ПАМЯТКА КЛИЕНТА

о возможных угрозах хищения денежных средств с использованием системы «iBank 2» и способах защиты

Для исключения несанкционированного доступа в систему электронного банкинга КБ «НМБ» ООО проводит комплекс мероприятий для усиления Вашей информационной и финансовой безопасности. Представляем Вам «Памятку о возможных угрозах хищения денежных средств с использованием системы «iBank 2» и способах защиты», а также предлагаем ряд мер, которые повысят уровень Вашей информационной и финансовой безопасности.

Хищение денежных средств с расчетных счетов возможно при получении злоумышленниками доступа к Секретным ключам ЭЦП и паролям. Для того, чтобы предотвратить хищение и использование Вашего Секретного ключа ЭЦП КБ «НМБ» ООО настоятельно рекомендует придерживаться приведенных ниже правил:

- Для хранения файлов с секретными ключами ЭЦП использовать внешние носители: дискеты, флеш-диски, **специализированные устройства – USB-токены «iBank 2 Key».** При этом владелец такого внешнего носителя должен хранить его в условиях, исключающих доступ к нему третьих лиц, например, личный сейф.
- Использовать **IP-фильтрацию** - дополнительный сервис, запрещающий пользование ключами ЭЦП на компьютерах вне вашего офиса. IP-фильтрация позволяет быть уверенным в том, что информация, передаваемая в банк, будет обработана только в случае совпадения IP-адреса передающего компьютера с IP-адресом клиента, хранящимся в базе данных банка;
- Использовать **SMS-Банкинг**. Сервис позволяет оперативно получать информацию о входе в систему, о поступлении платежных поручений, о движении средств и т.д. При получении сообщения о несанкционированной операции Вы должны связаться с Банком для её приостановки.
- Не хранить на носителях с ключами ЭЦП какую-либо другую информацию;
- Не допускать использования «пустых» или простых паролей, например 123456, qwerty, для всех учётных записей, имеющих право входа в Windows. Осуществлять периодическую смену паролей, рекомендуемая частота смены паролей -1 раз в месяц;
- Не передавать ключи ЭЦП ИТ-сотрудникам для проверки работы Системы «iBank 2» и проверки настроек взаимодействия с Банком. При необходимости проведения проверок владелец ключа ЭЦП должен лично подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа «iBank 2», и ввести пароль, исключая умышленное наблюдение посторонними лицами;
- Не передавать ключи ЭЦП замещающим сотрудникам (заместителям, временно исполняющим обязанности). Для таких сотрудников необходимо получить персональные ЭЦП и внести их в банковскую карточку;
- При увольнении ответственного или технического сотрудника, имевшего доступ к Секретному ключу ЭЦП, обязательно заблокировать его ключ ЭЦП;
- При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с Системой «iBank 2», проверить их на отсутствие вредоносных программ;
- В случае если работа в системе Интернет-банкинг продолжительна, отключать и извлекать носители с ключами ЭЦП, если они не используются для работы. Носители с ключами ЭЦП должны находиться в компьютере только в момент подписания документов, и извлекаться сразу после подписания документов;
- Выделить отдельный компьютер, который будет использоваться только для работы с Системой «iBank 2» и не выполнять на этом компьютере никакие другие задачи;
- Ограничить доступ к компьютерам, используемым для работы с Системой «iBank 2» и исключить к ним доступ персонала, не работающего с Системой «iBank 2»;
- Исключить обслуживание компьютеров, используемых для работы с Системой «iBank 2», нелояльными ИТ-сотрудниками;
- При обслуживании компьютера ИТ-сотрудниками, обеспечивать контроль над выполняемыми ими

действиями;

