## Рекомендации по информационной безопасности для клиентов «СОЦИУМ-БАНК» (ООО), использующих систему HandyBank

Система HandyBank позволяет пользователям осуществлять операции с денежными средствами, находящимися на соответствующих счетах. Работа с денежными средствами должна выполняться с максимальной осторожностью. Выполнение нижеследующих рекомендаций поможет сделать взаимодействие с системой HandyBank более безопасным.

1. Общие рекомендации
	1. Для доступа в учетную запись на личном компьютере установите сложный пароль. Общие правила составления пароля:
2. Длина пароля должна быть не менее 7 символов.
3. Пароль должен содержать различные символы: цифры, заглавные и строчные буквы, специальные символы: !, ), $ и т.п.
4. Придумайте свой пароль самостоятельно и никому его не сообщайте.
5. Постарайтесь запомнить свой пароль. Если Вы записали пароль на бумаге, храните его в месте, недоступном для посторонних лиц, если Вы храните пароль на компьютере, то делайте это в неявном виде.
6. Обязательно смените пароль в том случае, если он стал известен постороннему лицу.
7. Не используйте в качестве пароля: последовательности символов состоящие из одних цифр (в том числе даты, номера телефонов и т.п.); последовательности повторяющихся букв или цифр; подряд идущие в раскладке клавиатуры или в алфавите символы; имена и фамилии.

К паролю для мобильного устройства должны применяться все те же правила, что и к обычному, за исключением некоторых особенностей, таких как отсутствие возможности использования букв, длина пароля и т.п.

* 1. Установите на свой компьютер/мобильное устройство лицензионное антивирусное программное обеспечение. Регулярно производите его обновление и полную антивирусную проверку компьютера/мобильного устройства, а также обновление операционной системы и используемых программ (браузера и иных прикладных программ). Используйте программное обеспечение только из проверенных и надежных источников.
	2. Удаляйте конфиденциальную информацию в случае передачи компьютера/мобильного устройства другим лицам. Воспользуйтесь функцией восстановления заводских настроек.
	3. Сверяйте данные об операциях, указанные в полученных от смс-сообщениях, с данными по фактически совершенным операциям на предмет выявления несанкционированных операций.
	4. После окончания работы в системе HandyBank обязательно завершайте сеанс, используя кнопку «Завершить сеанс».
	5. Ни при каких условиях не сообщайте информацию о Вашем логине, пароле, одноразовых паролях, используемых для подтверждения операций, и иных сведениях, используемых для авторизации в каналах дистанционного обслуживания никому, включая сотрудников Банка.
1. Рекомендации по использованию Интернет-банка HandyBank
	1. Прежде чем пройти авторизацию в Интернет-банке, убедитесь, что соединение происходит в защищенном режиме с использованием протокола HTTPS (появляется буква S в адресной строке: https://socium-bank.handybank.ru), удостоверьтесь в правильности сертификата SSL-соединения. Ссылка для входа в Интернет-банк указана на сайте Банка www.socium-bank.ru.
	2. Не пользуйтесь Интернет-банком в общедоступных местах, на компьютерах, безопасность которых вызывает сомнения (например, в Интернет-кафе, чужой компьютер). Если Вы все же заходили с чужого компьютера, смените пароль для входа в Интернет-банк с Вашего персонального компьютера, как только будет такая возможность.
	3. Установите и используйте персональный брандмауэр для входа в Интернет, это позволит предотвратить несанкционированный доступ к информации на Вашем компьютере.
	4. Не пользуйтесь Интернет-банком на компьютере, который используется под учетной записью, имеющей права администратора системы, а также, если имеется подозрение, что компьютер заражен вирусной программой. Симптомы заражения: на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы; произвольно, без участия пользователя, на компьютере запускаются какие-либо программы; на экран выводятся предупреждения о попытке какой-либо из программ выйти в Интернет, хотя пользователь этого не инициировал; частые зависания и сбои в работе компьютера, медленная работа компьютера при запуске программ; невозможность загрузки операционной системы, исчезновение файлов и каталогов или искажение их содержимого.
2. Рекомендации по использованию Мобильного банка HandyBank
	1. Устанавливайте приложение Мобильный банк и его обновления только из приложений Apple AppStore, Google Play Market. Ссылки для установки указаны на сайте Банка http://socium-bank.ru/person/sistema-internet-bankinga-handybank/.
	2. Не «взламывайте» систему защиты iPhone (jailbreak) и не открывайте «root» доступ для устройств на операционной системе Android, так как это делает уязвимым Ваше мобильное устройство.
	3. Подключите элементы дистанционного управления (для дистанционной блокировки и дистанционного удаления данных с мобильного устройства при утрате мобильного устройства).
	4. При утрате мобильного телефона (иного устройства), на который подключена услуга смс-информирования, направляются одноразовые пароли или на которое установлено приложение Мобильный банк, незамедлительно обратитесь к своему оператору сотовой связи для блокировки SIM-карты и в Банк для блокировки доступа к системе HandyBank.
	5. При смене номера телефона, обратитесь в Банк для внесения соответствующих изменений.

Не стоит забывать, что перечисленные выше меры повышают степень защиты Вашей конфиденциальной информации и как следствие Ваших денежных средств, однако не являются полной гарантией защиты от мошеннических действий.