ПАМЯТКА ДЛЯ КЛИЕНТОВ

О мерах по обеспечению информационной безопасности

Уважаемый Клиент!

Коммерческий банк «Газтрансбанк» (Общество с ограниченной ответственностью), далее – «Банк», напоминает Вам о необходимости соблюдать принципы обеспечения информационной безопасности при эксплуатации программного обеспечения системы «Клиент-Банк» с целью защиты информации от воздействия вредоносного кода и исключения случаев несанкционированного доступа к рабочему месту, с целью недопущения осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.

Средства и методы защиты информации, применяемые в Банке, позволяют обеспечить необходимый уровень безопасности при осуществлении переводов денежных средств и предотвратить мошеннический вывод денежных средств со счетов клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.

Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами), а также воздействием вредоносного кода.

«Фишинг» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой «Клиент-Банк», компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО) либо на перехват информации, в том числе паролей.

1. Рекомендации по защите информации от воздействия вредоносного кода

1.1. На персональном компьютере Клиента должно быть установлено лицензионное антивирусное ПО.

1.2. Антивирусное ПО должно регулярно обновляться. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов производится антивирусным средством в автоматическом режиме.

1.3. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства.

1.4. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

1.5. При использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное ПО, разработанное специально для почтовых клиентов.

1.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т. п.) рекомендуется приостановить работу с системой до полного устранения неисправностей.

1.7. Старайтесь не использовать компьютер, с которого Вы осуществляете переводы денежных средств, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

1.8. Не открывайте файлы, полученные по электронной почте от неизвестных отправителей.

2. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

2.1. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, Банка), и предназначены для сбора конфиденциальной информации обманным путем.

2.2. Перед просмотром электронного письма всегда проверяйте адрес

отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

2.3. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.

2.4. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. В настоящем электронном письме Банк всегда приветствует Вас, обращаясь по имени и фамилии либо по названию компании. Типичное фишинговое письмо начинается с обезличенного приветствия.

2.5. Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашему счету угрожает опасность, если Вы немедленно не обновите критически важные данные.

2.6. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

3. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

3.1. Рекомендуем регулярно менять пароль для работы со своими учетными данными в системе Клиент-Банк. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

3.2. Рекомендуется хранить ключевую информацию на отчуждаемом носителе (USB-накопителе) и хранить его в сейфе или запираемом шкафу, исключив возможность несанкционированного доступа.

3.3. Банк настоятельно рекомендует использовать криптографические средства защиты (USB-токен) только во время работы с системой «Клиент-Банк». Крайне опасно подключать USB-токен к компьютеру на постоянной основе, без необходимости использования его в это же время в системе «Клиент-Банк».

3.4. В случае временного перерыва в работе с компьютером (совещание, обед и т.д.) необходимо завершить работу с программой «Клиент-Банк», убрать в сейф ключевой носитель, выключить или заблокировать компьютер.

3.5. Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные (например, сведения о Вашем банковском счете и т. д.).

3.6. В том случае, если Вы обнаружили, что Ваш пароль от банковской системы скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный

только Вам, удовлетворяющий требованиям п. 3.1

3.7. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в систему, необходимо как можно быстрее обратиться в Банк для получения инструкций по смене пароля.

3.8. Никому не разглашайте пароль от банковской системы. Банк не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли, PIN-коды и т.п.).

3.9. Запрещается записывать пароли на бумажных листках (или в текстовых файлах на компьютере), оставлять их в легкодоступных местах (на рабочем столе), передавать неуполномоченным лицам.

3.10. Не пересылайте файлы с конфиденциальной информацией для работы в банковской системе по электронной почте или через SMS-сообщения.

3.11. Рекомендуем исключить возможность физического доступа к компьютеру, с которого Вы осуществляете работу в системе, посторонних лиц.

3.12. Незамедлительно обращайтесь в Банк в том случае, если Вы получили уведомление системы об операции, которую Вы не проводили.

3.13. В случае возникновения компрометации также необходимо срочно связаться со специалистами Банка любым доступным способом и детально описать, что произошло. Это позволит Банку оперативно заблокировать доступ к Вашему счету через «Клиент-Банк».

Компрометация системы «Клиент-Банк» это:

- Любые кадровые перестановки лиц, имевших доступ к компьютеру и ключам.
- Любые Ваши подозрения в несанкционированном доступе (локально или по сети) неуполномоченных лиц к компьютеру, ключам, программе «Клиент-Банк», паролям.
- Обнаружение вируса на компьютере.
- Работа с компьютера с сетью Интернет без включенной защиты, просмотр Интернет - сайтов, не относящихся к «Клиент-Банк», установка любых программ с нелицензионных дисков или по сети.

3.14. Обращайте внимание на необычные сообщения системы и непонятное поведение компьютера. Любые запланированные сервисные работы на стороне серверов Банка всегда предваряются письмом от Управления информационных технологий. Даже в случае аварийной ситуации никакие иные предупреждения, например, в виде всплывающих окон с сообщениями о сервисных работах, не исходят от Банка и могут явиться результатом действия троянских программ или вирусов.

В случае невозможности подключения к системе «Клиент-Банк», наличия ошибки с сообщением о техническом сбое или проводимых обновлениях Системы, не заявленных Банком, а также в случае обнаружения несанкционированных входов в Систему (успешных или неуспешных), срочно свяжитесь со специалистами Банка любым доступным способом.

Номера телефонов Контакт - центра ООО КБ «ГТ банк»: +7(861)279-17-46, +7(861)279-03-05