- На компьютерах, используемых для работы с Системой «iBank 2», исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т. п. По возможности, полностью запретить все соединения (входящие и исходящие) с сетью Интернет, разрешив только доступ к необходимым ресурсам;
- Использовать только лицензионное программное обеспечение, обеспечив автоматическое обновление системного и прикладного программного обеспечения;
- Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечив возможность автоматического обновления антивирусных баз, а также еженедельную полную антивирусную проверку;
- Применять на рабочем месте специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение и т.п.;
- Осуществлять антивирусную проверку любых файлов и программ, загружаемых из сети Интернет, полученных по электронной почте или на внешних носителях (дискеты, флеш-накопители, CD/DVD и др.);
- Проводить полную антивирусную проверку после любых действий внештатных IT-специалистов или других сотрудников, выполнявших операции на компьютере, используемом для работы с системой. Например, решение технических проблем: подключения к сети Интернет, установки или обновления бухгалтерских и информационно-правовых программ;
- Не допускать работу под учётной записью Windows, имеющей права администратора. Необходимо использовать учётную запись с ограниченными правами в операционной системе Windows, установленной на компьютере;
- Запрещать использование любых средств удалённого (дистанционного) доступа, которые обычно используется IT-специалистами для удалённой поддержки. Заблокировать возможность использования таких средств с помощью файрвола (программного и/или аппаратного);
- При возникновении подозрений на копирование Секретных ключей ЭЦП или наличие в компьютере вредоносных программ – обязательно заблокировать ключи ЭЦП;
- Если Вы заметили проявление необычного поведения программного обеспечения Системы «iBank 2» или какие-то изменения в интерфейсе программы – позвонить в Банк и выяснить, не связаны ли такие изменения с обновлением версии программного обеспечения. Если нет – заблокировать ключи ЭЦП.

Хищение денежных средств с расчетных счетов при получении злоумышленниками доступа к Секретным ключам ЭЦП и паролям с целью направления в Банк платежных поручений, заверенных от Вашего лица похищенным ключом ЭЦП предположительно могут осуществить:

- ответственные сотрудники Вашей организации, ранее имевшие доступ к Секретным ключам ЭЦП;
- штатные ИТ-сотрудники Вашей организации, имеющие или имевшие технический доступ к носителям (дискеты, флеш-носители, жесткие диски и пр.) с Секретными ключами ЭЦП, а также доступ к компьютерам организации, с которых осуществлялась работа по Системе «iBank 2»;
- нештатные, приходящие по вызову, ИТ-специалисты, обслуживающие компьютеры Вашей организации, осуществляющие профилактику и подключение к Интернету, установку и обновление бухгалтерских и информационно-правовых программ (другого программного обеспечения) на компьютеры, с которых осуществлялась или осуществляется работа по Системе «iBank 2»;
- другие злоумышленники путем заражения через Интернет Ваших компьютеров вредоносными программами, через уязвимости системного и прикладного программного обеспечения с последующим дистанционным хищением Секретных ключей ЭЦП и паролей.

Таким образом, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием действующих Секретных ключей ЭЦП, имеющие обычные реквизиты получателей и типовые назначения платежа.

КБ «НМБ» ООО напоминает Вам о том, что:

- не имеет доступа к Вашим Секретным ключам ЭЦП и не может от Вашего имени сформировать корректную ЭЦП под электронным платежным поручением;
- не осуществляет рассылку электронных писем с просьбой прислать Ваш Секретный ключ ЭЦП или пароль;
- Банк не рассылает по электронной почте программы для установки на Ваши компьютеры. В случае если Вы получили подобное письмо от имени Банка, содержащее программу для установки или запрос на предоставление ключей ЭЦП/паролей, необходимо незамедлительно сообщить об этом в Службу технической поддержки клиентов Банка;
- ответственность за конфиденциальность Ваших Секретных ключей ЭЦП лежит на Вас, как единственных владельцах Секретных ключей ЭЦП;
- если Вы сомневаетесь в конфиденциальности своих Секретных ключей ЭЦП или есть подозрение в их компрометации (копировании), Вы должны незамедлительно заблокировать Ваши ключи ЭЦП;

изменение пароля доступа к Секретному ключу ЭЦП не защищает Вас от использования злоумышленниками ранее похищенного ключа