

Рекомендації щодо безпечного використання системи дистанційного банківського обслуговування «СМАРТ-ГРАНТ»

Шановні клієнти!

У зв'язку зі зростанням кількості кіберзлочинів, пов'язаних з несанкціонованим переказом коштів з рахунків клієнтів, які обслуговуються за допомогою систем дистанційного банківського обслуговування, та з метою попередження можливих збитків від шахрайських дій сторонніх осіб, **наполегливо просимо Вас** під час використання системи «СМАРТ-ГРАНТ» **дотримуватись** нижченаведених організаційних та технологічних заходів безпеки.

№ з/п	Зміст рекомендація	Поради для користувачів	
		Веб-додатку	Мобільного додатку
1	Здійснюйте доступ до системи «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
2	Забезпечте належний захист обладнання, що використовується для роботи у системі «СМАРТ-ГРАНТ»	– використовуйте сучасне антивірусне програмне забезпечення , для якого постійно надходять оновлення антивірусних баз даних, та проводьте періодичні перевірки комп'ютера на наявність зловмисного коду ¹ (щонайменше 1 раз на місяць); – забезпечуйте своєчасне встановлення оновлень безпеки операційної системи, браузерів та іншого програмного забезпечення комп'ютера, що використовується для роботи	– використовуйте сучасне антивірусне програмне забезпечення , для якого постійно надходять оновлення антивірусних баз даних, та проводьте періодичні перевірки мобільного обладнання на наявність зловмисного коду ¹ (щонайменше 1 раз на місяць); – забезпечуйте своєчасне встановлення оновлень безпеки операційної системи та іншого програмного забезпечення

¹ 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.

		<p>у системи «СМАРТ-ГРАНТ»;</p> <p>– не використовуйте на комп'ютері, що використовується для роботи у системи «СМАРТ-ГРАНТ», системне або прикладне програмне забезпечення, для якого офіційно припинено підтримку виробника (не надходять більше оновлення безпеки, що усувають наявні технічні вразливості);</p> <p>– не встановлюйте жодне неперевірене або неліцензійне програмне забезпечення, наприклад, завантажене з ресурсів безкоштовного файлового обміну у мережі Інтернет;</p> <p>– здійсніть установку та оновлення будь-якого програмного забезпечення лише з офіційних сайтів виробників.</p>	<p>мобільного обладнання, на якому встановлено мобільний додаток «СМАРТ-ГРАНТ»;</p> <p>– здійсніть установку та оновлення будь-якого програмного забезпечення лише з офіційних магазинів App Store, Google Play тощо.</p>
3	<p>Забезпечте належний захист конфіденційних даних², що використовуються для</p>	<p>– встановлюйте надійний пароль³ доступу до системи «СМАРТ-ГРАНТ»;</p> <p>– не записуйте Логін та/або пароль доступу до системи «СМАРТ-ГРАНТ» в блокнотах, на</p>	<p>– встановлюйте надійний пароль³ доступу до мобільного додатку «СМАРТ-ГРАНТ»;</p> <p>– не записуйте Логін та/або пароль доступу до мобільного додатку «СМАРТ-</p>

² Логін, пароль та код авторизації

³ Для створення надійного паролю доступу варто керуватися наступними принципами:

- пароль повинен містити не менше 8 символів;
- пароль повинен містити літери як верхнього (A-Z), так і нижнього регістру (a-z), числа (0-9), а також спец символи (@, ! тощо);
- НЕ слід використовувати в якості пароля своє ім'я або прізвище, дату свого народження, найпоширеніші паролі (qwerty, 123456, 098765, 1111, password) тощо;

