Рекомендации

о мерах безопасного использования системы дистанционного банковского обслуживания «HandyBank»

клиентами АО КИБ «ЕВРОАЛЬЯНС» - физическими лицами

Уважаемые клиенты!

Настоящие рекомендации разработаны АО КИБ «ЕВРОАЛЬЯНС» (далее – Банк) в целях:

- предотвращения хищения денежных средств, находящихся на Ваших банковских счетах при осуществлении расчетов с использованием системы дистанционного банковского обслуживания (далее – ДБО),
- доведения до клиентов Банка информации о возможных рисках получения несанкционированного доступа к системам ДБО с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими средствами, и о рекомендуемых мерах по снижению рисков проведения злоумышленниками несанкционированных платежей.

При работе с системой ДБО «HandyBank» рекомендуем:

1. **Соблюдать ОБЩИЕ МЕРЫ БЕЗОПАСНОСТИ при работе с системой ДБО:**
   - Не работайте с системой ДБО через публичные сети (кафе, рестораны, магазины, иные общественные места).
   - Используйте только собственные специально выделенные электронные устройства (компьютер, ноутбук, планшет, смартфон). Не используйте чужие электронные устройства.
   - Прежде чем ввести пароль в системе ДБО, убедитесь, что соединение установлено именно с сервером Банка, в адресной строке браузера должен отображаться адрес https://euroalliance.handybank.ru/. Обратите внимание, что адрес начинается с httpS:// («s» означает secured — защищенный). Рядом с адресной строкой Вы можете нажать на значок «замок» и проверить информацию о безопасности соединения с данным сайтом.
   - Перед началом работы в системе «HandyBank» выполните проверку компьютера или другого электронного устройства, с которого осуществляется работа с системой ДБО, на наличие вредоносных программ. При возникновении любых подозрений на компрометацию электронного устройства, с которого осуществляется работа с системой ДБО (наличие вредоносных программ), незамедлительно обратитесь в Банк по телефону: **(4932) 41-22-38, 8-800-700-92-22** и временно заблокируйте Вашу учетную запись в системе ДБО. Далее следуйте инструкциям сотрудников Банка.
   - При возникновении малейших подозрений и странностей в работе системы, в случае любых изменений в привычных для Вас процессах установления соединения с системой ДБО, немедленно обратитесь в Банк по телефону: **(4932) 41-22-38, 8-800-700-92-22.**
   - Регулярно контролируйте состояние своих счетов в системе ДБО и незамедлительно сообщайте обо всех подозрительных или несанкционированных

Вами финансовых операциях работникам Банка по телефону **(4932) 41-22-38, 8-800-700-92-92.**

- В случае сбоев в работе компьютера или иного устройства, с которого осуществляется работа с системой ДБО, его поломки во время сеанса работы с системой ДБО, или сразу после завершения сеанса работы (проблемы с операционной системой, жестким диском и т.п.), незамедлительно обратитесь в Банк по телефону **(4932) 41-22-38, 8-800-700-92-92** и убедитесь, что от Вашего имени не производились несанкционированные списания денежных средств с Ваших банковских счетов.
- Не оставляйте без присмотра и не передавайте посторонним лицам мобильный телефон, используемый Вами для получения Handy-кода.
- В случае если у Вас неожиданно перестала работать СИМ-карта телефона, оперативно обратитесь к своему оператору сотовой связи для блокировки абонентского номера и замены СИМ-карты, а также обратитесь в Банк для выявления возможных несанкционированных операций.
- При потере телефона/смене номера телефона, который использовался в HandyBank, обязательно обратитесь в Банк.
- Пользуйтесь дополнительными возможностями системы HandyBank в части обеспечения безопасности (управление лимитами операций, ограничение списка получателей и т.п.). Узнайте подробнее об этих возможностях в управлении банковских карт по телефону **(4932) 41-22-38**.

