# Банк «Прохладный» ООО

УТВЕРЖДЕНО
ПРЕДСЕДАТЕЛЕМ ПРАВЛЕНИЯ
БАНКА «ПРОХЛАДНЫЙ» О О О
ПРОТОКОЛ № 5-а ОТ «20» ЯНВАРЯ 2016 г.

# ИНФОРМАЦИЯ ДЛЯ КЛИЕНТОВ БАНКА «ПРОХЛАДНЫЙ»ООО О ВОЗМОЖНЫХ РИСКАХ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

2016 г.

**Информация для клиентов Банк «Прохладный» ООО о возможных рисках получения несанкционированного доступа к защищаемой информации путем использования ложных ресурсов сети Интернет с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, рекомендуемых мерах по их снижению и рекомендации по защите информации от воздействия вредоносного кода и несанкционированного доступа путем использования ложных ресурсов сети Интернет:**

1. Не сообщайте посторонним лицам персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, логины и пароли доступа к ресурсам Банка, историю операций, так как эти данные могут быть перехвачены Злоумышленниками и использованы для получения доступа к Вашим счетам.

2. Не записывайте логин и пароль на бумаге, мониторе или клавиатуре.

3. Не используйте функцию запоминания логина и пароля в браузерах.

4. Не используйте одинаковые логин и пароль для доступа к различным системам.

5. Не пользуйтесь системами, требующими ввода логина и пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых Вы не уверены. По возможности совершайте операции только со своего личного Средства доступа в целях сохранения конфиденциальности персональных данных и (или) информации о банковском счете.

6. Всегда явным образом завершайте сеанс работы с Системой, используя пункт меню «Выход».

7. В случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web-страницу). После возвращения к своему Средству доступа обязательно смените логин и пароль.

8. Если Вы получили на электронную почту письмо с просьбой обновить или подтвердить персональную и любую другую конфиденциальную информацию со ссылкой на какой-либо сайт (в том числе – сайт Банка), помните, что Банк никогда не просит передать данные по электронной почте. Обновление ключевых персональных данных осуществляется только сотрудником Банка и только по обращению Клиента. Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них.

9. Не открывайте приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способное украсть Ваши идентификационные данные для входа в Систему.

10. При регистрации на сторонних интернет-сайтах всегда изменяйте пароли, которые приходят Вам по электронной почте. Помните, что Банк никогда не направляет пароли по электронной почте.

11. Регулярно, не реже одного раза в месяц, производите смену пароля.

12. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] < >. Настоятельно рекомендуется использовать специализированные программы- генераторы паролей (http://www.infotecs.ru/Soft/pass.htm).

13. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

14. При использовании ЭП не позволяйте третьим лицам производить за Вас генерацию ключей.

15. При использовании ЭП присоединяйте ключевой носитель ЭП к компьютеру непосредственно перед началом работы с Системой. По окончании работы извлекайте ключевой носитель из компьютера.

16. Используйте лицензированное программное обеспечение. ПОМНИТЕ: помимо того, что за пользование нелицензированным программным обеспечением предусмотрена уголовная ответственность в соответствии со статьей 146 УК РФ, использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа на Ваш компьютер.

17. Регулярно (не реже раза в неделю) проводите проверку на наличие новых версий программного обеспечения и обновляйте антивирусные базы. В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль в Системе.

18. Не запускайте на своем компьютере программы, полученные из незаслуживающих доверия источников.

19. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

20. Не храните незашифрованные личные данные на жестком диске, так как эти данные могут быть похищены Злоумышленниками и использованы для получения доступа к Вашим счетам.

21. Если Вам пришло письмо или SMS-сообщение о выигрыше в акции, лотерее, розыгрыше удостоверьтесь в его подлинности, прежде чем отсылать деньги на чей-то счет с использованием Системы. Все акции, проводимые Банком не требуют от Клиента перевода денежных средств для получения приза.

22. Перед вводом своего логина и пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности, и информацию о Вашем последнем доступе в Систему. Например, при осуществлении переводов денежных средств в платежном сервисе Системы CONTACT CONTACT24 существует риск получения несанкционированного доступа к защищаемой информации путем использования ложных ресурсов сети Интернет лицами, не обладающими правом распоряжения этими денежными средствами, т.е. злоумышленниками.

Для реализации этого злоумышленник может создать сайт-копию сайта, например с именем www.contact24.ru, тогда как адрес подлинного сайта www.contact24.com.

Он будет выглядеть как сайт платежного сервиса, но при этом при вводе данных, они будут отправляться не в CONTACT24, а злоумышленнику. Попадание на такой сайт-двойник возможно, например, с различных внешних ссылок, на которых установлена переадресация на сайт злоумышленника.