	отримання доступу до системи «СМАРТ-ГРАНТ»	<p>папірцях, у текстових файлах тощо;</p> <ul style="list-style-type: none"> – не зберігайте Логін та/або пароль доступу до системи «СМАРТ-ГРАНТ» у пам'яті браузера; – нікому, зокрема співробітникам Банку⁴, не повідомляйте пароль доступу та/або код авторизації до системи «СМАРТ-ГРАНТ»; – нікому не передавайте телефон (SIM-картку), на номер якого надсилаються коди авторизації до системи «СМАРТ-ГРАНТ»; – не залишайте без особистого нагляду телефон (SIM-картку), на номер якого надсилаються коди авторизації до системи «СМАРТ-ГРАНТ»; – в налаштуваннях телефону забороніть відображення тексту SMS-повідомлень на екрані блокування. 	<p>ГРАНТ» в блокнотах, на папірцях, у текстових файлах тощо;</p> <ul style="list-style-type: none"> – нікому, зокрема співробітникам Банку⁴, не повідомляйте пароль доступу та/або код авторизації до мобільного додатку «СМАРТ-ГРАНТ»; – нікому не передавайте мобільне обладнання, на якому інстальовано мобільний додаток «СМАРТ-ГРАНТ»; – не залишайте без особистого нагляду мобільне обладнання, на якому інстальовано мобільний додаток «СМАРТ-ГРАНТ»; – в налаштуваннях мобільного обладнання забороніть відображення тексту SMS-повідомлень на екрані блокування.
4.	Забезпечте належний захист даних телефонної автентифікації ⁵	<ul style="list-style-type: none"> – не повідомляйте стороннім особам дані, що використовуються для телефонної автентифікації користувачів системи «СМАРТ-ГРАНТ»; – не записуйте дані, що використовуються для телефонної автентифікації користувачів системи «СМАРТ-ГРАНТ», в блокнотах, на папірцях, у текстових файлах тощо. 	

⁴ Наголошуємо, що співробітники Банку при здійсненні технічної підтримки та наданні консультацій щодо використання системи «СМАРТ-ГРАНТ» ніколи не цікавляться інформацією про паролі та/або коди авторизації.

⁵ Таємне питання та відповідь

УВАГА!

У разі виявлення:

- втрати телефону (SIM-картки), на номер якого надсилаються коди авторизації до системи «СМАРТ-ГРАНТ»;
- втрати мобільного обладнання, на якому інстальовано мобільний додаток «СМАРТ-ГРАНТ»;
- несанкціонованого доступу до системи «СМАРТ-ГРАНТ» або виникнення підозри про такий доступ;
- несанкціонованої зміни інформації Клієнта в системі «СМАРТ-ГРАНТ» або виникнення підозри про таку зміну;
- тощо.

НЕГАЙНО повідомляйте про виявлені факти Службу підтримки Клієнтів для термінового блокування роботи Клієнта системі «СМАРТ-ГРАНТ» до з'ясування обставин **за телефонами:**

- (057) 714 17 41;
- 063 495 97 77;
- 050 404 17 41;
- 067 574 74 41.

Примітка

Нагадуємо, що відповідно до умов Публічної пропозиції (оферта) на укладення Договору на банківське обслуговування фізичної особи з використанням системи дистанційного банківського обслуговування «СМАРТ-ГРАНТ», особа, яка ввела правильний код авторизації та пройшла верифікацію в системі «СМАРТ-ГРАНТ», вважається для Банку Клієнтом та всі дії, що зроблені нею в системі «СМАРТ-ГРАНТ», включаючи проведені банківські операції, вважаються Банком такими, що здійснені Клієнтом особисто та від власного імені.

Тож до моменту повідомлення Банку про факт несанкціонованого доступу до системи «СМАРТ-ГРАНТ» та/або події, що можуть його спричинити, дії Банку щодо здійснення операцій за рахунками Клієнта на підставі даних, які надійшли засобами системи «СМАРТ-ГРАНТ», є правомірними.

З метою попередження можливих збитків від шахрайських дій сторонніх осіб із використанням системи дистанційного банківського обслуговування просимо Вас неухильно дотримуватись:

– організаційних та технологічних заходів безпеки, передбачених Публічною пропозицією (оферта) на укладення Договору на банківське обслуговування фізичної особи з використанням системи дистанційного банківського обслуговування

«СМАРТ-ГРАНТ»;

– цих рекомендацій щодо безпечного використання системи «СМАРТ-ГРАНТ».

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.