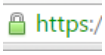
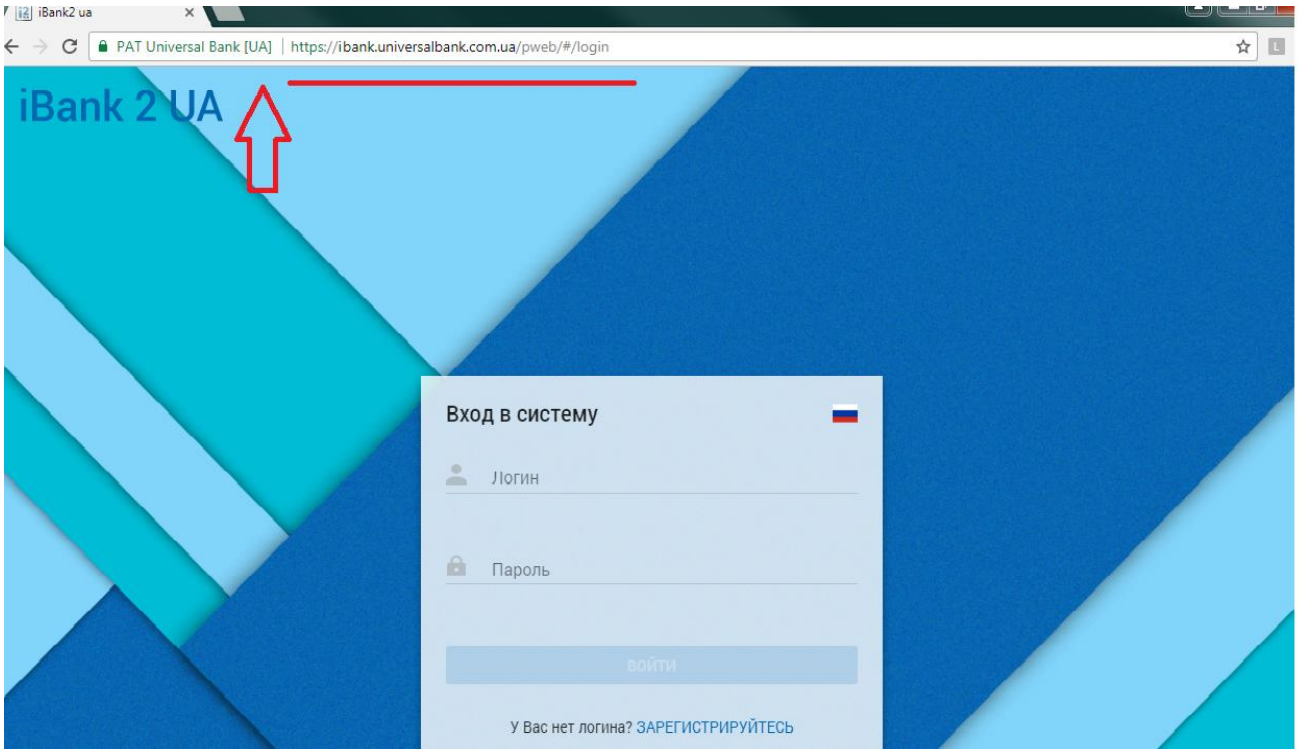
Рекомендації щодо безпечної роботи в системі «Інтернет-банкінг»

Для безпечної роботи в системі «Інтернет-банкінг» ознайомтеся з рекомендаціями фахівців інформаційної безпеки, що дозволять значно знизити ризики шахрайських операцій з рахунками, доступ до яких здійснюється каналами Інтернет-банкінгу.

Перед початком роботи з Інтернет-банкінгом переконайтеся, що адреса банку введена правильно https://ibank.universalbank.com.ua/pweb/. Адреса сторінки повинна починатися з https://, у браузері вона найчастіше позначається піктограмою з зображенням замку 

та/або виділяється кольором, що означає використання посиленого сертифікату безпеки банку. Лише після цього можете вводити Ваш логін та пароль. Валідна сторінка зображена на мал. 1



Не вводьте конфіденційних даних (паролів, ідентифікаторів) у вікна програм, якщо вони відрізняються від стандартних (інші форма, колір, логотипи, написи, шрифти); відображаються не так, як завжди (в іншому порядку). Уважно читайте всі повідомлення, що виникають на екрані комп'ютеру.

Не надсилайте будь-яку персональну інформацію – логін, пароль, контрольне слово тощо незахищеними каналами зв'язку (електронні листи, SMS-повідомлення і т. п.) на прохання псевдопредставників банку.

Не надавайте третім особам SIM-картку з номером мобільного телефону, який визначений для отримання OTP-паролів. Не використовуйте смартфони, на які були отримані права суперкористувача (Root) для отримання паролю для входу до системи «Інтернет-банкінг».

Не використовуйте прості паролі (123456,QWERTY). Довжина пароля має бути не менше 7-ми знаків, містити різні типи символів (літери, цифри, спеціальні символи) та бути різними для кожної служби, веб-сайту або системи.

Щоденно аналізуйте всі повідомлення про прийняті та неприйняті банком електронні розрахункові документи і негайно повідомляйте банк про випадки несанкціонованого зарахування (перерахування) коштів!

Встановіть на робочу станцію, з якої здійснюється доступ до системи «Інтернет-банкінг», ліцензійне антивірусне програмне забезпечення. Підтримуйте оновлення версій, регулярно та своєчасно оновлюйте антивірусні бази даних. Встановіть на робочу станцію: ліцензійне антишпигунське програмне забезпечення (antispyware); програмний персональний мережевий екран (файервол, брендмауер).

Мережевий екран необхідно налаштувати таким чином, щоб максимально обмежити вихідний та вхідний мережевий трафік. Зокрема, рекомендується дозволити доступ тільки до ресурсів системи «Інтернет-банкінг» та інших мінімально необхідних ресурсів. Наприклад, для оновлення баз вірусних сигнатур антивірусних програмних засобів, оновлення антишпигунських програмних засобів, операційної системи та іншого програмного забезпечення.

Антивірусне та антишпигунське програмне забезпечення налаштуйте для моніторингу всіх подій та періодичного сканування даних, що зберігаються на жорсткому диску персонального комп’ютера, з якого здійснюється доступ до системи «Інтернет-банкінг».

Регулярно та своєчасно оновлюйте системне програмне забезпечення робочої станції, за допомогою якого здійснюється доступ до системи «Інтернет-банкінг», особливо, операційної системи, web-браузеру, Java-машини. Рекомендується активувати можливість автоматичного оновлення програмного забезпечення.

Не рекомендуємо встановлювати на робочі станції, через які ведеться робота з системою «Інтернет-банкінг», програмне забезпечення з ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо). Не рекомендується здійснювати з такого комп’ютеру доступ до ненадійних (незнайомих) Інтернет ресурсів.

Під час доступу до системи «Інтернет-банкінг» суворо не рекомендується працювати в операційній системі з обліковим записом користувача, який має розширені права в операційній системі, наприклад, «Адміністратор».

Не рекомендується здійснювати доступ до системи «Інтернет-банкінг» через посилання, отримані електронною поштою, а також із неконтрольованих та ненадійних робочих станцій, розташованих в Інтернет кафе, готелях, офісах, інших організаціях тощо.