Руководство для клиентов «Приорбанк» ОАО, пользующихся системой «Клиент-Банк» для юридических лиц и индивидуальных предпринимателей.

Данная информация предназначена для того, чтобы помочь клиентам обеспечить должную безопасность передачи данных при использовании системы «Клиент-Банк».

- Для работы в Клиент-банке рекомендуется использовать отдельный компьютер.
- Не рекомендуется использовать на компьютере нелицензированное программное обеспечение (операционную системы, иное программное обеспечение).
- На компьютере необходимо работать с минимальными полномочиями прав пользователя.
- Не желательно пользоваться внешней (интернет) электронной почтой на данном рабочем месте. При необходимости использования – предпринять все меры внимательности и предосторожности для противодействия намерениям злоумышленников по заражению компьютера (обращать внимание если неизвестный адресат, вредоносные вложения и ссылки).
- Операционная система на компьютере с Клиент-банком должна своевременно обновляться (актуальное, поддерживаемое разработчиком лицензионное ПО).

- Установите на компьютере, который Вы используете для работы с системой «Клиент-Банк», антивирусное программное обеспечение и межсетевой экран (firewall), настройте их в соответствии с рекомендациями поставщика.
- Регулярно устанавливайте обновления безопасности, включая антивирусные сигнатуры.
- Никогда и ни при каких обстоятельствах никому не передавайте свои секретные параметры (Имя пользователя, пароль для входа, ЭЦП).
- Носитель с ключом ЭЦП должен использоваться ТОЛЬКО в момент подписания документа. ПОСЛЕ ПОДПИСАНИЯ НОСИТЕЛЬ ДОЛЖЕН БЫТЬ ИЗВЛЕЧЕН ИЗ КОМПЬЮТЕРА!

Ознакомьтесь с Политикой безопасности, принятой в «Приорбанк» ОАО и описанной ниже.

- Рекомендуется сменить стандартный пароль администратора после первого входа.
- Рекомендуется создавать отдельные учетные записи для пользователей с разграничением прав и задач.
- Придумайте себе надёжный Пароль.
- Не сохраняйте свои Имя пользователя, пароль для входа на компьютере/цифровом носителе, доступ к которому имеют другие лица.
- Не используйте для Клиент-Банка Имя пользователя и пароль, которые уже используются Вами для авторизации на сайтах социальной сети (интернет-магазины, чаты и другие).
- Не используйте бесплатные WiFi-точки для доступа к своим аккаунтам (ввода паролей) и совершения платежей.

Политика безопасности

Никто из работников банка, лиц и организаций, связанных с банком, или кто бы то ни было никогда и ни при каких обстоятельствах не может и не должен просить, либо требовать предоставления конфиденциальной информации, касающейся электронных каналов обслуживания. К конфиденциальной информации относятся:

1. Имя пользователя,
2. Пароль на вход в систему,
3. ЭЦП,
4. Номера карточек, PIN-коды и другая информация, размещенная на пластиковых карточках.

Разглашение указанной информации может создать предпосылки к осуществлению в отношении Вас мошеннических действий и привести к финансовым и моральным потерям, как для Вас, так и для Банка.

В случае обращения к Вам по телефону, посредством почтовых или электронных рассылок, личного либо любого другого запроса на предоставление указанной информации, пожалуйста, немедленно сообщите об этом сотрудникам банка:

по телефонам: +375 17 289-90-87, 487 (Velcom, МТС или life:)),187 по г. Минску, +375 17 289-92-92 (круглосуточно),

на e-mail: fraud@priorbank.by или prior@priorbank.by

по факсу: +375 17 289-91-91 либо любым другим способом.

Выбор надежного пароля

Надежный пароль — это такой пароль, который трудно угадать, но легко запомнить. Слишком сложные пароли, скорее всего, будут записаны и вследствие этого станут ненадёжными.

Чтобы пароль было трудно угадать, он должен обладать специфическими синтаксическими характеристиками.

При выборе пароля желательно следовать следующим правилам:
. Пароль должен состоять, по меньшей мере, из 8 знаков (чем длиннее пароль и больший набор символов, тем лучше);
. Пароль должен представлять собой сочетание заглавных и строчных букв латинского алфавита, цифр и, если возможно, спецсимволов; Не следует выбирать в качестве пароля (чтобы исключить вероятность определения пароля путем перебора) слова, содержащихся в стандартных словарях: имена, сокращения, слова, взятые из словарей (включая иностранные словари) или логические последовательности;
. Пароль недолжен содержать в себе повторяющихся последовательностей знаков (например, в слова «access» содержится больше двух идентичных знаков, следующих друг за другом), очевидных последовательностей или узоров, образуемых символами, нанесенными на клавиши клавиатуры (например, asdfghjkl или erdfcv).
. Перемежайте короткие слова цифрами или специальными символами, например, this:Is:One.good:PassWord или 3Doggiesareloud!
. Создавайте аббревиатуру из начальных букв слов, составляющих предложение, которое вы можете без труда запомнить. Например, вы можете составить аббревиатуру Tpftssivhtc из начальных букв слов в предложении «This password for the security system is very hard tocrack».