Приложение 10

к Правилам предоставления дистанционного банковского обслуживания
с использованием системы Интернет-Банк «Частный клиент» в Банке «Таврический» (ПАО)

Рекомендации по снижению рисков при работе системы Интернет-Банк «Частный клиент»

Для снижения рисков убытков в результате неправомерного использования Системы необходимо выполнять следующие рекомендации:

1. Обеспечить хранение информации о Пароле способом, делающим Пароль недоступным третьим лицам, в том числе Клиенту запрещается в ответ на телефонные звонки, SMS или e-mail сообщения, поступившие от любых лиц, в том числе представившихся сотрудниками Банка, сообщать Логин и (или) Пароль, выполнять рекомендации, связанные с вводом каких-либо данных на любых страницах, открытых браузером, или с повторным входом в Систему, а также незамедлительно уведомлять Банк о Компрометации Пароля в порядке, предусмотренном пунктом 4.2 Правил. Несоблюдение вышеуказанных требований безопасности является нарушением порядка использования Системы.
2. Ограничивать доступ третьих лиц к информации об SMS-коде в период соединения с Системой.
3. Обязательно проверять текст SMS-сообщений, содержащих SMS-код с деталями выполняемой операции. Если в SMS-сообщении указан код для операции, которую не совершал Клиент или Клиенту предлагается его ввести/назвать, чтобы отменить якобы ошибочно проведенную по счету Клиента операцию, ни в коем случае нельзя вводить данный код в Системе и не называть его, в том числе сотрудникам Банка.
4. Заблокировать (заменить) SIM-карту, в случае утери мобильного телефона, на который приходят SMS-сообщения с SMS-кодом.
5. Прекратить работу в Системе в случае поступления нестандартных запросов.
6. Устанавливать мобильные приложения Банка только из авторизированных магазинов App Store и Google Play. Перед установкой приложения убедиться, что их разработчиком является Center of Financial Technologies.
7. Использовать лицензионное программное обеспечение (операционную систему, приложения), в том числе на мобильном телефоне, полученное из проверенных и надежных источников, своевременно устанавливать все обновления программного обеспечения, повышающие его безопасность.
8. Использовать лицензионную антивирусную программу, в том числе на мобильном телефоне, своевременно обновлять антивирусные базы данных, проводить периодическое сканирование своего компьютера.
9. Установить и настроить персональный брандмауэр (firewall) на компьютере, в случае если компьютер работает в сети.
10. Помнить, что при вводе личной информации любой веб-адрес в адресной строке Системы должен начинаться с «https». Если в адресе не указано «https», это значит, что Клиент находится на незащищенном веб-сайте, и вводить данные нельзя, так как они будут переданы в открытом (незашифрованном) виде и могут быть перехвачены.
11. Отключить функцию автозаполнения в установках браузера.
12. Использовать систему фильтрации ложных web-узлов (антифишинг).
13. Не использовать права администратора при отсутствии необходимости. В повседневной практике входить в Систему как пользователь, не имеющий прав администратора.
14. Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
15. Запретить в межсетевом экране соединение с интернет по протоколам FTP, SMTP. Разрешить соединение SMTP только с конкретными почтовыми серверами, на которых зарегистрированы электронные почтовые ящики Клиента.
16. Не открывать электронные почтовые сообщения и сообщения систем мгновенного обмена сообщениями, в том числе вложенные в них файлы, поступающие от неизвестных отправителей.
17. Не оставлять без присмотра свой компьютер, мобильный телефон в период соединения с Системой.
18. Использовать кнопку «Выход» после окончания работы в Системе.
19. Выполнять условия Правил, в том числе пункт 2.6.6 Правил.