РЕКОМЕНДАЦИИ
КЛИЕНТАМ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ
ПРИ РАБОТЕ С СИСТЕМОЙ “БАНК-КЛИЕНТ”

Уважаемые Клиенты!

В целях снижения рисков, возникающих при осуществлении взаимодействия с системой дистанционного банковского обслуживания "Банк-Клиент", доводим информацию о необходимости принятия Вами дополнительных мер безопасности и контроля. Предлагаемые меры безопасности помогут Вам предотвратить хищение денежных средств, возможное при реализации злоумышленником:

- перехвата управления компьютером;
- получения криптографических ключей и паролей доступа к системе "Банк-Клиент";
- проведения несанкционированного платежа в банк.

В качестве таких мер АО «ОРБАНК» предлагает Вам реализовать следующее:

1. Ограничение доступа к компьютеру, с которого осуществляется работа с системой "Банк-Клиент"

1.1. Располагайте компьютер в помещении, ограничивающем возможность несанкционированного доступа к нему.
1.2. Предоставляйте право доступа к компьютеру только лицам, работающим с системой "Банк-Клиент".
1.3. Не оставляйте компьютер без контроля при включенном питании и, в особенности, загруженном программном обеспечении системы «Банк-Клиент».
1.4. При перерыве в работе производите процедуру гашения экрана - автоматическую (активируемую по времени простоя) или вручную (комбинация клавиш <Win> + <L>). Для выхода из режима гашения экрана настройте и используйте запрос ввода пароля доступа.
1.5. При повседневной работе не используйте на компьютере учетную запись с избыточными (например, администраторскими) правами доступа к ресурсам компьютера.

2. Применение специализированных средств защиты компьютера от нежелательного программного воздействия.

2.1. Рекомендуется к установке:

- межсетевой экран - разрешающий доступ к внешним сетям только программам, необходимым для работы (в частности с системой "Банк-Клиент"), и запрещающим любое несанкционированное обращение к компьютеру из внешних сетей.
- антивирусная защита - предотвращающая проникновение и активизацию на компьютере вредоносного программного обеспечения (например: вирусы, программы-шпионы и пр.).
- программно-технические средства защиты от несанкционированного доступа.

2.2. Отсутствие или неправильная настройка/ эксплуатация специализированных средств защиты компьютера значительно увеличивает потенциальную возможность проникновения вредоносного программного обеспечения.
2.3. При подозрениях на наличие вирусов на компьютере (например, неожиданных "зависаниях", перезагрузках, несанкционированной сетевой активности), рекомендуется воздержаться от использования системы "Банк-Клиент" до выяснения / исправления ситуации.

3. Контроль установленного на компьютер программного обеспечения

3.1. Устанавливайте только лицензионное программное обеспечение, во избежание попадания на компьютер специальных "шпионских" программ
3.2. Рекомендуется не устанавливать на компьютер более одной операционной системы, во избежание несанкционированного доступа к информации на компьютере.
3.3. Регулярно проверяйте наличие обновлений:

- операционной системы (желательно в автоматическом режиме и, в особенности, имеющих отношение к информационной безопасности компьютера);
- прикладного (офисного) программного обеспечения;
- межсетевого экрана;
- антивирусной системы и ее баз.

3.4. Используйте только доверенные источники для обновления программного обеспечения (рекомендуемые производителем/ поставщиком).
3.5. Не устанавливайте обновления программного обеспечения, полученные по электронной почте.
3.6. При работе с системой "Банк-Клиент" исключите одновременный с ней запуск других программ.
3.7. Активируйте и проверяйте встроенный в операционную систему аудит событий (уровни: “Приложение”, “Безопасность”, “Система”).
3.8. Отключите функцию "автоматическое выполнение" для подсоединяемых к компьютеру внешних носителей информации (например: флеш-карт, компакт-дисков), поскольку имеются вредоносные программы, распространяемые именно этим способом.

