Предупреждение о фишинге

Многие интернет-сервисы, использующие для аутентификации пару логин/пароль, подвергаются фишинговым атакам. Цель злоумышленников – направить клиента на поддельный сайт, внешне неотличимый от настоящего, с целью кражи логина и пароля клиента.

Сервис «Интернет-банк для юридических лиц» («iBank2») коммерческого банка «Хлынов» не подвержен фишинговым атакам, в связи с использованием процедур криптографической аутентификации клиентов (установления гарантированно защищённого канала связи с сервером системы «Интернет-банк» с помощью электронного ключа).

Как не стать жертвой фишинга?

Доступ к банковским сервисам необходимо осуществлять только по ссылкам с официального сайта банка www.bank-hlynov.ru. Никогда не вводите ваши учетные данные для доступа в банковский сервис на других сайтах, даже если они имеют внешнюю схожесть с оригиналом. Обязательно проверяйте строку адреса в браузере!!! Отличие даже в одном символе в строке адреса может привести к печальным последствиям. Будьте внимательны и бдительны! Это защитит вас от попадания на фишинговый (подложный) сайт.

Если обнаружили, что ввели учетные данные на подложном сайте, вам необходимо немедленно изменить пароль доступа на официальном ресурсе банка, чтобы помешать мошенникам осуществить доступ к вашему счету.

При наличии любых подозрений о мошеннических действиях в отношении Вас, просим немедленно обратиться в банк!

Напоминаем, что банк ни при каких условиях не запрашивает конфиденциальную информацию клиента (логины, пароли, данные банковской карты, PIN-код и т.д.), в том числе через электронную почту, по телефону и т.п.