РЕКОМЕНДАЦИИ
клиентам АО «Народный банк»
по обеспечению Информационной безопасности
при работе в системе «ДБО BS-Client x64»

Системное и прикладное программное обеспечение, (операционные системы, Web-браузеры, почтовые клиенты и пр.), далее по тексту ПО, персональных компьютеров, могут содержать уязвимости при использовании сети Интернет. Злоумышленники пытаются найти эти уязвимости и внедрить вредоносный код в ПО компьютера клиента используя среду Интернет, с целью похищения секретного ключа электронной подписи (ЭП) клиента и проведения электронного платежа от имени клиента.
На повышение риска хищения ЭП влияют следующие факторы:

- Отсутствие на компьютере антивируса с актуальными базами и действующих средств фильтрации входящего и исходящего трафика (брандмаурер, он же файервол);
- Отсутствие на компьютере актуальных обновлений операционной системы;
- Использование пиратского программного обеспечения, в котором возможны вирусы и «закладки»;
- Использование в браузере опций разрешения исполнения программ на компьютере клиента;
- Работа на постороннем компьютере вне фирмы клиента;
- Постоянно подключенный к компьютеру секретный ключ ЭП;
- Доступ третьих лиц (технический персонал и т.д.) к секретным ключам ЭП.

Рекомендации по безопасной работе в сети Интернет

1. Не отвечайте на подозрительные письма с просьбой выслать пароль и другие конфиденциальные данные. Подобное письмо наверняка создано злоумышленниками. АО «Народный банк» , далее по тексту Банк, никогда не запрашивает у клиентов конфиденциальную информацию по электронной почте.
2. При использовании служб мгновенного обмена сообщениями – ICQ, InstantMessaging, Mail.ru-агент и т.д. необходимо соблюдать рекомендации аналогично работе с почтовыми клиентами – не принимайте файлы из неизвестных источников, к файлам из известных источников относиться с осторожностью. Проверяйте все полученные файлы антивирусными программами.
3. Не устанавливайте и не сохраняйте подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Такие файлы лучше немедленно удалять. В случае необходимости загрузки файла, убедитесь, что он проверен антивирусом.
4. Откажитесь от посещения сайтов сомнительного содержания (сайты бесплатных программ, хакерские сайты и т.п.). Зачастую такие сайты содержат вредоносные программы, загружаемые и запускаемые при входе на сайт.

Риск использования ложных (фальсифицированных) ресурсов сети Интернет

Фи́шинг (англ. phishing, от phone – телефон и fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является доступ к конфиденциальной информации пользователей, которая в дальнейшем может привести к получению доступа к номерам счетов, паролей, PIN-кодов пластиковых карт и других данных жертвы. Несанкционированный доступ достигается путём проведения мошенниками, так называемыми фишерами, массовых рассылок электронных писем от имени популярных брендов (банков, кредитных организаций, интернет-магазинов, форумов, аукционов и пр.), а также личных сообщений внутри различных сервисов, в том числе от имени Банка, содержащих предложения обновить или предоставить те или иные конфиденциальные

данные. Помимо этого в рассылках могут использоваться специализированные вирусы-черви и шпионские программы для незаметного перенаправления пользователя на фальсифицированные (фишинговые) сайты.

Методы противодействия фишинговым атакам

Не вводите конфиденциальные данные, если окно для ввода отличается от стандартного окна сайта Банка (логотип другой кредитной организации, другие надписи, шрифт и тому подобное) или отображается не так как всегда (нарушен порядок работы в системе).

Внимательно следите за сообщениями, которые появляются на экране компьютера и проверяйте правильность адресной строки системы клиент-банк **«ДБО BS-Client x64»** https://client.nb-bank.ru/

Особое внимание уделяйте наличию протокола **https** в начале адреса, который свидетельствует о наличии защищенного соединения, так как злоумышленники часто используют ложные (фальсифицированные) ресурсы сети Интернет для хищения паролей и др. конфиденциальных данных. Никогда не следует отвечать на письма, запрашивающие конфиденциальную информацию. Никогда не заходите на web-сайт Банка через гиперссылки, которые могут ссылаться на мошеннические web-сайты. Необходимо набирать полный web-адрес Банка http://www.nb-bank.ru/

Общие рекомендации.

