Рекомендации по обеспечению безопасности перевода денежных средств

Распоряжение денежными средствами при помощи банковских карт, электронных кошельков и дистанционных каналов обслуживания является источником повышенного риска мошеннических операций. Настоящие Рекомендации призваны проинформировать Клиентов ООО РНКО «Платёжный конструктор», о случаях повышенного риска использования электронного средства платежа, о способах снижения рисков повторного осуществления перевода денежных средств без согласия Клиента или с согласия, полученного под влиянием обмана или при злоупотреблении доверием, о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления банковских операций лицами, не обладающими правом их осуществления, и мерами по их снижению.

Если РНКО отдельным сообщением просит Вас ещё раз ознакомиться с настоящими Рекомендациями и, одновременно, РНКО отказала Вам в проведении каких-либо платежей - РНКО считает, что Вы можете стать жертвой повторных мошеннических операций и Вам необходимо уделить особое внимание своей безопасности.

1. Никому не сообщайте одноразовые пароли, полученные для доступа в системы (программы, личные кабинеты), используемые для перевода денежных средств (в том числе – электронных денежных средств), вне зависимости от того, сформированы ли они Вами самостоятельно или получены по SMS/push.

2. Отключайте, извлекайте носители с ключами электронной подписи (токены), если они не используются для работы (проведения платежей).

3. Не пользуйтесь личными кабинетами, системами дистанционного банковского обслуживания и электронного документооборота, платежными приложениями с гостевых рабочих мест или с электронных устройств, принадлежащих иным лицам. При использовании гостевых рабочих мест и таких электронных устройств повышается риск несанкционированного использования ключей электронной подписи и паролей.

4. Ограничьте доступ к электронным устройствам, используемым для дистанционного получения банковских услуг. По возможности исключите или ограничьте удаленное управление электронным устройством, применяемым для таких операций.

5. На электронных устройствах, используемых для дистанционного получения банковских услуг, исключите посещение сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения. Такие сайты и программное обеспечение могут являться разносчиками вредоносного программного обеспечения, предназначенного для кражи денежных средств.

6. Убедитесь перед вводом своих данных на сайтах, используемых для проведения платежей, что соединение установлено с желаемым сайтом. Для этого необходимо проверить правильность указания адреса сайта в строке браузера и наличие сертификата безопасности (https в адресной строке).

7. В случае обнаружения подозрительных сайтов, доменные имена и стиль оформления которых сходны с сайтами, используемыми Вами для проведения платежей, – сообщите об этом через форму обратной связи на настоящем сайте.

8. Используйте только лицензионное программное обеспечение или свободно распространяемое программное обеспечение с официальных сайтов (операционные системы, офисные пакеты, антивирусное программное обеспечение и пр.).

9. Обеспечьте автоматическое обновление системного и прикладного программного обеспечения, средств антивирусной защиты и антивирусных баз.

10. Применяйте на рабочем месте лицензионные персональные межсетевые экраны, антишпионское программное обеспечение и т.п.

11. Исключите обслуживание электронных устройств, используемых для проведения операций с денежными средствами, лицами, не состоящими с Вами в договорных отношениях, посторонними лицами.

12. При обслуживании электронного устройства иными лицами - обеспечивайте контроль за выполняемыми ими действиями.

13. Никогда не передавайте ключи электронной подписи, иные инструменты авторизации в системах проведения операций с денежными средствами иным лицам для проверки работоспособности или настроек таких систем. При необходимости таких проверок – самостоятельно используйте носители ключевой информации, вводите логины и пароли способом, исключающим его доступность иным лицам.

14. При завершении отношений с лицами, осуществлявшими обслуживание электронных устройств, применяемых для проведения платежей, или имевшими временных доступ к таким устройствам - убедитесь в отсутствии вредоносных программ на таких устройствах.

15. Если используемые Вами ключи, логины и пароли доступны иным лицам в силу каких-либо правоотношений между такими лицами и Вами – немедленно по завершении таких отношений блокируйте доступ указанных лиц к системам перевода денежных средств и отзывайте их ключи электронной подписи, используемые при платежах.

16. Если для перевода денежных средств Вы используете ключ электронной подписи, то при возникновении подозрений на несанкционированную работу в применяемых Вами для проведения операций с денежными средствами системах или при наличии вредоносных программ на электронных устройствах обратитесь в кредитную организацию, выдавшую соответствующий ключ электронной подписи.

17. При получении от кредитной организации уведомления о приостановке или отказе в проведении операции – рассмотрите полученную информацию на предмет того, свидетельствует ли она о списании Ваших денежных средств без Вашего согласия либо с согласием, полученным под влиянием обмана или при злоупотреблении доверием. Если Вы считаете, что операция соответствует указанным критериям – обратитесь в соответствующую кредитную организацию по реквизитам, указанным на сайте такой организации, и сообщите о несанкционированном списании денежных средств.

18. При получении сообщений и звонков, требующих или подразумевающих возможность предоставления собеседнику информации о Ваших счетах, операциях, денежных средствах или инструментах доступа к ним, а также настаивающих на проведении платежа или иных операций с активами:

18.1. Контролируйте источник такого сообщения, в том числе:

I. Сопоставьте такие сообщения с иными сообщениями от этого же отправителя (например – на основании заголовка письма).

II. Не нажимая на ссылку в сообщении наведите курсор на неё и проверьте, куда она ведёт.

III. Обратите внимание на орфографию, стиль и язык сообщения – сообщения с явными ошибками, неграмотные сообщения могут свидетельствовать о мошеннических действиях.

IV. При возникновении сомнения – самостоятельно найдите контактные данные отправителя и обратитесь к нему за подтверждением сообщения.

18.2. Контролируйте осведомлённость отправителя – проверьте, действительно ли отправитель сообщения знает всю информацию о Вас, которую он должен знать (при получении сообщения от работодателя или работника – вашу должность, при получении сообщения от кредитной организации – ваше полное имя, номера ваших счетов).

18.3. Не спешите предоставлять затребованную информацию. Если отправитель сообщения настаивает на срочном предоставлении информации – используйте другой способ связи, чтобы проверить благонадёжность источника (при получении сообщения по телефону – свяжитесь с отправителем по известному Вам адресу электронной почты).

18.4. При получении сообщения от неизвестного источника, представляющегося сотрудником какой-либо (в том числе – государственной) организации – требуйте предоставить имя, должность, номер телефона источника или его непосредственного руководителя. При получении этих сведений – проверьте эту информацию в интернете или обратитесь в такую организацию самостоятельно по реквизитам, указанным на её сайте.

19. При необходимости оперативной связи с РНКО используйте реквизиты, указанные на сайте РНКО https://paymentkit.ru/.