Рекомендації щодо безпечного використання Мобільного застосунку izibank та виявлення фішингових вебсайтів

1. Під час використання Мобільного застосунку izibank (далі – МЗ) не залишайте мобільний телефон без нагляду.
2. Здійснюйте регулярне та своєчасне оновлення операційної системи свого мобільного пристрою (смартфону) та МЗ тільки з офіційних джерел. Оновлення дозволить виправити уразливості в програмному забезпеченні та зменшити ризики інфікування шкідливими програмами.
3. Важливо забезпечити/гарантувати Клієнтом неможливість отримання третіми особами інформації про Логін, Пароль, номер фінансового телефону тощо. Ризик і відповідальність за несанкціоноване використання Логіна, Пароля несе виключно Клієнт. Використовуйте надійні паролі для запобігання несанкціонованого доступу до мобільного пристрою.
4. Уникайте відкриття невідомих посилань, отриманих через електрону пошту чи в СМС-повідомленні від невідомих абонентів.
5. Забезпечте захист свого мобільного пристрою та SIM-картки, на номер якої здійснена реєстрація в Мобільному застосунку.
6. Не залишайте мобільний пристрій із активною сесією роботи Мобільного застосунку без нагляду. Виходьте з МЗ, навіть якщо потрібно відійти на невеликий час.
7. У випадку виявлення здійснення несанкціонованого доступу до Облікового запису в застосунку, негайно зверніться до Операційного центру izibank за телефоном 0800-605-005, 8(044) -224-67-27 або у месенджері та повідомте про втрату.
8. Уважно перевіряйте вебсайти, на яких ви здійснюєте онлайн покупки: якщо вони будуть вам підозрілі - не вказуйте там жодних своїх даних.
9. У разі необхідності введення автентифікаційних даних переконайтеся, що з'єднання зашифроване. На це вказує адреса, яка починається з https:// та іконка закритого замка; також перевірте сертифікат веб-сайту (достатньо натиснути на замок).
10. Перевіряйте сайт, використовуючи ресурс «Чорний список» від Асоціації ЄМА на наявність шахрайських сайтів в списку або сервіс кіберполіції «STOP FRAUD».