Рекомендації клієнтам щодо безпечного використання системи дистанційного обслуговування - Мобільного додатку GlobusPlus (далі – Мобільний додаток).

З метою мінімізації ризику впливу шахрайських дій сторонніх осіб під час роботи з Мобільним додатком Клієнт зобов'язаний:
1. Не відправляти будь-яку персональну інформацію - логін, пароль, номер картки та інше незахищеними каналами зв'язку (електронна пошта, SMS-повідомлення тощо) на прохання третіх осіб (в т.ч. особам, що видають себе за представників Банку), а у разі настання такого випадку негайно зв'язатися з контакт центром Банку і повідомити про такий випадок для отримання додаткових консультацій.
2. Використовувати Мобільний додаток встановлений з авторизованих джерел розробників операційних систем Google Inc., Apple Inc.
3. З метою мінімізації ризику впливу шахрайських дій сторонніх осіб під час роботи з Мобільним додатком Банк рекомендує Клієнту:
4. Не використовувати однакові логін і пароль для доступу до різних систем. Рекомендовано використовувати пароль до Мобільного додатку, що складаються з літер, цифр і символів, довжина якого повинна бути не менше 4-х знаків.
5. Періодично змінювати пароль. Рекомендований термін зміни пароля - не рідше ніж кожні 90 днів.
6. Налаштовувати SMS-інформування про рух коштів на Банківському (-их) рахунку (-ах) та платіжних картках для контролю несанкціонованого використання коштів.
7. Не записувати логін і пароль на папері, моніторі, у файлі і т.п., а також не повідомляти їх третім особам. А у випадку виникнення у Клієнта підозри на те, що логін і/або пароль став відомий стороннім особам, негайно змінити його або звернутися до контакт центру Банку для отримання додаткових консультацій.
8. Дотримуватися загальних правил безпеки: не поширювати реквізити своїх карт, дані щодо тимчасових ОТР- паролів та дані щодо паролю, не проводити операції з рахунками в місцях загального доступу, не використовувати WI-FI у публічних місцях. У випадку втрати Номера мобільного (фінансового) телефону Клієнта, або у випадку підозри на компрометацію пароля, Клієнт повинен одразу звернутися в контакт центр Банку для тимчасового блокування Номера мобільного (фінансового) телефону Клієнта в системах Банку та блокування доступу Клієнта до Мобільного додатку. Номер мобільного (фінансового) телефону Клієнта може бути змінений Клієнтом лише після особистого звернення Клієнта на відділення Банку з письмовою заявою, складеною за формою Банку та проведення повторної ідентифікації Клієнта.
9. Клієнт самостійно має забезпечити недоступність для третіх осіб логіна та пароля до Мобільного додатку.
10. Клієнт самостійно і в повному обсязі несе відповідальність за всі наслідки, спричинені здійсненням доступу та/або ініціюванням операцій третіми особами, у разі отримання ними інформації про логін, пароль в будь-який спосіб, зокрема, але невиключно через безпосереднє з необережності чи з відома повідомлення Клієнтом зазначеної в цьому пункті конфіденційної інформації третім особам, підбора третіми особами логіну, паролю, у випадку отримання третіми особами доступу до Номера мобільного (фінансового) телефону Клієнта, на який Банк здійснює надсилання паролів/кодів, тощо.
11. Клієнт зобов'язаний вжити всіх можливих заходів для запобігання втрати/крадіжки конфіденційної інформації, в тому числі логіну та пароля, надійно зберігати портативний пристрій з встановленою SIM-карткою Номера мобільного (фінансового) телефону, на який Банком здійснюється надсилання електронних повідомлень, не передавати портативний пристрій у користування третім особам, негайно звертатись до мобільного оператора для блокування SIM-картки Номера мобільного (фінансового) телефону у разі її втрати, не повідомляти інформацію, яка дає змогу ініціювати операції/відновлювати доступ до Мобільного додатку третім особам, в тому числі, але не виключно, якщо ці особи представляються працівниками Банку (окрім самостійного звернення Клієнта до Контакт центру Банку або відділення Банку), працівниками підрозділу безпеки Банку / НБУ /

правоохоронних органів тощо. Клієнт зобов’язаний негайно, в найкоротший проміжок часу з моменту настання події, інформувати Банк про:
- розголошення/втрату/крадіжку конфіденційної інформації, в тому числі кодів/паролів, які дають змогу здійснювати платіжні операції або відновити доступ до Мобільного додатку;
- про зміну/блокування/тимчасову недоступність Номера мобільного (фінансового) телефону;
- несанкціоновані Клієнтом платіжні операції;
- про дзвінки/SMS-повідомлення/Viber–повідомлення тощо від третіх осіб щодо намагання отримати інформацію, яка дає змогу ініціювати операції/ відновити доступ до Мобільного додатку.

Недотримання Клієнтом передбачених цим пунктом зобов’язань вважається діями (чи бездіяльністю), що призводять до несанкціонованого використання Мобільного додатку і відповідальність за проведені за допомогою Мобільного додатку операції несе Клієнт.

Безпека облікового запису Клієнта Банку в Мобільному додатку залежить від того яким чином Клієнт Банку зберігає свій мобільний телефон, планшет, або інший пристрій, що використовується для підключення до Мобільного додатку. У випадку, якщо Клієнт Банку добровільно надає третім особам свій мобільний телефон, планшет, комп'ютер або інший пристрій, третя сторона буде мати доступ до облікового запису Клієнта Банку в Мобільному додатку та персональної інформації цього Клієнта Банку, при цьому Банк не несе відповідальності за такі випадки та їхні наслідки.

Клієнт Банку несе пряму відповідальність за контроль доступу до свого мобільного телефону, планшета або іншого мобільного пристрою, який використовується для здійснення Операцій в Мобільному додатку, а також за інші сервіси та програми, що можуть бути встановлені на такі пристрої. Клієнт Банку також несе відповідальність за зберігання своїх паролів та розповсюдження (поширення) даної інформації третім особам.

Для належного отримання послуг в Мобільному додатку Клієнт зобов’язаний своєчасно встановлювати доступні оновлення Операційної системи і додатків на своєму мобільному телефоні, планшеті, або іншому пристрої, що використовується для підключення до Мобільного додатку. Використовувати на своєму мобільному телефоні, планшеті, або іншому пристрої, що використовується для підключення до Мобільного додатку сучасне антивірусне програмне забезпечення і своєчасно встановлювати на нього оновлення антивірусних баз.