Акционерное общество
Банк «Национальный стандарт»

Уважаемые Клиенты!

АО Банк «Национальный стандарт» информирует Вас о том, что высокие темпы развития Интернет-технологий предоставляют пользователям максимальную мобильность и удобство. Одновременно с этим, а также принимая во внимание ухудшение экономической ситуации в стране, растет число целенаправленных атак злоумышленников на компьютерные системы клиентов банков с целью кражи средств с банковских счетов, а сами атаки становятся все более изощренными.

Одна из основных угроз — это получение злоумышленниками удаленного доступа к компьютеру, на котором используются системы «Банк-Клиент», как правило путем вирусного заражения через сообщения электронной почты, сайты в сети интернет, интернет-мессенджеры и пр.

АО Банк «Национальный стандарт», обращает Ваше внимание на необходимость соблюдения следующих мер безопасности**:**

- В случае компрометации или подозрения на компрометацию незамедлительно обратиться в Банк для блокирования доступа в систему «Банк-Клиент» (далее — система).
- Подключать ключевой носитель (Рутокен и пр.) к компьютеру только на время использования (вход в систему и непосредственно подпись документа), извлекать ключевой носитель из компьютера в остальное время. Не оставлять ключевой носитель без присмотра, не передавать его другим лицам, включая других уполномоченных для работы в системе лиц. Хранить ключевые носители в защищенном месте.
- Не оставлять без контроля компьютер при активной сессии работы в системе. Если Вы оставляете компьютер без контроля, то необходимо осуществлять выход из системы, используя соответствующие кнопки системы «Выйти» или «Завершить», после чего закрыть окно интернет-браузера, извлечь ключевой носитель и произвести блокировку компьютера одновременным нажатием на клавиатуре ⊞ и L.
- Исключить удаленное управление компьютером без явного подтверждения каждого подключения уполномоченным на доступ в систему лицом.
- Осуществлять вход в систему только по официально предоставленным ссылкам https://enter1.ns-bank.ru и https://enter2.ns-bank.ru**.** Убедиться, что при входе в систему установлено защищенное соединение («https» в начале адресной строке). Не входить в систему по ссылкам с других сайтов или сообщений электронной почты, т.к. злоумышленники часто используют фишинговые сайты (сайты-двойники). При обнаружении сайта-двойника немедленно сообщить об этом в службу технической поддержки Банка для проведения расследования.
- Включить и настроить межсетевой экран (брандмауэр) таким образом, чтобы ограничить доступ как к сети интернет и из неё.
- Не посещать с компьютера, используемого для работы с системой, сайты социальных сетей, развлекательные и игровые сайты, сайты знакомств, сайты, распространяющие программное обеспечение, музыку, фильмы и т.п. в целях предотвращения заражения компьютера.
- Установить антивирусное программное обеспечение и регулярно производить его обновление и обновление других программных продуктов и операционной системы. Не использовать операционную систему и программное обеспечение, для которых

прекращен выпуск обновлений безопасности (Windows XP, Windows Server 2003 и пр.). Использовать программное обеспечение только из проверенных и надёжных источников.

- Отключить режим автозапуска на сменных носителях (CD, флешки и т.п.). Выполнять антивирусную проверку всех сменные носителей.
- Не запускать неизвестные программы. Не устанавливать надстройки и плагины в интернет-браузер (например, от поисковых служб Яндекс, Google и т.п., дополнительные панели, различные «ускорители интернет» и т.п.).
- Установить для повседневной работы ограниченные права доступа к компьютеру и не работать с правами Администратора.
- Если возникает подозрение на заражение компьютера вирусом, немедленно прекратить работу в системе и провести полную антивирусную проверку.
- Использовать надежные пароли для доступа в систему «Банк-Клиент» и пароли для входа в операционную систему, имеющие длину не менее 8 символов и содержащих цифры, заглавные и строчные буквы. Производить регулярную смену паролей и немедленно менять пароли после любого подозрения на компрометацию. Пароли запрещено произносить вслух, выводить на экран, кому-либо передавать.
- Все работы, связанные с поддержкой и обслуживанием компьютера, осуществлять под контролем лица, уполномоченного для работы в системе.
- При увольнении ответственного работника, имевшего доступ к ключам электронной подписи, выполнить замену ключей.
- При увольнении специалиста, обслуживавшего компьютеры с установленной системой, проверить компьютеры на отсутствие вредоносных программ и сменить все электронные ключи, расположенные на незащищенных носителях (любые, кроме Рутокен). Крайне рекомендуется переустановить операционную систему компьютера.

Также рекомендуется:

- Не устанавливать программное обеспечение без особой необходимости.
- Использовать компьютер только для работы с банком и бухгалтерского учета.
- Установить пароль на вход в BIOS Setup компьютера. Настроить в BIOS Setup возможность загрузки операционной системы только с основного жесткого диска и пароль на загрузку компьютера.
- Не открывать письма электронной почты или сообщения интернет-мессенджеров (ICQ, Viber, WhatsUp, Facebook messenger и проч.) от неизвестных отправителей. Сразу удалять их, не открывать вложенные файлы, не переходить по содержащимся в таких письмах ссылках.
- Настроить аудит (протоколирование) событий в операционной системе и другом программном обеспечении. Периодически просматривать журналы аудита и реагировать на ошибки и попытки несанкционированного доступа.

Более подробная информация размещена на сайте www.ns-bank.ru в разделе Корпоративным клиентам → Расчетно-кассовое обслуживание → Документы → Памятка о мерах по безопасному использованию электронного средства платежа и системы дистанционного банковского обслуживания.

Просим не экономить время на соблюдении мер безопасности и искренне благодарим Вас за сотрудничество!