

---

## Пам'ятка для безпечного використання Вашої платіжної картки.

### Безпека Ваших даних

1. Тримайте в секреті PIN-код та тризначний номер на звороті картки, пароль до мобільного додатку / Онлайн банку, одноразові SMS- паролі. Повідомляти можна тільки 16- значний номер картки.
2. Ніколи і нікому не повідомляйте PIN -код по телефону та не відправляйте його за допомогою SMS або електронною поштою
3. 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.
4. Якщо Ви використовуєте Apple Pay чи Google Pay, встановіть на смартфоні підтвердження платежів через Face ID або Touch ID.
5. Не реагуйте на підозрілі повідомлення про виграш , про блокування картки, де просять зателефонувати і дізнатись деталі.
6. Якщо Вам дзвонять під різними приводами та намагаються отримати будь-яку інформацію, пов'язану із картою, покладіть слухавку та самі передзвоніть до Контакт-центру.
7. Якщо Ви розкрили дані платіжної картки шахраям, негайно блокуйте картку, телефонуйте в банк за телефоном, що вказаний на звороті картки.

### Безпека онлайн розрахунків.

1. Підключіть послугу 3-D Secure, що дозволяє здійснювати безпечні розрахунки в інтернеті, відправляючи одноразові паролі на номер Вашого телефону для підтвердження операції.
2. Перевіряйте сайти, на яких плануєте онлайн покупки- не натрапте на сайт-двійник.
3. Використовуйте тільки перевірені сайти. Уважно перевіряйте правильність назви та адреси сайту, щоб не опинитися на фішинговому ресурсі.
4. Звертайте увагу на контактні дані магазину чи продавця. Наявність лише мобільного телефону, інтернет-сторінки та посилання на Viber/Telegram-канал- ознака шахрайської сторінки. Досвідчений продавець зазвичай пропонує кілька способів оплати. Якщо маєте сумніви- обирайте післяплату.
5. Сайти, які приймають онлайн платежі мають містити https:// та значок «Замочок»
6. На сайті мають бути значки захисту онлайн покупок від платіжних систем - Verified by Visa та Mastercard Secure card.
7. Перевірити сайт можна за допомогою спеціального сервісу Кіберполіції <https://cyberpolice.gov.ua/stopfraud/> або сервісу Асоціації «ЄМА » <https://www.ema.com.ua/blacklist/>.
8. Якщо ви зрозуміли, що потрапили в руки шахраям через фішинговий сайт – повідомте про це Кіберполіцію. Залиште заяву в Кіберполіцію за посиланням <https://ticket.cyberpolice.gov.ua/> або телефонуйте за номером -0800505170.

9. Якщо ви ввели дані платіжної карти на шахрайському сайті - негайно блокуйте карту, телефонуйте в Банк за телефоном, що вказаний на звороті картки.

Безпеку при використанні картки в банкоматі та в магазинах через POS-термінали.

1. Прикривайте рукою клавіатуру під час введення PIN-коду, запевніться, що на банкоматі немає накладок (на клавіатурі, приймачі картки).
2. Коли розраховуєтесь в магазинах, не передавайте картку в руки касирів під час розрахунків, тримайте картку в полі вашого зору.
3. Якщо плануєте значні витрати за кордоном, випустіть окрему картку та поповнюйте її на суму запланованих витрат.
4. Звертайте увагу на суму на екрані POS-терміналу, на чеку та в повідомленні про списання грошей.

Безпека в онлайн-банку/мобільному додатку.

1. Перед початком роботи обов'язково переконайтеся, що ви використовуєте офіційну версію мобільного додатку або 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. Зверніть увагу, щоб на вашому ПК, з якого здійснюється вхід та подальша робота в онлайн-банку, було встановлено ліцензійне антивірусне ПЗ.
9. 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.
10. 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.

11. Аватар (зображення користувача) – функція захисту від фішингу. 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.

#### Розповсюджені схеми шахрайства з використанням платіжних карток.

1. 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. 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 фішингові 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.
2. Надсилання SMS, Viber- або Telegram-повідомлень, повідомлень в соціальних мережах, а також електронних листів з інформацією про виграш в лотереях, в яких ви не брали участь;
3. Розсилки фейкових повідомлень про проведення соціальних виплат від ООН, Червоного Хреста, інших міжнародних або урядових організацій, великих українських компаній та фондів, крупних торговельних мереж з вказанням телефонних номерів чи посилань на шахрайські сторінки з вимогою ввести ваші особисті дані та дані картки;
4. Повідомлення або дзвінки з невідомих номерів телефону про надходження, зняття, блокування коштів з необхідністю підтвердити операцію або зателефонувати за наданим номером,
5. Дзвінки та в подальшому отримання посилання для встановлення «нової версії додатку банку»,
6. Дзвінки та повідомлення від імені Банку про блокування вашої картки чи облікового запису в мобільному додатку Банка,
7. Проведення опитувань «з метою покращення якості надання послуг», «підписання петицій» з проханням вказати ваші особисті дані чи дані вашої картки;
8. Використання шахрайських інтернет-крамниць та оголошень з мінімальними цінами, дані оплати з яких передаються шахраям.

Блокуйте картку негайно, якщо:

1. Вашу картку вкрадено, втрачено або залишено в банкоматі.

2. Ви підозрюєте, що реквізити картки (номер, PIN-код, CVV – три останні цифри, зазначені на магнітній полосі на звороті картки, термін дії) стали відомі іншим особам.
3. Ви отримали SMS /PUSH повідомлення про операцію, яку не здійснювали.
4. Ви підозрюєте несанкціонований доступ або зміну Вашої інформації в системах дистанційного обслуговування.
5. 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.