Рекомендації щодо безпечного використання електронних платіжних засобів (платіжних карт) АТ «БАНК «ГРАНТ»

Шановні клієнти!

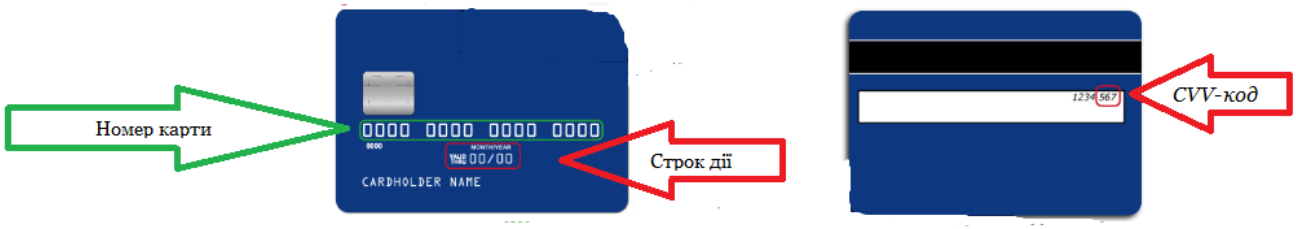
У зв'язку зі зростанням кількості кіберзлочинів, пов'язаних з несанкціонованим переказом коштів з рахунків клієнтів, які обслуговуються за допомогою електронних платіжних засобів, та з метою попередження можливих збитків від шахрайських дій сторонніх осіб, **наполегливо просимо Вас** під час використання платіжної карти АТ «БАНК «ГРАНТ» **дотримуватись** нижченаведених організаційних та технологічних **заходів безпеки**.

1. **Забезпечте належний захист Вашої платіжної карти та конфіденційних даних**, що застосовуються для підтвердження правочинності її використання:

– **ніколи не передавайте** Вашу **платіжну карту** стороннім особам;

– **не залишайте** Вашу **карту без особистого нагляду** у місцях, до яких можуть отримати доступ сторонні особи;

– **нікому**, зокрема, **співробітникам Банку**[1], **не повідомляйте ПІН-код** Вашої карти, **строк її дії та CVV-код**, зазначений на зворотному боці картки;



За жодних обставин нікому не розголошуйте строк дії карти та CVV-код

Повідомляти можна ЛИШЕ 16-значний номер карти

Примітки 1

*Наголошуємо, що **співробітники Банку** при здійсненні технічної підтримки та наданні консультацій щодо використання платіжних карт АТ «БАНК «ГРАНТ» **ніколи не цікавляться інформацією про ПІН-код Вашої карти, строк її дії або CVV-код.***

– **ніколи не записуйте та не зберігайте ПІН-код** Вашої карти **разом з самою картою**.

2. **Забезпечте належний захист даних телефонної автентифікації** користувача платіжної карти АТ «БАНК «ГРАНТ»:

– **не повідомляйте стороннім особам таємне питання та відповідь**, що використовуються для телефонної автентифікації користувача платіжної карти;

– **не записуйте та не зберігайте таємне питання та відповідь**, що використовуються для телефонної автентифікації користувача платіжної карти, у місцях, до яких можуть мати доступ сторонні особи.

3. **Забезпечте належний захист** Вашої платіжної карти **під час користування банкоматами**:

– **надавайте перевагу банкоматам**, розташованим **у відділеннях банків, великих торгівельних або торгівельно-розважальних центрах, супермаркетах** тощо;

– **надавайте перевагу банкоматам**, розташованим **у середині приміщень**;

– **перед використанням** банкомату візуального його огляньте та **переконайтеся у відсутності видимих накладок** на картоприймачі, клавіатурі або отворі для видачі грошей, а також **інших сторонніх пристроїв** незрозумілого призначення;

– **прикривайте клавіатуру** рукою під час введення ПІН-коду.

