Венецбанк
основан в 1990 г.

Акционерное общество Банк «Венец»
432071, г. Ульяновск, ул. Марата, д.19; тел. / факс (8422) 32 62 84,
ИНН 7303024532, ОГРН 1027300000166, БИК 047308813
к/с № 30101810200000000813 в Отделении по Ульяновской
области Волго-Вятского главного управления ЦБ РФ
Многоканальная линия 8 800 707 55 99, www.venets-bank.ru,
e-mail: office@venets-bank.ru

ПАМЯТКА ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ ЭЛЕКТРОННЫХ СЕРВИСОВ

При работе с Электронной подписью/Аналогом собственноручной подписи:

Запомните, что для входа в сервис Личный кабинет вам требуется вводить только ваш логин и пароль. Не нужно вводить номер вашего мобильного телефона, номер вашей банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации в сервисе Личный кабинет.

Никогда и ни при каких обстоятельствах не сообщайте никому свои пароли для входа в сервис Личный кабинет или для подтверждения платежей, а также номера ваших карт и CVV2/CVC2 коды и иные Аутентификационные данные, используемые Вами в рамках ДБО.

Обязательно сверяйте текст сообщений, содержащий пароли (коды), с деталями выполняемой Вами операции.

Если в сообщении указан пароль (код) для совершения операции, которой 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 сервисе Личный кабинет и не называйте его, в том числе сотрудникам/представителям Банка.

В случае утери Абонентского устройства, на который приходят разовые пароли, немедленно заблокируйте его (используемую SIM-карту), войдите в альтернативную версию сервиса Личный кабинет (Электронного сервиса) и удалите телефон из списка зарегистрированных устройств для получения PUSH/СМС-сообщений.

Запишите контактный телефон Банка в адресную книгу или запомните его. В случае если в сервисе Личный кабинет 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 Карте.

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 Абонентского устройства.

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

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

Используйте только доверенные компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным программным обеспечением и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного программного обеспечения, своевременно обновляйте лицензионную операционную систему и браузеры.

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.

Используйте виртуальную клавиатуру для ввода пароля.

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

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

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

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.

Не давайте разрешения неизвестным программам выходить в Интернет.

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

Не отвечайте на подозрительные звонки, электронные письма и сообщения из любых систем мгновенного обмена сообщениями, которые запрашивают конфиденциальную информацию. Банк никогда не обращается к клиентам с подобными просьбами.

Помните! Банк (в том числе Технологические партнеры) не проводит тестовых операций с Клиентами и не обращается к Клиентам за помощью в совершении операций.

Будьте внимательны: в случае возникновения подозрений на мошеннические (неправомерные) действия, ни в коем случае не проводите никаких действий (операций), сообщите о произошедшем в Информационный центр Банка как можно максимально быстро банк с целью оперативного реагирования на ситуацию!