Рекомендації щодо виявлення фішингових веб-сайтів

Шановні клієнти!

У зв'язку зі зростанням кількості кіберзлочинів, пов'язаних з крадіжками конфіденційних даних клієнтів для подальшого несанкціонованого переказу коштів з їх рахунків, за допомогою фішингових сайтів – «клонів» справжніх Інтернет-магазинів, постачальників послуг, Інтернет-банкінгів, та з метою попередження можливих збитків від шахрайських дій сторонніх осіб, **наполегливо просимо Вас** під час виконання розрахунків у мережі Інтернет **дотримуватись** нижченаведених **заходів безпеки**.

1. **Будьте пильні** під час роботи у мережі Інтернет **та пам'ятайте, що фішинговий сайт — це шахрайський веб-ресурс**, який виманює реквізити платіжних карток під виглядом надання послуг, що не існують (наприклад, поповнення мобільного рахунку, переказів з картки на картку), або веб-ресурс організації, якій користувач довіряє (наприклад, клон інтернет-банку), що має на меті збір конфіденційних даних, що використовуються для доступу до систем дистанційного банківського обслуговування (логін, пароль, код авторизації), для подальшої крадіжки грошових коштів з рахунків довірливих клієнтів.

2. Завжди **користуйтеся лише перевіреними джерелами інформації.**

Пам'ятайте, єдиними інформаційними ресурсами АТ «БАНК «ГРАНТ» у мережі Інтернет є:

- **https://www.grant.ua** – офіційний веб-сайт АТ «БАНК «ГРАНТ» у мережі Інтернет;
- **https://ws.grant.ua –** офіційна сторінка системи дистанційного банківського обслуговування «СМАРТ-ГРАНТ».

3.**Здійснюйте доступ** до системи дистанційного банківського обслуговування «СМАРТ-ГРАНТ» виключно **офіційними каналами**:

– **здійснюйте вхід** до веб-додатку «СМАРТ-ГРАНТ» виключно **на** офіційному **сайті** системи **https://ws.grant.ua;**

– **здійснюйте завантаження** мобільного додатку «СМАРТ-ГРАНТ» виключно **за посиланням** на App Store/Google Play, розміщеним **на** офіційному **сайті Банку https://www.grant.ua.**

4. **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[1];**

Примітки 1

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 вебсайт до «чорного списку» за посиланням ***https://www.ema.com.ua/citizens/blacklist/***

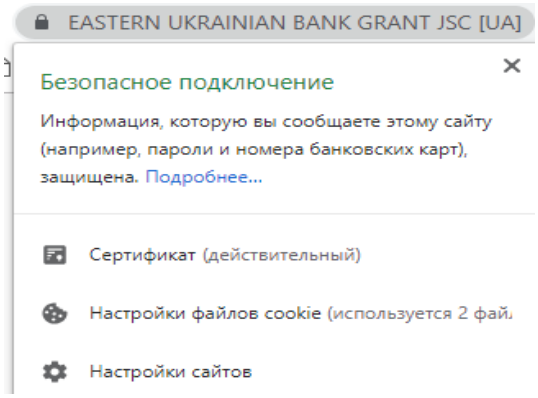
– **перед введенням** конфіденційних даних Вашої платіжної карти, **переконайтеся**, що обраний Вами **сайт використовує безпечний протокол** передачі даних (адреса сайту починається з «https://»), а наданий йому сертифікат є чинним[2];

Примітки 2

Для перевірки чинності сертифікату:

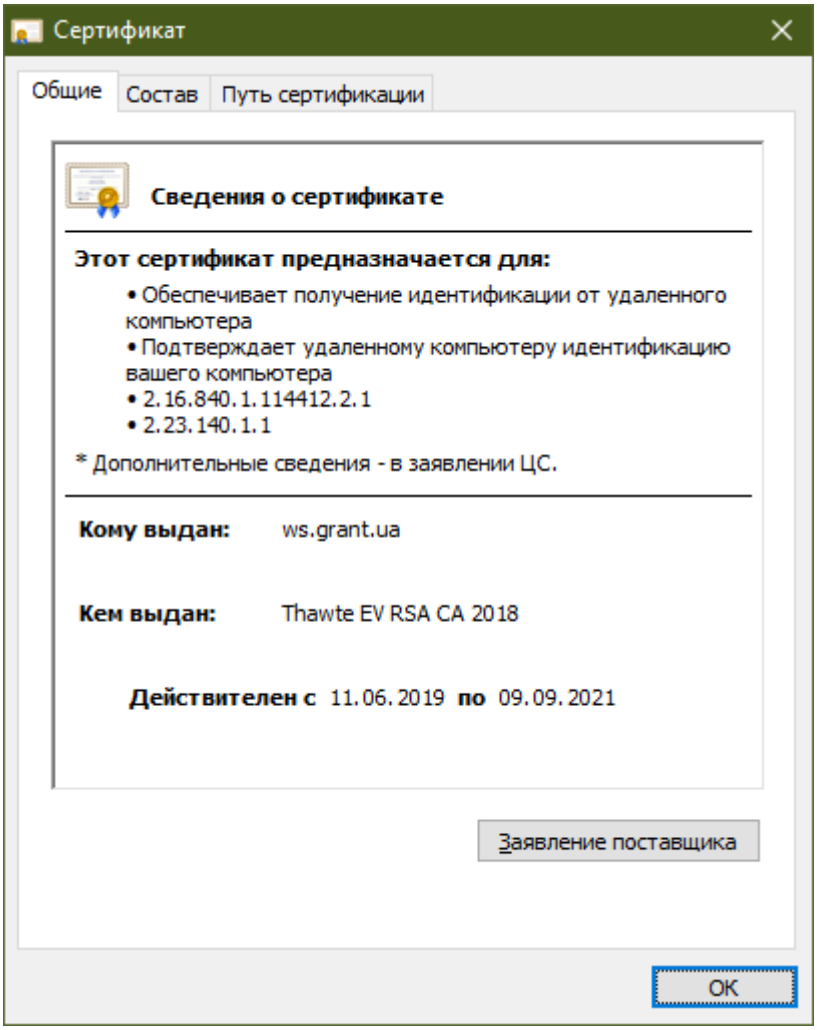
1. Кликніть лівою кнопкою миші по значку

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



Примітки 2 (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**[3];

Примітки 3

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.