Клиентам системы **«ДБО BS-Client x64»** рекомендуется:

- Охрана и организация режима в помещении, где размещено рабочее место для работы в системе **«ДБО BS-Client x64»**, должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.
- На компьютерах, используемых для работы в системе дистанционного банковского обслуживания **«ДБО BS-Client x64»**, устанавливайте пароль на уровне BIOS и уровне операционной системы.
- Используйте предоставляемую Банком возможность закрепления за компьютером клиента одного или нескольких статических интернет-адресов (IP-адресов). Указанная мера возможна только для компьютеров, имеющих выход в Интернет со статическими IP-адресами;
- Используйте и оперативно обновляйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ;
- Устанавливайте и активизируйте персональный межсетевой экран (брандмаурер, он же файервол) защиты и фильтрации входящего и исходящего трафика только по разрешенным IP-адресам. В настройках персонального межсетевого экрана рекомендуется запретить все входящие и исходящие IP-пакеты, за исключением UDP-трафика с DNS-сервером и исходящие TCP-соединения с сервером Банка системы **«ДБО BS-Client x64»**;
- Используйте только лицензионное антивирусное ПО с ежедневно обновляемыми базами;
- Используйте носитель с ключами ЭП (USB-токен) только на момент проведения операций, не оставляйте его постоянно подключенным к компьютеру. В противном случае, **с** помощью вредоносных программ со встроенным механизмом удаленного управления (RAdmin, TeamViewer, VNC и др.) злоумышленники могут подключиться к консоли инфицированного компьютера, подключиться к порталу Банка, использовав ранее перехваченный пароль доступа и постоянно подключенный носитель ключа ЭП от имени клиента, создать платежные поручения, подписать их и отправить в Банк. Также возможны попытки хищений с использованием вредоносных программ, обеспечивающих дистанционный доступ к USB-портам компьютера клиента. При этом вход в систему **«ДБО BS-Client x64»** осуществляется с компьютера злоумышленника, а работа с USB токеном, подключенным к компьютеру клиента происходит дистанционно.

Незамедлительно сообщайте в Банк о факте невозможности получения доступа к системе **«ДБО BS-Client x64»**;

- Проводите электронные платежи с использованием специально выделенного для этих целей компьютер. Данный компьютер не рекомендуется использовать для другой работы в сети Интернет, в том числе для получения электронной почты и т.п.;
- Работайте в Интернете с ограниченными правами (под учетной записью) пользователя, а не администратора (если войти в Интернет с правами администратора, в случае проникновения на компьютер вирус получит эти неограниченные права и доступ ко всем ключевым данным на компьютере);
- В случае использования браузера Internet Explorer правильно настройте его:
  - разрешать выполнение программ из Интернета только для доверенных сайтов;
  - отключить функцию автозаполнения полей (хранение в памяти браузера личной информации): в настройках Internet Explorer "Сервис"(Tools) – "Свойства обозревателя"(InternetOptions) – "Содержание"(Content) - "Автозаполнение" (AutoComplete), предварительно очистив кэш (память) браузера;
  - отключите в браузере опции разрешения исполнения программ на компьютере клиента типа Active X;
- Необходимо организовать доступ к компьютеру и секретным ключам ЭП, исключающий работу на нем посторонних лиц;
- Смените ключ ЭП при увольнении ответственных сотрудников клиента, имевших доступ к ключам клиента, или возникновении подозрений на доступ к нему посторонних лиц. При компрометации или попытке компрометации ключей ЭП, увольнения ответственного сотрудника или ИТ специалиста, который имел доступ к компьютеру или ключам ЭП, срочно обратитесь в Банк для блокировки ключей ЭП и генерации новых.;
- Клиентам отправляется SMS-оповещение о движении средств по счету, в случае получения оповещения о несанкционированной операции по счету, немедленно обратитесь в Банк.
- При генерации ключа ЭП не создавайте простые и легкие пароли (111111, 12345, abcdefg, qwerty и т.п.), не стоит ставить в качестве пароля дату рождения, номер телефона и другие данные, которые можно легко узнать;
- Никогда никому не передавайте аппаратный ключ с ключом ЭП. Для хранения носителей ключей ЭП используйте надежные металлические хранилища**.**

Важно помнить также, что средства защиты данных, применяемые в системах Банка, не распространяют свое действие за их пределы и не могут предохранять компьютер клиента от заражения его вредоносными компьютерными вирусами. В связи с этим, сам клиент должен предпринимать меры по антивирусной защите своего компьютера. Для обеспечения безопасности данных клиента при пользовании системами Интернет-банкинга необходима установка на компьютере и регулярное обновление антивирусных программ. В противном случае, возможно, что вводимая клиентом информация окажется доступной злоумышленникам, использующим и активно распространяющим в сети Интернет шпионские вирусные программы.

Если у Вас возникло подозрение, что Ваш компьютер заражен (неадекватная реакция на Ваши действия, самостоятельная активность, появляющиеся непонятные окна и т.п.), немедленно обращайтесь в Банк.

По результатам проведенной 30.01.2016г. внутренней самооценки - информационная безопасность АО «Народный банк» соответствует требованиям стандарта Банка России по "Обеспечению информационной безопасности организаций банковской системы Российской Федерации".