4. **Забезпечте належний захист** Вашої платіжної карти **під час розрахунків у POS-терміналах**:

– **перед здійсненням** розрахункової **операції** завжди **переконуйтеся, що сума** списання, відображена на екрані терміналу, **зазначена вірно**;

– **надавайте перевагу** здійсненням розрахунків із використанням **чипу**, а не магнітної стрічки, якщо дозволяють технічні характеристики терміналу та Вашої карти;

– **самостійно виконуйте всі операції** із терміналом (зокрема, для зчитування магнітної стрічки/чипу) та **не передавайте** Вашу платіжну **карту** співробітникам установи, за послуги якої здійснюєте розрахунок;

– **не користуйтеся терміналами**, **що не потребують попередньої авторизації** для списання коштів (транзакція виконується без введення ПІН-коду);

– **не використовуйте** для розрахунків у POS-терміналах платіжну **карту, на рахунку якої** постійно зберігаються та/або періодично надходять **значні грошові кошти[2]**.

Примітки 2

Для розрахунків краще замовити окрему платіжну карту та здійснювати переказ коштів на її рахунок, наприклад, за допомогою системи дистанційного банківського обслуговування «СМАРТ-ГРАНТ», невеликими сумами.

У цьому випадку, навіть у разі отримання шахраями даних Вашої карти, достатніх для її підроблення, Ви ризикуєте лише сумою переказу, тоді як решта Ваших коштів залишається у безпеці.

5. **Забезпечте належний захист** Вашої платіжної карти під час розрахунків **у мережі Інтернет**:

– **здійснюйте онлайн-розрахунки виключно на перевірених сайтах** великих Інтернет-магазинів, постачальників послуг тощо та **уважно перевіряйте їх адресу[3];**

Примітки 3

Наголошуємо, що шахраї можуть створювати сайти - «клони» справжніх Інтернет-магазинів, постачальників послуг тощо з ідентичним оформленням. Тому перед здійсненням розрахунків слід уважно перевірити дані, зазначені у адресному рядку браузера.

У разі виявлення у написанні імені сайту:

1) зайвих цифр або букв;

Наприклад, https://booking1.uz.gov.ua/ru/ *замість* https://booking.uz.gov.ua/ru/

2) незначних відмінностей у написанні

Наприклад, https://booking.us.gov.ua/ru/ *, замість* https://booking.uz.gov.ua/ru/

3)використання піддомену у адресі сайту

Наприклад, https://booking.uz.com.gov.ua/ru/ *, замість* https://booking.uz.gov.ua/ru/

ВІДМОВТЕСЯ від здійснення платіжної операції.

Також, перед здійснення онлайн-розрахунку, доцільно перевірити, чи не входить веб-сайт до «чорного списку» за посиланням ***https://www.ema.com.ua/citizens/blacklist/***

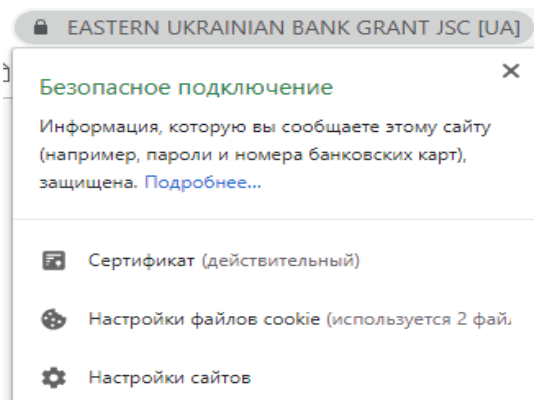
– **перед введенням** конфіденційних даних Вашої платіжної карти, **переконайтеся**, що обраний Вами **сайт використовує безпечний протокол** передачі даних (адреса сайту починається з «https://»), а наданий йому сертифікат є чинним[4];

Примітки 4

Для перевірки чинності сертифікату:

