Як уберегтися від шахрайства?

1. Картка. Зберігати ПК в недоступному для сторонніх місці.

2. Картка. Мати декілька ПК для різних цілей: для зняття коштів в АТМ і розрахунків в магазинах - одна ПК; для розрахунків в мережі Інтернет - інша ПК з відповідними лімітами.

3. Кодове слово пароль. НЕ використовувати прості, легко відгадувані слова (дівоче прізвище матері, дату народження, і т.д.)

4. ПІН-код. Не записувати ПІН-код на ПК. Не вибирати ПІН-код 0000, 1111, 1234 і т.п.

5. Ліміти. Встановити карткові ліміти в межах сум операцій, характерних саме для вас.

6. SMS-банкінг (StarSMS). Обов'язково підключити SMS-банкінг до ПК.

7. Картка. Не давати ПК в руки стороннім особам. При оплаті товарів і послуг тримайте картку в полі зору, щоб будь-яка оплата здійснювалася в вашій присутності.

8. АТМ. Перед проведенням операцій в АТМ оглянути АТМ на наявність сторонніх пристроїв, пошкоджень, подряпин, залишків клею. Прикривати рукою клавіатуру при введенні ПІН-коду.

9. Виписка. Перевіряти виписку по рахунку щомісяця. Якщо ви побачили операцію, яку не проводили, зверніться до відділення і напишіть заяву в Банк.

10. Комп'ютер / смартфон. Проводити операції по ПК в мережі Інтернет на знайомих офіційних сайтах з використанням захищеного протоколу передачі даних https: // (замість http: //).

11. Комп'ютер / смартфон. В мережі Інтернет використовувати для розрахунків технологію 3D Secure і / або Verified by Visa.

12. Комп'ютер / смартфон. Використовувати ліцензійне програмне забезпечення на пристроях і встановити ліцензійний антивірус.

13. Комп'ютер / смартфон. Працювати тільки на захищеному персональному комп'ютері з обмеженим фізичним доступом до нього сторонніх осіб. Не відкривати комп'ютерні файли або посилання, отримані з ненадійних джерел, не відповідати на такі повідомлення.

14. Ніколи не повідомляти термін дії ПК, секретний код (CVV2 / CVC2) та паролі з смс-повідомлень особам, які телефонують або надсилають e-mail повідомлення, смс повідомлення і представляються співробітниками Банку, МПС Visa Inc. і MasterCard WorldWide, Нацбанку України, СБУ та різних інших організацій, і просять повідомити особисті дані нібито для проведення процесу ідентифікації, підтвердження наявності ПК на руках, для зарахування коштів на рахунок т.д.

15. Картка. Перейти на використання ПК з чіпом.

16. Картка. Повідомити Банк про виїзд за кордон. Це можна зробити через сайт my.ukrsibbank.com.

17. Картка. Негайно повідомити в Банк про втрату / крадіжку ПК, операції по ПК, які ви не проводили, підозрілі пристрої на АТМ, про розголошення конфіденційних даних по ПК чи дзвінок від шахрая.

19. Картка. Бути обачним при проведенні операцій по ПК.

19. Картка. Бути завжди на зв'язку з Банком, номери для телефонного зв'язку:

0 800 505 800, 729 з мобільного, 044 590 06 75 за кордоном.