2. Обеспечить БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО УСТРОЙСТВА, которое используется для работы с ДБО (компьютер, ноутбук, планшет, смартфон):

- Используйте для работы в системе ДБО специально выделенное для этих целей устройство (компьютер, ноутбук, планшет, смартфон).
- Применяйте на Ваших электронных устройствах только лицензионное системное, прикладное и антивирусное программное обеспечение.
- Своевременно устанавливайте обновления программного обеспечения, выпускаемого его производителями.
- Используйте актуальную версию антивирусной программы. Своевременно, желательно в автоматическом режиме, устанавливайте обновления всех компонентов и информационных баз антивирусной программы.
- Еженедельно осуществляйте полную проверку электронного устройства, с которого осуществляется работа с системой ДБО, на наличие/отсутствие вредоносного кода.
- Установите на Вашем компьютере или другом электронном устройстве, с которого осуществляется работа с системой ДБО, специализированные средства безопасности – персональные межсетевые экраны (firewall), а также средние или высокие параметры безопасности и конфиденциальности установленного Интернет-браузера.
- Включите систему фильтрации ложных web-узлов (антифишинг) в своем Интернет-браузере, если Интернет-браузер её не имеет – обновите браузер.
- При работе в сети Интернет никогда не соглашайтесь на установку каких-либо дополнительных программ или компонентов, если Вы не уверены в их предназначении.

- Не открывайте письма и вложенные в них файлы, полученные по электронной почте от неизвестных Вам отправителей. Не переходите по ссылкам, содержащимся в подобных письмах. Открывайте файлы или интернет-ссылки, пришедшие по электронной почте даже от знакомых Вам людей только если они присланы Вам по Вашей просьбе. Помните, что сообщение может быть отправлено от имени Вашего знакомого человека вредоносной программой, захватившей контроль над его компьютером или учетной записью в социальной сети.
- Исключите посещение непроверенных Интернет-сайтов.
- В случае появления предупреждений Интернет-браузера о перенаправлении Вас на другой сайт при подключении к системе ДБО, немедленно обратитесь в **Банк по телефону: (4932) 41-22-38, 8-800-700-92-22.**

3. ИСКЛЮЧИТЬ ДОСТУП ПОСТОРОННИХ ЛИЦ К ЭЛЕКТРОННОМУ УСТРОЙСТВУ, с которого осуществляется работа с системой ДБО:

- Не устанавливайте на устройстве, с которого осуществляется доступ к HandyBank, программы удаленного администрирования и доступа к данному устройству.
- Работайте на компьютере или другом электронном устройстве, на котором установлена система ДБО, только с правами пользователя (не администратора). Не отключайте UAC (user account control, контроль учетных записей пользователей) в системе Windows. Невыполнение этих требований существенно увеличивает риск заражения вредоносными программами. Учетная запись «Гость» на электронном устройстве, с которого осуществляется работа с системой ДБО, должна быть выключена.

4. ЗАЩИТИТЬ КОД ДОСТУПА К СИСТЕМЕ ДБО от хищения и копирования:

- Смените свой код доступа (handy-пароль) при первом входе в систему ДБО.
- Запомните код доступа. Никогда не разглашайте его и не записывайте его в местах, доступных посторонним лицам (в т.ч. родственникам).
- Периодически (не реже одного раза в месяц) меняйте код доступа к системе ДБО.
- Никому не сообщайте сведения о коде доступа, в т.ч. сотрудникам Банка. Помните, что Банк никогда не запрашивает эту информацию.
- Код доступа не должен быть простым, должен содержать не менее 8 символов, включающие строчные и прописные буквы латинского алфавита, цифры, символы верхнего и нижнего регистра клавиатуры компьютера.
- Незамедлительно сообщайте в Банк о факте невозможности получения доступа в систему ДБО по причине несовпадения кода доступа на вход в систему, в случае его многократного ввода.
- Для подтверждения расчетных (платежных) документов всегда используйте sms-код.