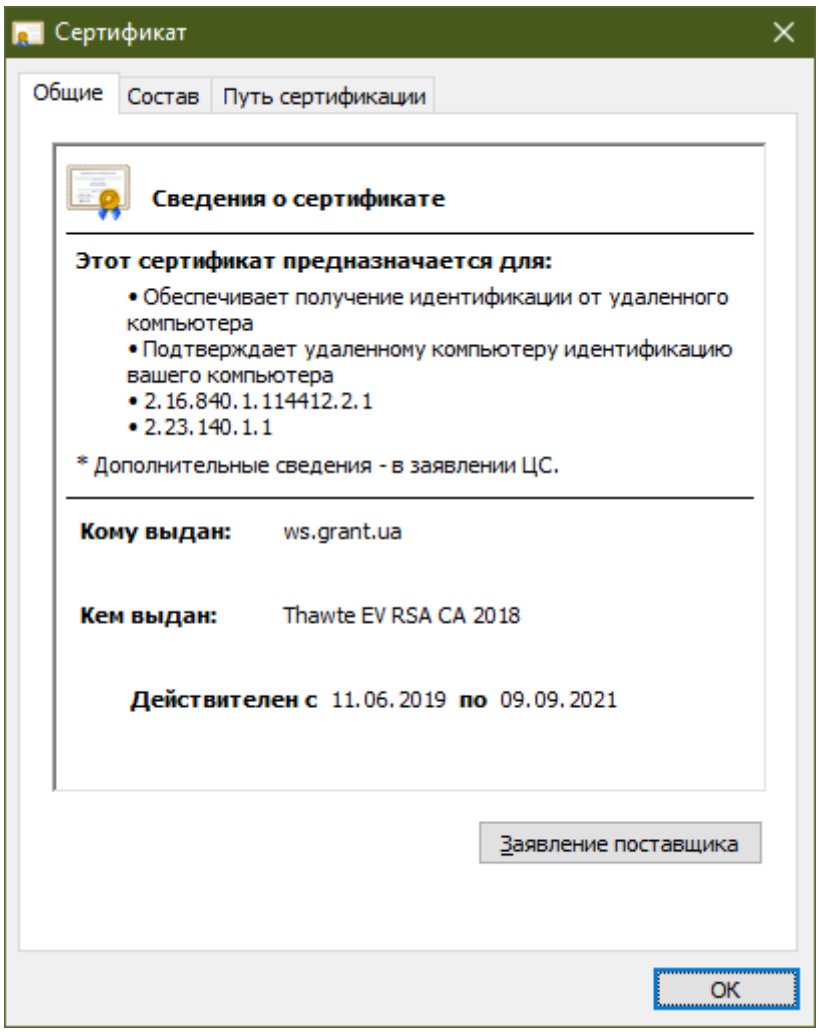
1. Кликніть лівою кнопкою миші по значку

2. У відкритому вікні кликніть лівою кнопкою миші по пункту Сертифікат



Примітки 4 (продовження)

3. Уважно ***перевірте відомості про те кому виданий сертифікат*** *(чи співпадають дані про власника, зазначені у сертифікаті, та дані сайту),* ***ким він виданий*** *(чи не є видавач та власник однією особою)* ***та строк чинності сертифіката****.*



У разі виникнення сумніві щодо будь-якого з зазначених реквізитів сертифікату ВІДМОВТЕСЯ від здійснення платіжної операції.

– **не використовуйте** для онлайн-розрахунків платіжну **карту, на рахунку якої** постійно зберігаються та/або періодично надходять **значні грошові кошти**[5];

Примітки 5

Наголошуємо, що у разі отримання шахраями повних реквізитів Вашої карти (її номер, строк дії та CVV-код), Ви ризикуєте втратите всі кошти, що зберігаються на її рахунку.

Для онлайн-розрахунків краще замовити окрему платіжну карту та здійснювати переказ коштів на її рахунок, наприклад, за допомогою системи дистанційного банківського обслуговування «СМАРТ-ГРАНТ», безпосередньо перед онлайн-покупкою.

