Памятка пользователя системы «Интернет – Банк»

Уважаемый клиент!

Вы стали пользователем системы «Интернет – Банк». Пожалуйста, внимательно прочтите эту краткую памятку пользователя.

1. Запустите любой интернет обозреватель Вашего компьютера и перейдите на страницу входа в систему «Интернет – Банк».

2. Введите Ваш логин и пароль. Временный Пароль для входа Вы получили sms-сообщением на номер мобильного телефона. Система «Интернет – Банк» предложит Вам изменить пароль на постоянный автоматически.

3. В системе «Интернет – Банк» отображается информация по Вашим счетам. Чтобы изучить историю операций по своему счету, запросите выписку, воспользовавшись ссылкой: **«*Выписка по счету*»**.

4. Через систему «Интернет – Банк» можно оплатить услуги более чем 5000 поставщиков услуг по всей России. Это сотовая связь, телевидение и интернет, коммунальные услуги и многое другое. Для оплаты данных услуг используйте раздел: **«*Оплата услуг*»**. Если вы планируете регулярно совершать оплату за какую-либо услугу, удобно ее сохранить в раздел: **«*Мои услуги*»**.

5. В разделе: **«*Платежи, переводы*»** Вы сможете совершить перевод между счетами или отправить платеж по любым известным Вам произвольным реквизитам.

6. В разделе: ***«Заявления, сообщения»*** Вы сможете отправить сообщение в Банк, выбрав тип сообщения и заполнив предлагаемую форму.

7. Обратите внимание! В целях безопасности в системе «Интернет – Банк» предусмотрено использование разовых секретных паролей для подтверждения платежей. Запросите пароль после формирования платежа, нажав на кнопку: «Получить пароль». Пароль Вы получите sms-сообщением на номер мобильного телефона.

Рекомендации об организационных мерах, необходимых для обеспечения безопасной работы в сервисе «FAKTURA.RU» на компьютере клиента:

1. Запомните, что для входа в Интернет-банк Вам требуется вводить только Ваш логин и пароль!

2. Никогда и ни при каких обстоятельствах не сообщайте никому свои пароли для входа в систему «Интернет-Банк» или для подтверждения платежей.

3. Обязательно сверяйте текст sms-сообщений, содержащий пароль, с деталями выполняемой Вами операции. Если в sms-сообщении указан пароль для платежа, который Вы не совершали или Вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по Вашему счету платеж, ни в коем случае не вводите его в систему «Интернет-Банк» и не называйте его, в том числе сотрудникам Банка.

4. В случае утери мобильного телефона, на который приходят sms-сообщения с разовым паролем, немедленно заблокируйте sim-карту.

5. Запишите контактный телефон Вашего Банка в адресную книгу или запомните его. В случае если в личном кабинете системы «Интернет-Банк» Вы обнаружите телефон, отличный от записанного, в особенности, если Вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в Банк по ранее записанному Вами телефону. Также для этих целей подойдет телефон, указанный на вашей банковской карте «Золотая Корона» (при наличии).

6. Устанавливайте мобильные приложения Faktura.ru только из авторизованных магазинов App Store и Google Play. Перед установкой приложения убедитесь, что их разработчиком является Center of Financial Technologies. Используйте антивирусное программное обеспечение, в случае, если оно доступно для Вашего телефона/смартфона.

7. Избегайте регистрации номера Вашего мобильного телефона, на который приходят sms-сообщения с разовым паролем, в социальных сетях и других открытых источниках.

Общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на компьютерах:

1. Используйте только доверенные компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным программным обеспечением (далее – «ПО») и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного ПО, своевременно обновляйте лицензионную операционную систему и браузеры.

2. При вводе личной информации, ПОМНИТЕ, что любой веб-адрес в адресной строке Интернет-банка должен начинаться с «https». Если в адресе не указано «https», это значит, что Вы находитесь на незащищенном веб-сайте, и вводить данные нельзя.

3. Используйте виртуальную клавиатуру для ввода пароля.

4. Будьте внимательны: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в банк с целью оперативного блокирования доступа!

5. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

6. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора.

7. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагировать на ошибки.

8. Запретите в межсетевом экране соединение с Интернет по протоколам FTP, SMTP. Разрешите соединения SMTP только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики.

9. Не давайте разрешения неизвестным программам выходить в Интернет.

10. При работе в Интернете не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.

Желаем Вам приятной работы!