Захист ідентифікаційних даних:

Компрометація ідентифікаційних даних – це використання Вашого поточного рахунку в шахрайських цілях шахраєм, який володіє достатньою кількістю інформації про Вас, щоб відповісти на ідентифікаційні питання в телефонній розмові із співробітником Банку і отримати допуск до Вашого рахунку. Шахрай, знаючи ідентифікаційну інформацію про Вас (контрольне кодове слово, номер паспорта, ІПН, дату народження, адресу проживання або прописки), може без Вашого відома:

- Змінити адресу проживання, а через деякий час повідомити, що платіжна картка загублена / вкрадена та замовити нову платіжну картку на іншу поштову адресу.
- Змінити контактний номер телефону і, таким чином, перенаправити СМС про проведення операцій платіжною карткою / ідентифікаційні дзвінки служби моніторингу, Контакт-центру Банку та інших підрозділів Банку на свій (мобільний) номер телефону.
- Збільшити / зняти авторизаційні ліміти на проведення операцій і зняти всі Ваші кошти або витратити їх на товари та послуги.
- Анулювати (зняти) лічильники неправильно введеного PIN-коду.

Де шахраї можуть отримати ваші ідентифікаційні дані:

- Інтернет: у соціальних мережах ВКонтакте, Одноклассники, ВСети, Я.ру, Facebook, Google+, Tumblr, Twitter, Avaaz, Ask.fm, Badoo, Dudu, Flickr, Foursquare, Instagram, Last.fm, LinkedIn, LiveJournal, MySpace, Mixi, Orkut, Renren, Sina Weibo, SoundCloud, Tagged, відвідуючи відкриті сторінки та зламуючи закриті сторінки, Ваші електронні поштові скриньки, гаманці.
- Коли Ви передаєте персональні дані стороннім особам та організаціям у магазинах, на вулиці, приймаючи участь в акціях, розіграшах, отриманнях знижок (карток на знижки) на товари та послуги.
- В інших місцях, де Ви надаєте номер паспорта, ІПН, дату народження, адресу проживання або прописки.