У цьому випадку, навіть у разі отримання шахраями повних реквізитів Вашої карти, Ви ризикуєте лише сумою переказу, тоді як решта Ваших коштів залишається у безпеці.

– **не зберігайте** повні **реквізити** Вашої платіжної карти (її номер, строк дії та CVV-код) **у пам'яті браузера**;

– **не записуйте та не зберігайте** повні **реквізити** Вашої платіжної карти (її номер, строк дії та CVV-код) в блокнотах, на папірцях, у текстових файлах тощо;

– **використовуйте** сучасне **антивірусне програмне забезпечення**, для якого постійно **надходять оновлення** антивірусних баз даних, та проводьте **періодичні перевірки** комп'ютера/мобільного обладнання, на якому здійснюються онлайн-розрахунки, на наявність зловмисного коду (щонайменше 1 раз на місяць);

– **забезпечуйте** своєчасне **встановлення оновлень безпеки** операційної системи, браузерів та іншого програмного забезпечення комп'ютера/мобільного обладнання, що використовується для здійснення онлайн-розрахунків;

– **не використовуйте** на комп'ютері, що використовується для здійснення онлайн-розрахунків, системне або прикладне **програмне забезпечення**, для якого офіційно **припинено підтримку виробника** (не надходять більше оновлення безпеки, що усувають наявні технічні вразливості);

– **не встановлюйте** жодне **неперевірене або неліцензійне програмне забезпечення**, наприклад, завантажене з ресурсів безкоштовного файлового обміну у мережі Інтернет;

– **здійснюйте установку та оновлення** будь-якого програмного забезпечення лише **з офіційних сайтів** виробників.

Примітки 6

Наголошуємо, що шкідливе програмне забезпечення здатне перехоплювати будь-які дані з персональних комп'ютерів/мобільного обладнання клієнтів та зберігати/поширювати таку інформацію для подальшого несанкціонованого використання сторонніми особами злочинним шляхом.

УВАГА!

У разі виявлення:

- втрати платіжної карти АТ «БАНК «ГРАНТ» або виникнення такої підозри;
- компрометації конфіденційних даних платіжної карти (ПІН-коду, строку дії карти або CVV-коду) або виникнення такої підозри;
- несанкціонованого доступу до платіжної карти АТ «БАНК «ГРАНТ» або виникнення такої підозри;
- платіжних операцій, які Ви не виконували;
- тощо.

НЕГАЙНО повідомляйте про виявлені факти Службу підтримки Клієнтів для термінового блокування платіжної карти **за телефонами:**

- (057) 714 17 41;
- 063 495 97 77;

- 050 404 17 41;
- 067 574 74 41.

Примітка 7

Нагадуємо, що відповідно до вимог чинного законодавства України до моменту повідомлення користувачем Банку про втрату електронного платіжного засобу та/або платіжні операції, які він не виконував, ризик збитків від здійснення операцій та відповідальність несе користувач.

Тож до моменту повідомлення Банку про факт несанкціонованого доступу до платіжної карти АТ «БАНК «ГРАНТ» та/або події, що можуть його спричинити, дії Банку щодо здійснення операцій за рахунками Клієнта з використанням електронного платіжного засобу є правомірними.

З метою попередження можливих збитків від шахрайських дій сторонніх осіб із використанням електронних платіжних засобів просимо Вас неухильно дотримуватись:

– організаційних та технологічних заходів безпеки, передбачених договором банківського обслуговування з використанням електронного платіжного засобу;

– цих рекомендацій щодо безпечного використання електронного платіжного засобу.

Точне виконання цих правил позбавить Вас від проблем і неприємностей та забезпечить безпеку Ваших коштів на поточному рахунку.

Якщо у Вас є якісь сумніви у правильності Ваших дій або неясні питання, ми завжди готові надати Вам допомогу.