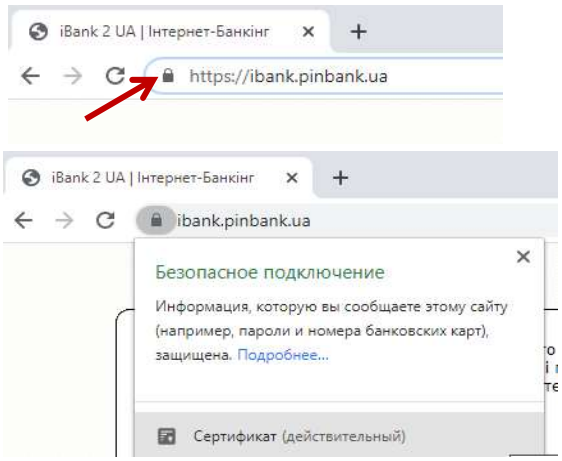
РЕКОМЕНДОВАНІ ЗАХОДИ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ СИСТЕМИ ДИСТАНЦІЙНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК»

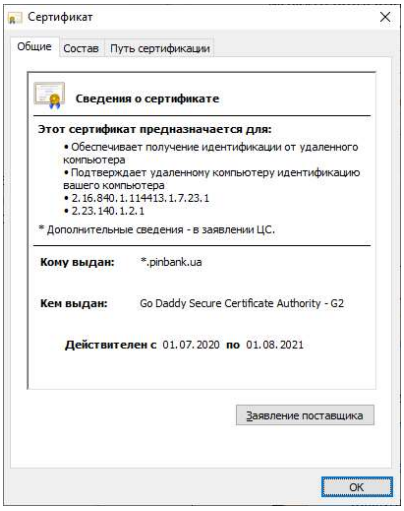
1. При доступі до системи дистанційного банківського обслуговування (ДБО) через веб-інтерфейс:

- обов'язково переконайтеся, що в адресному рядку браузера знаходиться адреса саме системи дистанційного обслуговування банку – "***https://ibank.pinbank.ua*** ";

  Зверніть увагу! Як правило, фішингові сайти, створені шахраями, мають дуже подібні до оригіналу адресу та зовнішній вигляд сторінок!

- завжди звертайте увагу на наявність у вікні браузера ознак захищеного з'єднання – це значок у вигляді замкнутого замка (вигляд цього значка та місце його відображення можуть відрізнятися залежно від браузеру та його версії), а також достовірний цифровий сертифікат банку





- відмовтесь від використання функції збереження паролів, яку пропонує браузер.

2. Уникайте використання системи дистанційного банківського обслуговування в публічних місцях з підключенням до відкритих wi-fi мереж (наприклад, кафе, готелі, торгові центри, зали очікувань тощо).

3. Встановлюйте паролі довжиною не менше 8 символів із застосуванням букв нижнього та верхнього регістрів, цифр та спеціальних знаків. Для досягнення більшої надійності та стійкості використовуйте в якості паролю словосполучення або фрази. Періодично змінюйте паролі.

4. Нікому не повідомляйте та не передавайте свій пароль, навіть керівнику, IT-адміністратору своєї організації або працівникам банку.

Зверніть увагу! Банк ніколи не запитує у клієнтів паролі, одноразові коди, копії криптографічних ключів, ПІН-коди та інформацію про строки дії платіжних карт, коди CVV2 ні телефонними дзвінками, ні в sms-повідомленнях, ні електронною поштою.

5. Приділяйте належну увагу зберіганню та використанню криптографічних ключів до системи дистанційного банківського обслуговування:

- зберігайте таємні ключі на захищених носіях (токенах);
- не тримайте носій з ключем постійно приєднаним до комп'ютера, а вмикайте його лише коли необхідно підписати документи;
- застосовуйте декілька підписів (2-3 ключі) для підтвердження і направлення фінансового документа на виконання в банк.

6. При роботі в системі дистанційного банківського обслуговування:

- не залишайте без нагляду комп'ютер або інший пристрій, з якого здійснюєте доступ до системи;
- завершуйте роботу з системою натисканням кнопки «вихід» (і закривайте вікно браузеру у разі використання веб-інтерфейсу), якщо закінчили роботу в системі або хочете відлучитися з місця.

7. На комп'ютері або іншому пристрої, з якого здійснюєте доступ до системи:

- для постійної роботи на комп'ютері використовуйте обліковий запис звичайного користувача, а привілейовані облікові записи з правами адміністратора застосовуйте лише у випадку необхідності, завжди звертайте увагу на запити операційної системи щодо підвищення привілеїв для встановлення програмного забезпечення або виконання операцій;
- використовуйте актуальні версії операційних систем, браузерів, іншого програмного забезпечення та регулярно їх оновлюйте. Де це можливо, налаштуйте оновлення в автоматичному режимі;
- використовуйте ліцензійні засоби антивірусного захисту та захисту від зловмисного програмного забезпечення, слідкуйте за регулярним оновленням сигнатур, періодично здійснюйте повне сканування локальних дисків;
- при роботі з електронною поштою відкривайте вкладення та посилання тільки від довірених відправників. Видаляйте без відкриття підозрілі електронні листи, листи від невідомих відправників, листи з прикріпленими файлами, які мають розширення *.exe, *.pif, *.vbs тощо.

  Зверніть увагу! Банк ніколи не розсилає електронною поштою програми для встановлення на комп'ютері або іншому пристрої, з якого здійснюєте доступ до системи ДБО.

8. Додатково перевірити, чи не внесений інтернет-сайт до «бази шахрайських сайтів» Української міжбанківської асоціації членів платіжних систем ЄМА, можна за посиланням https://ema.com.ua/report-an-incident/black-list/.

9. Додатково перевірити інформацію про банк та його відокремлені підрозділи можна у довіднику банків, розміщеному на офіційній сторінці НБУ, за посиланням https://bank.gov.ua/ua/supervision/institutions/ .

10. У випадках

- втрати паролю,
- втрати криптографічного ключа,
- неможливості увійти до системи через невідповідність паролю,
- при підозрі, що паролі/ключі стали відомі третім особам,
- виявлення спроби несанкціонованого доступу до системи тощо,
- виявлення підробленої сторінки банку (фішингового сайту),

для блокування доступу до системи та/або отримання рекомендацій щодо подальших дій негайно **зверніться до контакт-центру Банку за телефонами**: **0-800-50-70-80 або (044) 428-61-28 !**