РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ ИНТЕРНЕТ-БАНКА BALTIC INTERNATIONAL BANK И МОБИЛЬНОЙ АППЛИКАЦИИ BIB И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ, ПЛАНШЕТОВ И СМАРТФОНОВ

Для безопасного использования интернет-банка и мобильной аппликации BIB, пожалуйста, ознакомьтесь и соблюдайте рекомендации по защите персональных компьютеров, планшетов и смартфонов, а также рекомендации по безопасному использованию интернет-банка Baltic International Bank и мобильной аппликации BIB ("***B Online***").

Защита персонального компьютера под управлением операционной системы Windows, MacOS, Linux

- Устанавливайте программное обеспечение (ПО) только от надежных поставщиков;
- На устройстве доступа необходимо установить антивирусное и анти-шпионское ПО;
- Для защиты от вредоносного, шпионского и нежелательного ПО, поддерживайте актуальность антивирусного ПО, настройте ПО на автоматическое обновление, и выполнение полных проверок систем на регулярной основе. Напоминаем, что использование антивирусного ПО не дает полной гарантии защиты;
- Регулярно устанавливайте все новые обновления ПО, используя функцию автоматического обновления. Убедитесь, что всё ПО, в том числе операционная система и прикладное ПО (такое как Microsoft Office, Adobe Acrobat, QuickTime, iTunes, браузеры Chrome, Egde, Firefox и т.п.), обновлены до последней актуальной версии;
- Установите отдельный или включите встроенный в операционную систему локальный брандмауэр (firewall), сконфигурировав его таким образом, чтобы подключение с интернета к Вашему компьютеру было невозможно;
- Для доступа к интернет ресурсам на Вашем компьютере следует настроить непривилегированную учетную запись (пользователь, под которым Вы подключаетесь к своему компьютеру не должен обладать правами администратора);
- Не пользуйтесь «пиратским» ПО;
- Создавайте резервные копии важных данных.

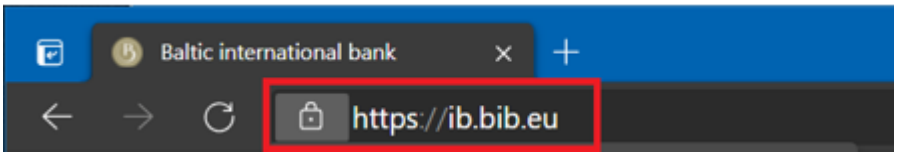
Защита планшетов и смартфонов

- Используйте разрешенные источники для загрузок (Apple App store для iPad и iPhone, Google Play для Android);

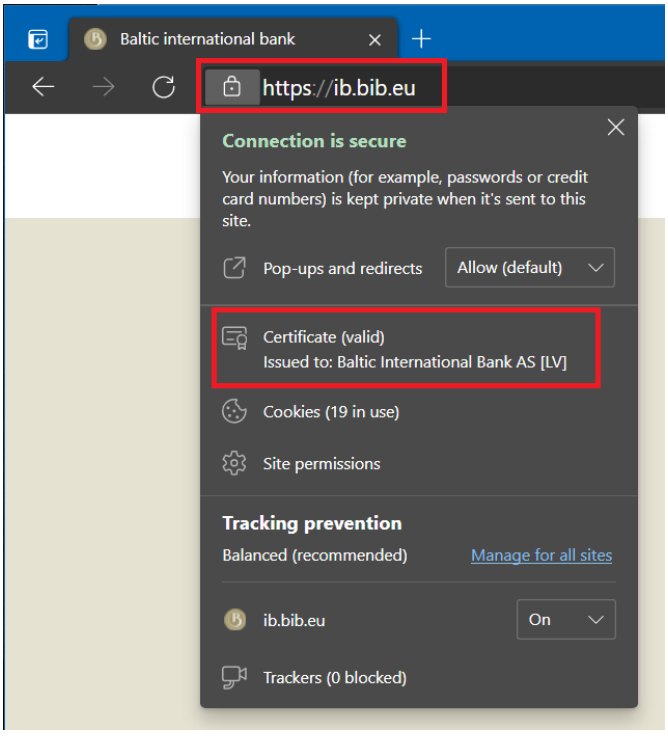
- Включите автоматическое обновление ПО, установленного на Вашем устройстве, следите и регулярно обновляйте до новейших версий операционную систему Вашего устройства;
- Не проводите на своем устройстве несанкционированные изменения для обхода ограничений и средств защиты, установленных производителем (jailbreake, root access);
- Активируйте защиту доступа к своему персональному устройству (PIN-код, биометрия);
- Создавайте резервные копии данных всего устройства.

Рекомендации по безопасному использованию интернет-банка Baltic International Bank и мобильной аппликации BIB (“*B Online*”)

- Перед тем как ввести коды доступа, убедитесь, что Вы находитесь на подлинной странице интернет-банка Baltic International Bank. Адрес должен начинаться с https://ib.bib.eu/.
- Соединение должно быть зашифровано, о чем свидетельствует наличие пиктограммы замка в адресной строке браузера:



- Подлинность сертификата можно проверить, нажав на пиктограмму замка. В настоящее время издателем сертификата является фирма DigiCert:



- Не пользуйтесь публично доступными компьютерами (например, библиотеки, интернет-кафе, и т.п.);
- Не подключайте свои портативные устройства к бесплатным и неизвестным Wi-Fi сетям;
- Не соглашайтесь с предложением веб-браузера или других систем, сохранить имена входа и пароли;
- Осуществляйте правильное завершение сеанса работы с интернет-банком. Простого закрытия активного окна недостаточно, используйте пункт меню «ВЫЙТИ»;
- Не используйте один и тот же компьютер/планшет/смартфон, который вы используете для работы с интернет-банком, совместно с третьими лицами (в том числе Вашими родственниками или детьми);
- Никогда не используйте гиперссылки, чтобы попасть на сайт интернет-банка, не доверяйте ссылкам, полученным из поисковых систем и электронной почты;
- Baltic International Bank **никогда никаким образом** (по электронной почте, SMS/MMS, телефону) не запрашивает у своих клиентов коды доступа, пароли, PIN-коды и т.п.;
- Запрещено разглашать кому-либо код пользователя, пароль, PIN-код и другую идентифицирующую Вас информацию;
- Храните средства авторизации интернет-банка (имя пользователя, Digipass, PIN-код, активационные ключи) в безопасности;

Если у Вас возникло подозрение на несанкционированное использование интернет-банка или несанкционированный доступ третьих лиц к Вашим средствам авторизации и другой идентифицирующей Вас информации, незамедлительно сообщите об этом своему персональному банкиру.