**Пам’ятка Клієнта по роботі з системою**

**«Інтернет-Банкінг» для фізичних осіб**

*Шановний клієнте!*

При використанні системи «Інтернет-Банкінг» для фізичних осіб, переконайтеся в тому що встановлене безпечне з'єднання з сервером банку. В адресному рядку перевірте наявність напису my.creditwest.ua з іконкою замку. Натиснувши на напис, ви можете переконатися в захищеному з'єднанні з сервером банку.

Система «Інтернет-Банкінг» для фізичних осіб забезпечує захист роботи Клієнта за допомогою захищеного SSL сертифікату, і протоколу обміну в середовищі Інтернет з використанням кодів підтвердження з SMS.

Для запобігання шахрайських дій сторонніх осіб під час роботи в системі «Інтернет-банкінг» для фізичних осіб і піклуючись про безпеку платежів Банк також рекомендує:

* встановити ліцензійне антивірусне програмне забезпечення і мережевий екран (наприклад, Brandmauer, Firewall), які блокують втручання в роботу з платежами небезпечного програмного забезпечення;
* проводити періодичне сканування комп'ютера на наявність небезпечного програмного забезпечення;
* не встановлювати і не використовувати на комп'ютерах з яких працюєте в системі "Інтернет-банкінг" програми віддаленого доступу (наприклад, AmmyyAdmin, TeamViewer і т.д.);
* встановити пароль для доступу до комп'ютера, а також, блокування екрану через 5 хвилин не використання, з якого зазвичай здійснюється вхід у систему "Інтернет-банкінг" для фізичних осіб;
* перед початком роботи з системою «Інтернет-банкінг» для фізичних осіб обов'язково переконатися, що адреса <https://my.creditwest.ua/ifobsCreditWest/#/login/sign-in> введена правильно, і тільки після цього вводити логін і пароль;
* при здійсненні першого входу в систему «Інтернет-банкінг» Клієнт повинен в найкоротший термін змінити пароль, надісланий банком на номер телефону Клієнта, на власноруч створений постійний пароль;
* відключити або не користуватися функцією запам'ятовування логіна і пароля або автозаповнення текстових полів в браузерах;
* використовувати паролі, що складаються з літер, цифр і символів. Не застосовувати тривіальні і прості паролі. Довжина пароля повинна бути не менше 8 символів;
* не записувати пароль на папері, моніторі, в файлі і т.д. і не повідомляти їх третім особам. Якщо у Вас виникла підозра, що пароль став відомий стороннім особам, негайно змініть його;
* періодично міняти паролі (входу в комп'ютер і входу в систему «Інтернет-Банкінг» для фізичних осіб). Рекомендований термін зміни пароля – не більше 180 днів;
* обов'язково використовувати кнопку «Вихід» після закінчення роботи в системі «Інтернет-Банкінг» для фізичних осіб;
* використовувати ліцензійне програмне забезпечення на комп'ютері, з якого здійснюються платежі засобами системи «Інтернет-Банкінг» для фізичних осіб. Встановлювати оновлення, рекомендовані компаніями - виробниками програмного забезпечення;
* не відправляти будь-яку персональну інформацію - логін, пароль, контрольні SMS, коди і т.д. незахищеними каналами зв'язку (електронні листи, SMS-повідомлення тощо) та/або на прохання псевдо представників Банку.

У випадках виявлення несанкціонованого доступу або підозри на несанкціонований доступ до рахунку або компрометації/підозри на компрометацію логіну, пароля, необхідно у момент коли стало відомо, звернутися на гарячу лінію Банку за телефоном 0 800 501 800, або повідомити технічний персонал системи «Інтернет-банкінг» для фізичних осіб за телефоном: +38 044-365-00-22. При цьому обов'язково необхідно здійснити звірку залишку коштів на рахунку та перелік останніх платежів.

У разі виявлення несанкціонованого платежу у найкоротший термін передати до Банку письмове повідомлення, в якому докладно викласти всі обставини щодо несанкціонованого доступу.

Усі контакти для комунікації з Банком розміщенні на офіційному сайті Банку за посиланням: <https://www.creditwest.ua/kontakty>.