С целью снижению указанного риска, защиты от него, а также защиты от вредоносного кода рекомендуется:

- Для входа на сайт www.contact24.com наберите в адресной строке: c o n t a c t 2 4 . c o m
- Если переходите на сайт www.contact24.com по ссылке и входите в свой электронный счет, прежде чем ввести номер телефона и пароль, необходимо проверить подлинность сайта www.contact24.com по данным SSL-сертификата. Для это нужно в адресной строке IExplorer кликнуть на символ «замок» - Отчет о безопасности – Просмотр сертификатов – вкладка Состав - Субъект – CN=www.contact24.com O=JSCB RUSSLAVBANK. В качестве удостоверяющего центра, подтверждающего принадлежность сервера www.contact24.com АКБ «РУССЛАВБАНК» (ЗАО) – организатору платежного сервиса, используется центр сертификации компании thawte, его корневые сертификаты встроены в большинство пользовательских браузеров. В целях защиты от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет Клиенту рекомендуется проверять подлинность принадлежности сервера к Системе www.contact24.com – на соответствие цифрового сертификата SSL.

23. Используйте предлагаемые Банком услуги по дополнительному информированию о входе в Систему и совершаемых операциях. Регулярно проверяйте входящую электронную почту, а также контролируйте выписки по счетам . Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

24. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе, незамедлительно смените логин и пароль и сообщите об Инциденте информационной безопасности в Службу технической поддержки Банка. Следуйте указаниям специалистов Банка.

25. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших счетах, необходимо подать заявление на временное отключение от Системы, подать заявление о преступлении в правоохранительные органы и прекратить использование (обесточить) персональный компьютер в целях сохранения доказательной базы. Если Вы пользуетесь аналогичными Системами других банков – заблокируйте их до выяснения обстоятельств происшествия. Эти учетные записи также могут оказаться скомпрометированными.

26. В сети Интернет существует много ресурсов по вопросам информационной безопасности. Регулярно ознакамливайтесь с их содержимым. Помните, угрозы постоянно видоизменяются и развиваются! Вам могут быть полезны следующие ресурсы: «Безопасный интернет»: http://www.saferinternet.ru/ «Управление «К» предупреждает: будьте осторожны и внимательны!»: http://mvd.ru/upload/site1/mvd/mvd2/mvd3/broshyura_k_01_02_20121.pdf «Вредоносные программы в интернете»: http://mvd.ru/upload/site1/mvd/mvd2/mvd3/liflets_out_1.pdf «Владельцам пластиковых банковских карт»: http://mvd.ru/upload/site1/mvd1/liflets_out_2.pdf «Пользователям интернета»: http://mvd.ru/upload/site1/mvd1/liflets_out_3.pdf «Телефонные мошенники»: http://mvd.ru/upload/site1/mvd1/liflets_out_4.pdf «Безопасный интернет – детям»: http://mvd.ru/upload/site1/mvd1/liflets_k_deti_06.pdf «Инструкция по реагированию на инциденты в системах интернет-банкинга»: http://www.group- ib.ru/images/files/Group-IB_dbo_instruction.pdf

**ПАМЯТКА ДЛЯ КЛИЕНТОВ о действиях в случае обнаружения несанкционированного списания**

В случае обнаружения несанкционированного списания со Счета Банк рекомендует Клиенту осуществить следующие действия:

1. Максимально оперативно представить письменное заявление в Банк о факте несанкционированного списания с указанием даты, суммы платежа, других известных Клиенту обстоятельств, а также с просьбой об оказании содействия в возврате несанкционированно списанных денежных средств. Указанное заявление необходимо представить в Банк на бумажном носителе в срок не позднее 2-х рабочих дней с даты устного обращения в Банк.

2. Не использовать компьютеры, которые эксплуатировались для работы в Системе. Их необходимо отключить от сети и обесточить. С высокой долей вероятности они заражены специализированным вредоносным программным обеспечением, поэтому этот шаг позволит предотвратить последующие инциденты, а также сохранить доказательства для проведения технической экспертизы.

3. Произвести смену пароля, используемого для работы с Системой в соответствии с действующим Договором. До момента смены пароля работа в Системе будет прекращена в связи с компрометацией действующих средств доступа.

4. По факту несанкционированного доступа к компьютерной информации обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по статьям 272 и 273 УК РФ в связи с созданием, использованием и распространением неустановленными лицами вредоносных компьютерных программ, повлекшим

неправомерный доступ неустановленных лиц к компьютерной информации Клиента, что, в свою очередь, привело к несанкционированному Клиентом переводу денежных средств Клиента.

5. С копией указанного заявления с приложением копии талона правоохранительного органа о приеме заявления, обратиться в Арбитражный суд с исковым заявлением в отношение банка-получателя о возврате неосновательного обогащения с ходатайством об аресте похищенной суммы денежных средств на счете получателя в банке получателя и раскрытии персональных данных получателя в целях привлечения его в качестве соответчика (гл. 60 ГК РФ) Если известны полные реквизиты получателя – физического лица, указанный иск подается в суд общей юрисдикции.

6. Копии вышеуказанных обращений в правоохранительные органы и суд с отметками о приеме необходимо предоставить в Банк для того, чтобы Банк мог оказать содействие в возврате несанкционированно списанных средств.

**Указанные действия необходимо произвести в течение 2-х рабочих дней с даты обнаружения несанкционированного списания в целях оперативного противодействия дальнейшему переводу и обналичиванию денежных средств.**