Waybank

Осторожно – фишинговые сайты!

Как правило, мошенники распространяют вредоносный код (компьютерные вирусы) на различных сайтах, который «заражает» персональный компьютер или мобильное устройство клиента, посещающего данный ресурс. При попытке входа в систему Интернет-банкинга с зараженного устройства, вирус перенаправляет клиента на «фишинговый» сайт, который используется злоумышленниками для получения доступа к личному кабинету клиента.

Как правило, «фишинговые» сайты внешне практически не отличаются от настоящего сайта Интернет-банка. На поддельном сайте клиента могут попросить ввести не только логин и пароль, но и другую информацию, например, паспортные данные, номер телефона и т.п.

Как распознать «фишинговый» сайт:

- для входа в личный кабинет запрашивается номер мобильного телефона или другие данные, кроме логина и пароля;
- работа в системе проводится без защищенного соединения (при работе в защищенном режиме слева от адресной строки отображается символ замка или аббревиатура https в начале адресной строки);
- адрес сайта может не совпадать с официальным адресом системы Интернет-банкинга (https://ibank.rentabank.ru);
- при входе на сайт Интернет-обозреватель может предупреждать, что сертификату безопасности сайта нельзя доверять.

«ВЭЙБАНК» АО рекомендует соблюдать следующие правила информационной безопасности при работе в системе Интернет-банкинга:

- Не посещайте непроверенные и небезопасные сайты. Вы можете непреднамеренно загрузить на свой компьютер вирусы и шпионские программы.
- Не нажимайте на всплывающие окна, содержащие рекламу. Желательно настроить Ваш web- браузер на автоматическую блокировку таких окон.
- Не читайте подозрительных электронных писем от незнакомых людей. Письма могут содержать вирусы.
- Не подключайте к компьютеру непроверенные на наличие вирусов любые носители памяти (флеш-карты).
- Будьте внимательны к странным или непонятным сообщениям об ошибках web-браузера.
- В случае возникновения подозрений на наличие вирусов или шпионского ПО - просканируйте компьютер антивирусной программой.
- Используйте лицензионное антивирусное программное обеспечение и следите за его регулярным обновлением;
- Используйте современную операционную систему и своевременно устанавливайте все необходимые исправления и обновления;
- Используйте персональные межсетевые экраны и спам-фильтры.
- НЕ УСТАНАВЛИВАЙТЕ на мобильный телефон, на который приходят SMS-сообщения с кодом подтверждения, приложения, полученные из ненадежных источников.

В случае возникновения подозрения на мошенничество необходимо максимально быстро сообщить об этом в «ВЭЙБАНК» АО с целью оперативной блокировки доступа по телефону 8-495-900-10-47.