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.

Перед осуществлением входа в систему убедиться, что Вы находитесь на подлинном сайте. Не входите в систему по ссылкам с других сайтов или сообщений электронной почты, т.к. злоумышленники часто используют фишинговые сайты (сайты-двойники) для хищения Вашей аутентификационной информации (логин, пароль).

При обнаружении сайта-двойника немедленно сообщить об этом в службу технической поддержки Банка, для проведения расследования.

Убедиться, что при входе в систему установлено защищенное соединение («https» в начале адресной строке).

Никому и никогда не сообщать свой пароль к системе.

Не использовать предлагаемую браузером функцию сохранения паролей к сайтам.

Не запускать неизвестные программы, не открывать почтовые вложения от неизвестных отправителей.

Включить и настроить межсетевой экран (брандмауэр).

Установить на свой компьютер антивирусное программное обеспечение и регулярно производить его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ).

Не использовать операционную систему, антивирусное и иное программное обеспечение, для которых прекращен предусмотренный разработчиком выпуск обновлений безопасности, антивирусных баз (Windows XP, Windows Server 2003, Windows 7, 8, 8.1 и пр.).

Использовать программное обеспечение (операционные системы, приложения) только из проверенных и надёжных источников.

Не оставлять без контроля компьютер при активной сессии работы в системе. При оставлении компьютера необходимо осуществлять выход из системы, используя соответствующие кнопки системы «Выйти» или «Завершить», после чего закрыть окно Интернет-браузера, извлечь ключевой носитель (если имеется) и произвести блокировку компьютера одновременным нажатием на клавиатуре ⊞ и L. Возобновление работы на компьютере производить с использованием пароля доступа. По окончании рабочего дня производить выключение компьютера.

Отключать режим автозапуска на сменных носителях (CD, флешки и т.п.). Всегда проверять все, подключаемые к компьютеру, сменные носители на отсутствие вирусов и иных вредоносных программ.

Исключить удаленное управление компьютером, с которого осуществляется доступ в систему, без явного подтверждения каждого подключения уполномоченным на доступ в систему лицом.

Не устанавливать надстройки и плагины (например, от поисковых служб Яндекс, Google и т.п., дополнительные панели, различные «ускорители интернет» и т.п.) в интернет-браузер, который используется для доступа к системе.

Установить для повседневной работы ограниченные права доступа к компьютеру. Не работать с правами Администратора. Административные полномочия в операционной системе следует использовать только для установки и настройки операционной системы и программного обеспечения.

В случае если возникает подозрение на заражение компьютера вирусом, немедленно прекратить работу в системе и провести полную проверку компьютера на наличие вредоносного программного обеспечения.

Использовать надежные пароли для доступа в систему дистанционного банковского обслуживания и пароли для входа в операционную систему компьютера, имеющие длину не менее 8 символов и содержащих буквы из различных регистров (заглавные и строчные) и цифры. Производить регулярную смену паролей не реже одного раза в месяц и немедленно после любого подозрения на компрометацию. Использовать пароли только соответствующему уполномоченному для работы в системе лицу. Пароли запрещено произносить вслух, выводить на экран, кому-либо передавать.

Помнить о том, что сотрудники Банка не запрашивают у клиентов информацию о логинах и паролях, не просят выполнять денежные переводы.

Рекомендуется:

Избегать входа в систему в местах, где услуги Интернета являются общедоступными, например, Интернет-кафе, а также с неизвестных Вам компьютеров.

Не хранить на серверах электронной почты (в особенности, бесплатных ресурсов веб-почты) письма, содержащие конфиденциальную информацию.

Не устанавливать на компьютере, используемом для доступа в систему, программное обеспечение без особой необходимости.

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, WhatsApp, Telegram и проч.) от неизвестных отправителей, сразу удалять их, не открывать вложенные файлы, не переходить по содержащимся в таких письмах ссылках.

Более подробная информация размещена на сайте www.ns-bank.ru в Памятке 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!