работы с системой дистанционного банковского обслуживания, антивирусное программное обеспечение и настройте его в соответствии с рекомендациями поставщика. Регулярно устанавливайте обновления безопасности;
- Установите и используйте персональный брандмауэр или фаейрвол;
- Устанавливайте только те программы, разработчику которых Вы доверяете;
- Не открывайте и не отвечайте на подозрительные электронные письма, электронные письма от неизвестных отправителей, внимательно проверяйте правильность указанных в письмах ссылок на сайты.

3. Защищенное соединение:

- Проверяйте, действительно ли соединение происходит в защищенном режиме SSL — в окне Вашего веб-браузера должен быть изображен значок закрытого замка;
- Вы можете проверить подлинность сертификата (SSL) сервера, щелкнув на значке защищенного соединения:

Данные сертификата должны содержать следующую информацию:

Для системы дистанционного обслуживания юридических лиц **«iBank2»**
Кому выдан сертификат: ibank2.atbbank.ru
Кем выдан сертификат: COMODO High-Assurance Secure Server CA
Срок действия сертификата: с 28.02.2012 по 17.03.2017

Для системы дистанционного обслуживания физических лиц **«Частный Клиент»**
Кому выдан сертификат: client.atbbank.ru
Кем выдан сертификат: UTN-USERFirst-Hardware
Срок действия сертификата: с 23.06.2010 по 24.06.2015

Для информационной системы **«АТБ Инфо»**
Кому выдан сертификат: info.atbbank.ru
Кем выдан сертификат: COMODO High-Assurance Secure Server CA
Срок действия сертификата: с 02.08.2013 по 02.08.2018

Если Вы щёлкните по вкладке «Путь сертификации» («Certification Path»), Вы увидите действующий статус сертификата. Если статус сертификата отличен от: «This certificate is OK» или «Этот сертификат действителен», пожалуйста, немедленно выйдите из системы дистанционного банковского обслуживания и сообщите в службу технической поддержки Автотогрбанка по телефону 8 (495) 730-5115, электронной почте ps@atbbank.ru или обратитесь в ближайшее отделение Автоторгбанка.

- Для выхода из системы дистанционного банковского обслуживания используйте кнопку «Выход».
- При использовании USB-токена не оставляйте его подключенным к компьютеру после завершения работы в системе.

4. Парольная защита:

- Используйте сложные пароли, состоящие из букв, цифр и специальных символов, которые Вы сможете запомнить, не записывая;
- Никому не сообщайте и не передавайте конфиденциальные данные для входа в систему (пароли, ключи, PIN- коды и т.д.), в том числе родственникам, коллегам и сотрудникам Автоторгбанка.

5. Настройки обозревателя:

- При запросе окна обозревателя об использовании автозаполнения полей формы (логина и пароля) следует отказаться от данной функции. Если возможность автозаполнения личной информации в формах Вашего обозревателя уже активизирована, Вы можете отключить эту функцию вручную в настройках обозревателя. Для этого необходимо установить соответствующие параметры в меню «Сервис»(Tools) -> «Свойства обозревателя»(Internet Options) -> «Содержание»(Content) -> «Автозаполнение»(AutoComplete);
- Следует исключить сохранение конфиденциальных страниц (SSL-page) обозревателем. Для этого необходимо установить соответствующие параметры в меню «Сервис»(Tools) -> «Свойства обозревателя»(Internet Options) -> «Содержание»(Content) -> Формы (Forms).

6. Будьте бдительны:

- Автоторгбанк не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные, не просит сообщить или ввести куда-то Ваш пароль. Если это событие произошло, не отвечайте возможному мошеннику, а сообщите в службу технической поддержки Автотогрбанка по телефону 8 (495) 730-5115, электронной почте ps@atbbank.ru или обратитесь в ближайшее отделение Автоторгбанка.
- Всегда проверяйте адрес сайта:

Для системы дистанционного обслуживания юридических лиц «iBank2» - https://ibank2.atbbank.ru/;
Для системы дистанционного обслуживания физических лиц «Частный Клиент» - https://client.atbbank.ru/ (https://client.atbbank.ru/v1/cgi/bsi.dll?T=RT_2Auth.BF)
Для информационной системы «АТБ Инфо» - https://info.atbbank.ru/ (https://info.atbbank.ru/User/Login?ReturnUrl=%2f)
Вас могут пытаться обмануть, предлагая оставить Ваши пароль и логин на поддельном сайте, который может быть похож внешне на сайт Автоторгбанка. Если Вы обнаружите такой сайт, обязательно сообщите об этом в службу технической поддержки Автотогрбанка по телефону 8

(495) 730-5115, электронной почте ps@atbbank.ru или обратитесь в ближайшее отделение Автоторгбанка.

- При возникновении подозрения, что Ваши конфиденциальные данные для входа в систему стали известны третьим лицам или обнаружении несанкционированных операций в системе, просим Вас незамедлительно обратиться в службу технической поддержки Автотогрбанка по телефону 8 (495) 730-5115, электронной почте ps@atbbank.ru или обратитесь в ближайшее отделение Автоторгбанка.