ПРАВИЛА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВИКОРСИТАННІ СИСТЕМИ ДИСТАНЦІЙНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ КЛІЄНТІВ - ФІЗИЧНИХ ОСІБ ПАТ «ВЕРНУМ БАНК»

VERNUM Online

Дотримання елементарних правил безпеки дозволить Вам захистити себе від шахрайства!

Для доступу до особистого кабінету необхідний лише ІДЕНТИФІКАТОР (ЛОГІН) та ПАРОЛЬ. В разі, якщо від Вам вимагається введення будь-якої іншої інформації (номери банківських карток, номеру мобільного телефону, інших персональних даних), необхідно припинити роботу в системі та зателефонувати до Банку.

Банк ніколи НЕ ЗАПИТУЄ ПАРОЛІ ДЛЯ СКАСУВАННЯ ОПЕРАЦІЇ в VERNUM Online, оскільки скасування операції в системі не передбачена. Якщо Вам пропонується ввести пароль для скасування операції необхідно припинити роботу в системі та зателефонувати до Банку..

При отриманні SMS-повідомлення з разовим паролем уважно ознайомтесь з його змістом. **Вводити пароль слід лише в тому випадку, якщо операція ініційована особисто Вами**.

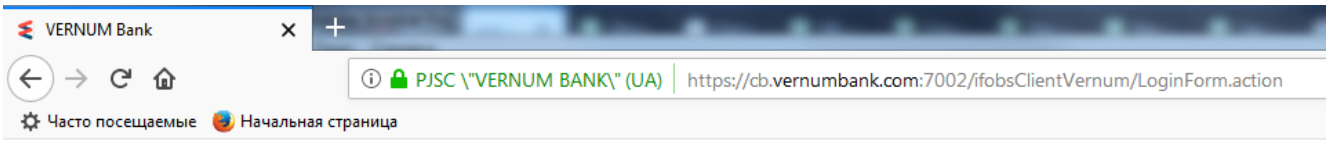
Перевірте, що встановлено захищене SSL-З'ЄДНАННЯ З ОФІЦІЙНИМ САЙТОМ ПОСЛУГИ

https://cb.vernumbank.com:7002/ifobsClientVernum/LoginForm.action.

При роботі з системою **VERNUM Online** в адресній строчці Вашого браузера відображається позначка безпечного з'єднання .

Використовуйте для роботи з системою **VERNUM Online** останні версії веб-браузерів.

Адресна строчка повинна містити найменування Банку та виглядати наступним чином:



За будь-яких обставин нікому не розголошуйте свій пароль, в тому числі працівникам Банку. ПАРОЛЬ ДЛЯ ВХОДУ в систему **VERNUM Online** - це Ваша особиста КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ.

Не встановлюйте на мобільний телефон або інший пристрій, на який Банк надсилає SMS-повідомлення з підтверджуючим разовим паролем, **додатки, завантажені з невідомих Вам джерел**. Пам'ятайте, що Банк не здійснює розсилки своїм клієнтам посилання або вказівки на встановлення додатків засобами SMS/MMS/E-mail-повідомлень.

В РАЗІ ВТРАТИ мобільного телефону (пристрою), на який Банк направляє SMS-повідомлення с підтверджуючим разовим паролем, або неочікуваним припиненням роботи SIM-карти, **Вам необхідно якомога швидше звернутись до свого оператора мобільного зв'язку та ЗАБЛОКУВАТИ SIM-КАРТУ, після чого звернутись до Банку**.

Задля безпеки Ви маєте можливість відстежувати дату та час останнього візиту в систему **VERNUM Online** (в правій верхній частині екрану).

В разі виявлення будь-якого шкідливого програмного забезпечення (віруси, троянські програми тощо) на ПК або мобільних пристроях, з яких здійснюється вхід в систему **VERNUM Online**, необхідно **В ОБОВ'ЯЗКООВМ УПОРЯДКУ здійснити вхід до системи з гарантованого не зараженого пристрою та змінити пароль доступу до системи VERNUM Online**.

Періодично змінюйте пароль для входу в систему **VERNUM Online**. Функціоналом Системи передбачена примусова зміна паролю 1 раз на рік, але Банк рекомендує Вам виконувати таку процедуру частіше.

Не використовуйте функцію «запам'ятовування пароля» веб-браузером або іншим програмним забезпеченням для входу в систему **VERNUM Online**.

Для коректного закриття сесії **вкрай важливо** здійснювати вихід із системи **VERNUM Online** за

допомогою натискання кнопки **«Вийти»**.

Уникайте використання для доступу в систему **VERNUM Online** чужих пристроїв або пристроїв, встановлених в публічних місцях.

На сайті ПАТ «ВЕРНУМ БАНК» вказані актуальні офіційні контактні телефони.

На обладнанні (ПК, мобільні пристрої тощо), з яких здійснюється робота в системі **VERNUM Online**, **використовуйте тільки ліцензійні операційні системи та антивірусні програми з регулярно оновлювальними антивірусними базами.** Також **регулярно оновлюйте операційну систему** (насамперед це стосується оновлень безпеки). При повсякденній роботі **не використовуйте обліковий запис з правами локального адміністратора** (використовуйте обліковий запис користувача).

ПАТ «ВЕРНУМ БАНК» інформує про те, що на сьогоднішній день спостерігається ріст шахрайських дій щодо клієнтів комерційних банків, які керують своїми рахунками за допомогою мережі Інтернет, засобами різних систем дистанційного банківського обслуговування.

Схеми шахрайських дій, як правило, будуються наступним чином. Зловмисники розповсюджують вірусні програми засобами різних інтернет-ресурсів – від соціальних мереж до звичайних новосних сайтів. Клієнт, який недостатньо уважно ставиться до виконання вимог інформаційної безпеки (наприклад: використовує неліцензійну операційну систему; не використовує програми захисту: антивірус, файєрвол тощо; постійно працює з правами адміністратора; не використовує пароль для власного облікового запису або використовує занадто легкий пароль тощо), під час відвідування інфікованих сайтів, інфікує власний пристрій: комп'ютер або мобільний пристрій. Як наслідок, шахраї отримують можливість керувати пристроями клієнта, в тому числі мають змогу перехоплювати його логіни та паролі, або, при спробі клієнта зайти до особистого кабінету, пере направити клієнта на «фішінгові» сайти, які зовнішньо практично не відрізняються від оригінальних сайтів систем дистанційного банківського обслуговування.

На підробленому сайті Вам можуть запропонувати ввести ідентифікатори та паролі, мобільний телефон та інші персональні дані, необхідні шахраям для отримання доступу до Вашої конфіденційної інформації.

Для захисту від шахрайських дій в системі **VERNUM Online** передбачено підтвердження всіх фінансових операцій та інформаційних повідомлень разовим паролем, який клієнт отримує в SMS-повідомленні, надісланому Банком. Отже, разовий пароль – це дуже критичний елемент безпеки, який не можна повідомляти іншим особам.

З повагою,

ПАТ «ВЕРНУМ БАНК»