Рекомендации клиентам по обеспечению безопасности при работе с системой Интернет-банк для ФЛ

Правила выбора секретного кода:

1. Устанавливайте свой секретный код самостоятельно, без участия третьих лиц.

2. Секретный код должен содержать не менее 4 различных символов. Чем сложнее будет код, тем труднее его будет подобрать.

3. Обязательно смените секретный код в том случае, если он стал известен третьему лицу.

4. Не используйте в качестве секретного кода:

- последовательности символов состоящие из одних цифр (в том числе даты, номера

телефонов и т.п.);

- последовательности повторяющихся цифр;

- подряд идущие в раскладке клавиатуры символы.

Не сообщайте третьим лицам идентификатор, секретный код и динамические пароли для входа в систему

Работники Банка (техническая поддержка, служба безопасности и т.д.) никогда не обращаются к Клиентам с предложениями: назвать секретный код, динамический пароль, полные реквизиты банковских карт или перечислить денежные средства на какой-либо счет.

Никогда не сообщайте в ответ на телефонные звонки, SMS или e-mail сообщения, поступившие, якобы, от работников Банка или иных третьих лиц, Вашу конфиденциальную информацию: Ваш секретный код доступа в систему Интернет-банк, динамический пароль, а также номер вашей банковской карты, ее CVC/CVV- и ПИН-коды.

Не записывайте идентификатор и секретный код там, где доступ к нему могут получить посторонние (включая записную книжку Вашего мобильного телефона или компьютера).

При утере мобильного телефона Вы подвергаетесь значительному риску со стороны злоумышленников. Будьте особенно бдительны и не оставляйте без Вашего внимания свой мобильный телефон.

Регулярно обновляйте антивирус и операционную систему

Используйте только лицензионную антивирусную программу!
Рекомендуем использовать решения от ведущих компаний в данной сфере, например:
Антивирус Касперского
Eset NOD32
Dr.web

Приобретайте программное обеспечение только в специализированных магазинах или с официальных сайтов производителей!

Ни в коем случае не качайте сомнительные антивирусы из интернета, которые сами по себе могут содержать вредоносные файлы!

Позвольте антивирусу и операционной системе обновляться в автоматическом режиме.

Рекомендуется полная еженедельная проверка компьютера на наличие вирусов.

Проверяйте антивирусом сменные носители (USB-flash, USB-hdd и прочее) перед началом использования.

Вирусные программы могут запоминать и отсылать всю информацию злоумышленникам. Если у вас есть подозрение, что ваш логин и пароль украдены, как можно быстрее смените ваш пароль в Интернет-банке.

Не открывайте письма от неизвестных отправителей

При работе с электронной почтой не доверяйте письмам от неизвестных отправителей, они могут содержать в себе вирусы!

Не переходите по ссылкам, приведенным в таких письмах. Не открывайте приложенные файлы.

Настоятельно рекомендуется все файлы, пришедшие по электронной почте, в отдельном порядке проверять антивирусом перед открытием

Начинайте работу в системе Интернет-банк только после того как убедитесь, что Вы находитесь на стартовой странице интернет-банка

Напоминаем, что вход в Интернет-банк осуществляется по адресу https://i.tagilbank.ru/

Убедитесь, что при входе на страницу адресная строка в Вашем браузере выделилась зеленым цветом (для Internet Explorer). Дополнительно в адресной строке должна появиться кнопка с символом "замок", в которой отображается английское наименование банка ОАО «Тагилбанк» – JSC Tagilbank. Это признак того, что установлено безопасное соединение, и канал передачи данных шифруется по протоколу SSL.

Обращаем Ваше внимание, что сайты, визуально напоминающие сайт интернет-банка, могут быть созданы мошенниками специально для незаконного получения Вашей персональной информации. Будьте бдительны!

Не работайте с системой Интернет-банк в интернет-кафе или на других компьютерах общего пользования

Не рекомендуется заходить в систему из мест большого скопления людей, например, «Интернет-кафе». Риск утечки информации значительно возрастает.

Не забывайте корректно завершать работу с системой Интернет-банк

Используйте для этого пункт меню «Выход».

Не посещайте сомнительные сайты

Чтобы минимизировать вероятность заражения компьютера вирусами, постарайтесь использовать только проверенные сайты, необходимые для работы.

Неофициальные новостные сервисы, развлекательные порталы, социальные сети, и прочие сайты, могут содержать вирусы. Даже разовый переход из поисковой системы по ссылке на сомнительный сайт может стать причиной заражения!

Никогда не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов!

Используйте только официальные контактные данные для связи с банком

Актуальную контактную информацию вы всегда можете посмотреть на нашем сайте http://tagilbank.ru/

Банк никогда:

- не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные (ФИО, данные документа, удостоверяющего личность, номер мобильного телефона, информацию банковской карты, CVV, ПИН, кодовое слово и пр.);

- не отправляет сообщения с формой для ввода Ваших персональных данных;

- не просит Вас зайти в личный кабинет системы Интернет-банк по ссылкам в письмах.

Банк обращает Ваше внимание на то, что выполнение вышеописанных рекомендаций позволит существенно минимизировать риски несанкционированного списания денежных средств с ваших счетов.