4. Эксплуатация электронной почты и сети Интернет

4.1. Рекомендуется ограничить информационный обмен только надёжными информационными порталами и проверенными корреспондентами электронной почты. По возможности не используйте компьютер, с которого осуществляется работа в системе "Банк-Клиент", для развлечений и Интернет-серфинга, не посещайте сайты сомнительного содержания (наибольшие источники распространения вредоносных программ). Например, вредоносная программа может проникнуть на компьютер, при ознакомлении с "интересной ссылкой", или скрываться под всплывающим окном рекламной ссылки на сайте, или в письме от якобы знакомого лица.
4.2. Относитесь с осторожностью к получаемым (в особенности исполняемым) файлам. Не сохраняйте и не устанавливайте файлы, полученные из ненадежных источников (например, скачанные с неизвестных сайтов Интернет, присланные по электронной почте, полученные в телеконференциях). В случае необходимости загрузки файла, проведите до его запуска проверку на содержание вирусов и программных закладок.
4.3. Для снижения вероятности использования злоумышленником уязвимостей браузера рекомендуется установить максимальный уровень безопасности (запрет языка Java, запрет сценариев, запрет загрузки элементов ActiveX). Для доверенных сайтов, требующих разрешения исполнения соответствующих элементов, необходимо индивидуально разрешить их исполнение, добавив сайты в список надежных.
4.4. Для ограничения возможности несанкционированного доступа от Вашего имени в систему "Банк-Клиент", рекомендуется предоставить в письменном виде в Операционное управление сетевой адрес (IP) компьютера, с которого доступ разрешён.
4.5. Обращаем Ваше внимание, что банк никогда не запрашивает у клиентов конфиденциальную информацию по электронной почте, поэтому не отвечайте на письма с просьбой выслать секретный ключ ЭЦП, пароль и другие конфиденциальные данные. Подобные письма создаются только злоумышленниками.

5. Использование криптографических ключей

5.1. Ограничивайте возможности несанкционированного доступа к криптографическим ключам:

- храните ключи на съёмном носителе (дискете, флеш-карте);
- не копируйте ключи на жесткий диск компьютера;
- не оставляйте носители ключей без присмотра (например, постоянно вставленными в компьютер), используйте их только в случае необходимости заверения документов.

Наличие у злоумышленника криптографических ключей позволит ему заверить от Вашего имени документ и передать его в банк на исполнение.
Рекомендуется в качестве носителя криптографических ключей использовать аппаратный электронный USB-ключ eToken (приобретается в Банке как отдельная услуга)
5.2. Напоминаем, что криптографические ключи необходимо менять:

- планово - не реже одного раза в год;
- внепланово - при смене лица, непосредственно работающего с ключами, или при подозрении в компрометации ключей (например, при вирусной активности на компьютере в период использования системы "Банк-Клиент").
-

6. Применение парольной защиты

6.1. Рекомендуется установить парольную защиту на доступ к BIOS компьютера и в операционную систему.
6.2. Периодически меняйте пароль для входа в ссистему «Банк-Клиент» (наиболее оптимальным сроком действия пароля является 3 месяца).
6.3. Рекомендуется установить пароль на ключевой контейнер, который защитит ключи в случае их утери или хищения.
6.4. Не передавайте пароли доступа к компьютеру лицам, не уполномоченным для работы с системой “Банк-Клиент”, а также не хранить пароли в общедоступном месте.
6.5. Для исключения несанкционированного доступа к ключевым документам и/ или системе “Банк-Клиент” применяйте пароли устойчивые к взлому.
6.6. Рекомендации при выборе пароля:

- оптимальная взломостойкость пароля достигается использованием не менее 8 символов;
- используйте в качестве пароля комбинацию знаков (букв, цифр и спецсимволов), смысл последовательности которых трудно определить (т.е. нежелательно использование: имени, фамилии, дня рождения и других памятных дат; номеров телефона, автомобиля; адреса местожительства и других данных, которые могут быть подобраны путем анализа личностной информации), это значительно усложнит процедуру взлома пароля методом подбора;
- не используйте в качестве пароля один и тот же повторяющийся символ либо комбинацию из нескольких символов, набираемых в закономерном порядке на клавиатуре (например, “1234567” или “qwerty” и т. п.), “Легкий” пароль значительно облегчает его взлом злоумышленниками и подвергает Вас финансовым рискам;
- не применяйте один и тот же пароль для доступа к различным по уровню защиты ресурсам (например: для электронной почты, Интернет и системой “Банк-Клиент”).

6.7. Не рекомендуется пользоваться возможностями программ, предлагающих хранение и автоматическую подстановку паролей (например, в браузере).

7. Взаимодействие с системой "Банк-Клиент"

7.1. Внимательно следите за сообщениями, которые появляются на экране компьютера.
7.2. При неожиданном "зависании" компьютера в момент работы с системой "Банк-Клиент", с последующим полным отказом в работе, необходимо позвонить в операционный отдел АО «ОРБАНК» и убедиться, что по Вашему счёту от Вашего имени не отправлен платёж.
7.3. Незамедлительно сообщайте в Банк о факте невозможности получения доступа к системе "Банк-Клиент", по причине несовпадения пароля на вход в систему. Обычной практикой злоумышленников является смена пароля для маскировки своих действий и получения дополнительного времени для успешного выполнения несанкционированных финансовых операций.

8. Меры по сохранности информации

8.1. Рекомендуется сделать резервную копию криптографических ключей на другой сменный носитель (например: дискета, CD/DVD диск) и храните его в сейфе.
8.2. Подключайте компьютер к сети электропитания через устройства бесперебойного питания.