Пам’ятка для безпечного використання Вашої платіжної картки

Забезпечте безпеку Ваших даних

- Запам’ятайте номер ПІН-коду, не тримайте записані паролі та коди поруч із карткою.
- Ніколи і нікому не повідомляйте ПІН-код по телефону та не відправляйте його за допомогою SMS або електронною поштою.
- Зверніть увагу, що співробітники банку не дзвонять Вам з метою з’ясування реквізитів картки і Ваших особистих даних. Винятком є Ваше спілкування з оператором у разі Вашого звернення до Контакт-центру.
- Якщо Вам дзвонять під різними приводами та намагаються отримати будь-яку інформацію, пов’язану із карткою, покладіть слухавку та самі передзвоніть до Контакт-центру.

Попіклуйтесь про безпеку розрахунків

- Прикривайте рукою клавіатуру під час введення ПІН-коду, запевніться, що на банкоматі немає накладок (на клавіатурі, приймачі картки).
- Намагайтесь використовувати для розрахунків в інтернеті особистий комп’ютер. Не вводьте свої дані, якщо не впевнені у справжності ресурсу. Для перевірки введіть будь-яку вигадану електронну адресу та випадковий набір букв/цифр як пароль. Сайт шахраїв прийме введені дані та просто переадресує Вас на іншу сторінку.
- Підключіть послугу 3-D Secure, що дозволяє здійснювати безпечні розрахунки в інтернеті, відправляючи одноразові паролі на номер Вашого телефону для підтвердження операції.
- Підключіть послугу SMS-info та отримуйте SMS про будь-який рух коштів на Вашому рахунку.

Блокуйте картку негайно, якщо:

- Вашу картку вкрадено, втрачено або залишено в банкоматі.
- Ви підозрюєте, що реквізити картки (номер, ПІН-код, CVV – три останні цифри, зазначені на магнітній полосі на звороті картки, термін дії) стали відомі іншим особам.
- Ви отримали SMS про операцію, яку не здійснювали.
- Ви підозрюєте несанкціонований доступ або зміну Вашої інформації в системах дистанційного обслуговування.
- Ви потрапили на фішингові вебсайти або отримані відомості подібного змісту.

Заблокувати картку Ви можете в онлайн-банку, Контакт-центрі або відділенні банку.

Негайно повідомте Банк про:

- втрату Вашої платіжної картки
- несанкціонований доступ або зміну Вашої інформації в системах дистанційного обслуговування
- виявлення Вами фішингового вебсайту Банку або отримання Вами відомостей (інформації) про фішинговий вебсайт Банку

Телефон Контакт-центру ПАТ «Банк Восток» – 0 (800) 30-70-10.

Безпека в інтернеті

1. Перед початком роботи обов’язково переконайтеся, що адресу сторінки онлайн-банку введено вірно https://my.bankvostok.com.ua/. Адреса сторінки повинна починатись з https:// (HyperText Transfer Protocol Secure). Позначається у оглядачі іконкою з замком та/або виділяється кольором, що вказує на використання посиленого протоколу безпеки. Тільки після цього можете вводити логін та пароль для входу в онлайн-банк.
2. Відключіть та не використовуйте функцію зберігання логіну та паролю або автозаповнення текстових полів у оглядачах.
3. Для коректного завершення роботи в онлайн-банку обов’язково використовуйте кнопку «Вихід».
4. Пам’ятайте! Чим складніший пароль – тим надійніша Ваша безпека.
5. Не зберігайте паролі: на папері, у файлі, телефоні чи інших носіях інформації. Облікові (авторизаційні) дані суворо конфіденційні. У разі підозри втрати облікових даних, терміново зверніться до Контакт-центру ПАТ «Банк Восток» за телефоном 0 (800) 30-70-10.
6. Не передавайте персональну інформацію: контрольне слово, номер платіжної картки за допомогою незахищених каналів зв'язку (електронна пошта, SMS-повідомлення, тощо). Логін та пароль – це ті дані, які не повинен знати ніхто крім Вас.
7. Увага! Банк не здійснює розсилку електронних листів та не телефонує з метою отримання персональної інформації клієнта, що пов'язана з паролями, одноразовими кодами, інформацією про номери платіжних карток, PIN-кодів, коди CVV2 тощо.
8. Користуйтесь послугою SMS-інформування, щоб контролювати безпеку руху коштів.
9. Зверніть увагу, щоб на вашому ПК, з якого здійснюється вхід та подальша робота в онлайн-банку, було встановлено ліцензійне антивірусне ПЗ.
10. При виявленні вірусного або зараженого ПЗ на комп’ютері, з якого здійснюється робота в онлайн-банку, зверніться до Контакт-центру ПАТ «Банк Восток», за телефоном 0 (800) 30-70-10.
11. У разі втрати телефону або блокуванні SIM-карти, які використовувались при роботі у системі, терміново зверніться до Контакт-центру ПАТ «Банк Восток», за телефоном 0 (800) 30-70-10.
12. Використання ПК для розрахунків в мережі Інтернет має підвищений ризик, тому рекомендуємо використовувати для подібних операцій спеціалізований банківський продукт Net.Card – ПК, яка може бути використана виключно для здійснення операцій за допомогою Інтернет/пошти/телефону. Вся інформація, що необхідна для здійснення розрахунків зазначена на ПК. Дана ПК не має магнітної смуги та ПІН-коду.
13. Аватар (зображення користувача) – функція захисту від фішингу (інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних

користувачів). Зображення, яке Ви обрали, відомо лише Вам. Якщо Ви увійшли до онлайн-банку та бачите інше зображення або воно відсутнє, можливо, Ваш аккаунт намагались зламати або його вже було зламано. Терміново зверніться до Контакт-центру ПАТ «Банк Восток» за телефоном 0 (800) 30-70-10.

14. Фішинг-вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів банків, сервісів з переказу або обміну валюти, інтернет-магазинів тощо. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані для подальшого використання такої інформації у своїх зловмисних цілях. До конфіденційної інформації відносяться логіни та паролі, реквізити платіжних карток (їх номери,термін дії, тощо) адресу електронної пошти, номери фінансових/контактних телефонів, відповіді на секретні питання і таке інше.

Така діяльнсть проводиться для використання несанкціонованих електронних листів (так званого СПАМу) та для переадресування користувачів на веб-сайти в інтернеті, які зовнішньо копіюють дизайн офіційних сайтів тих чи інших установ.

Тобто при виконанні певного алгоритму дій користувач добровільно направляє злочинцям інформацію, яка буде використана останніми у їхніх зловмисних цілях. Наприклад, отримавши від користувача-клієнта банківської установи інформацію про номер платіжної картки, термін її дії, ім’я та прізвище власника платіжної картки,CVV-код- зловмисники зможуть використати отриману інформацію для здійснення несанкціонованого списання коштів з такої платіжної картки.

Для унеможливлення потрапляння клієнтів банків на фітингові вебсайти Національний банк України на сторінці свого офіційного інтернет-представництва розмістив офіційний перелік вебсайтів банків України і, перейшовши за посиланням: https://bank.gov.ua/ua/supervision/institutions, Ви маєте змогу перевірити належність вебсайту конкретній банківській установі.