

**РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМЫ
ИНТЕРНЕТ-КЛИЕНТ ООО РНКО «Единая касса»**

Уважаемый клиент!

ООО РНКО «Единая касса» уведомляет Вас об участившихся в последнее время попытках хищения денежных средств Клиентов посредством системы дистанционного банковского обслуживания в ряде российских кредитных организаций. Во всех выявленных случаях злоумышленники пользовались халатностью Клиентов, хранящих секретные ключи в файлах на дисках или оставляющих носитель с ключевой информацией (USB-токен и др.) постоянно (круглосуточно) и бесконтрольно подключенным к компьютеру с доступом в Интернет. Чаще всего злоумышленник получает контроль над компьютером Клиента путем заражения его компьютерным вирусом, после чего ему становятся известны все пароли, вводимые Клиентом, и доступны все ресурсы компьютера.

Заражение компьютера в отсутствие антивирусной защиты может происходить незаметно для Клиента. Чаще всего заражение происходит при использовании нелицензионного программного обеспечения, полученного бесплатно с интернета, через рассылки заманчивых рекламных электронных сообщений или путем «фишинга» (выдача сайта - двойника мошенника за официальный интернет - сайт).

Особенное внимание необходимо уделить тем Клиентам с так называемым «домашним» компьютером, где выход в Интернет наиболее часто осуществляется без использования межсетевоего экрана и антивирусной защиты.

Определить работникам ООО РНКО «Единая касса» кто именно использует ключи электронной подписи в таких случаях невозможно. Как правило, преступниками выбирается последний рабочий день (пятница) для кражи средств, после чего они меняют пароль на вход с целью заблокировать доступ Клиента к системе дистанционного банковского обслуживания. Может проводиться также уничтожение данных с компьютера для того, чтобы Клиент в первую очередь занимался восстановлением работоспособности своего компьютера.

С целью исключения риска хищения средств с Ваших счетов, с использованием системы дистанционного банковского обслуживания (ДБО), рекомендуем дополнительные меры информационной безопасности:

1. При поломке компьютера, с которого осуществляется работа по системе дистанционного банковского обслуживания, немедленно сообщите об этом в ООО РНКО «Единая касса» для контроля операций по счету.
2. Сохраняйте в тайне закрытый (секретный) ключ электронной подписи. Не оставляйте ключевые носители в компьютере или на столе, если Вы покидаете свое рабочее место. По окончании работы ключевые носители необходимо убирать в надежное место, например, в сейф.
3. Немедленно заменяйте/перегенерируйте ключ электронной подписи в случаях его компрометации или подозрения на компрометацию, а также при истечении срока действия ключа с периодичностью, установленной договором и правилами работы в системе дистанционного банковского обслуживания. Кроме того, рекомендуется заменять ключи электронной подписи во всех случаях увольнения или смены лиц, ранее допущенных к работе с ними, в том числе руководителей организации, которые подписывали решения (доверенности) о допуске пользователей к ключам электронной подписи.
4. Не работайте в системе дистанционного банковского обслуживания с гостевых рабочих мест (интернет-кафе и т.д.).
5. Периодически изменяйте пароль входа в систему дистанционного банковского обслуживания.
6. Постоянно используйте лицензионное программное обеспечение и современные системы антивирусной защиты на Вашем компьютере.

В случае подозрения или обнаружения несанкционированного доступа в систему ДБО необходимо срочно позвонить в ООО РНКО «Единая Касса» для приостановления работы Вашей системы по следующим телефонам: +7 (495) 640-73-40, +7 (495) 640-73-50, доб.415 (с 8:00 до 20:00 МСК).