Уважаемый Пользователь системы Банк-Клиент «ELBRUS Internet»/«RBO»!

В настоящее время против пользователей систем Банк-Клиент российских банков активно действуют хакерские группы, которые внедряют на персональных компьютерах (ПК), подключенных к сети Интернет, вредоносное программное обеспечение (ПО). При обнаружении на компьютере клиента ПО или адресов систем Банк-Клиент вирус связывается с управляющим сервером и предоставляет злоумышленникам удаленное управление зараженным ПК, позволяющее осуществлять несанкционированные клиентами платежи. После этого злоумышленники пытаются вывести жесткий диск ПК клиента из строя с целью скрытия факта списания денежных средств.

Заражение ПК клиентов производится с использованием вирусных программ, массово распространяемых в сети Интернет через взломанные сайты, рекламно-баннерные сети, свободно распространяемые медиа контент и ПО, электронную почту и социальные сети (ok.ru, vk.com). При этом новые модификации вирусов, сигнатуры которых еще не включены в антивирусные базы, успешно преодолевают антивирусное ПО.

В системах «Банк-Клиент» АО Райффайзенбанк используются современные средства обеспечения информационной безопасности, направленные на обеспечение наиболее удобной работы с системой при поддержании высокого уровня безопасности. Вместе с тем, соблюдение приведенных рекомендаций позволит наиболее безопасно работать с Системой и уменьшить риски проведения несанкционированных операций:

- Если возможно, используйте для работы с Системой выделенный компьютер,
- Минимизируйте количество пользователей компьютера, установите для них надежные пароли, обеспечьте периодическую смену этих паролей,
- Не работайте на компьютере под учетными записями, имеющими административные права. Административная учетная запись может использоваться только для установки ПО Системы и средства криптографической защиты информации,
- Всегда корректно завершайте работу в системе в соответствии с Руководством пользователя,
- Блокируйте экран компьютера в случае ухода с рабочего места (даже кратковременного), в случае длительного отсутствия и по окончании рабочего дня обязательно выключайте компьютер,
- Самостоятельно или под личным контролем генерируйте в Системе свой секретный и открытый ключи,

Используйте сложные пароли, состоящие из букв, цифр и специальных символов. Регулярно, не реже 1 раза в 3 месяца, проводите смену пароля на вход в Систему.,

- Ни при каких обстоятельствах не передавайте никому конфиденциальные данные для входа в Систему (пароли, ключи, PIN-коды и т. д.), в том числе родственникам, коллегам или сотрудникам Банка,
- Храните ключевые носители в персональном сейфе, исключающем несанкционированный доступ к ним. Не записывайте секретный ключ на жесткий диск компьютера, на котором установлена Система, на сетевые диски и иные несъемные носители информации,
- Вставляйте ключевой носитель в компьютер только во время работы с Системой.

При выявлении следующих признаков незамедлительно обратитесь в службу поддержки ELBRUS Internet/RBO по телефонам, указанным в Руководстве пользователя или в ближайшее отделение Райффайзенбанка:

- утрата (потеря, хищение) ключевого носителя, PIN-конверта,
- конфиденциальные данные для входа в систему стали известны третьим лицам,

- обнаружены несанкционированные операции (смена пароля, создание платежных поручений) в Системе,
- нестабильная работа компьютера или его полная неработоспособность,
- самостоятельная (независимая от действий Клиента) работа Системы или компьютера: перемещение курсора, открытие и закрытие окон, заполнение строк документа.

Принимайте меры по контролю конфигурации компьютера, с использованием которого осуществляется работа с системой ELBRUS Internet/RBO, а также своевременно проверяйте корректность работы антивирусного ПО и актуальность антивирусных баз, в том числе:

- Настройте и контролируйте уведомления о действиях, произведенных в ELBRUS Internet.
- Используйте на компьютере только лицензионное программное обеспечение, дистрибутивы которого получены из надежных источников.
- Установите на компьютер антивирусное программное обеспечение. Обеспечьте автоматическое обновление антивирусных баз. Настройте еженедельное проведение полной антивирусной проверки компьютера.
- Организуйте автоматическую установку обновлений безопасности операционной системы и другого установленного на компьютере ПО по мере их выпуска производителями.
- Минимизируйте состав установленного на компьютере ПО. Исключите установку на компьютер любых программ, не требующихся для работы с ELBRUS Internet.
- Не допускайте установку на компьютер никаких программ для удаленного управления (RAdmin, VNC, TeamViewer и т.п.). Заблокируйте на нем работу встроенного сервиса удаленного доступа к рабочему столу.
- Полностью запретите (либо ограничьте) доступ по локальной сети к компьютеру.
- Исключить использование с компьютера интернет-ресурсов, не относящихся к работе в ELBRUS Internet/RBO, обновлению ПО и обновлению антивирусных баз.

Актуальные угрозы.

Указанные ниже угрозы актуальны для клиентов любых банков и не зависят от программного обеспечения, предоставляемого банками клиентам для проведения электронных переводов.

- подмена реквизитов получателя при выгрузке текстового документа из ПО 1С в систему Elbrus/RBO.

вредоносное ПО отслеживает появление на жестком диске ПК текстового файла «1C_to_kl».txt с данными платежа и подменяет реквизиты получателя. При этом поле «Наименование получателя» зачастую не меняется!

Важно! Необходимо сверять реквизиты получателя в системе Elbrus/RBO до подписания документа и отправки его в банк.

- подмена адреса отправителя в сообщении по электронной почте якобы от известного контрагента:

в результате взлома учетной записи электронного ящика контрагента злоумышленник получает доступ к его переписке. Затем злоумышленник отправляет сообщение контрагенту с поддельного адреса взломанного электронного ящика с указанием нужных ему реквизитов (при этом в поле «Наименование получателя» злоумышленник может указать наименование доверенного контрагента). Реже для переписки используется взломанный электронный ящик.

Важно! Не совершайте переводы по реквизитам, полученным по электронной почте!

АО «Райффайзенбанк» не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (пароли, ключи, PIN-коды и т. д.).
Будьте бдительны: не отвечайте на подобные запросы!