Рекомендації з питань безпеки використання систем дистанційного банківського обслуговування

Шановні клієнти!

Унеможливлюйте відвідування Інтернету з персонального комп'ютеру, на якому здійснюється підготовка та відправка документів до банку. Не відвідуйте сайтів сумнівного змісту та будь-яких інших Інтернет-ресурсів невиробничого характеру (соціальні мережі, конференції та чати, телефонні сервіси т. п.). Не читайте пошту та не відкривайте поштових вкладень до електронних листів, які надійшли від невідомих або підозрілих адресатів . Не слід здійснювати установку та оновлення будь-якого програмного забезпечення не з офіційних сайтів виробників.

- Налаштовуйте окремо мережеве обладнання, корпоративних і персональних комп'ютерів. Доступ до мережі Інтернет обмежуйте «білим списком» сайтів з усіх робочих місць, на яких здійснюється підготовка, підписання та відправлення платіжних документів. У «білий список» повинні включатися виключно перевірені сайти самої організації, банків, податкової служби, інших державних органів, доступ до яких необхідний у виробничому процесі, сервери оновлень системного та антивірусного програмного забезпечення.

- Мінімізуйте кількість користувачів комп'ютерів, на яких здійснюється підготовка та відправка документів до банку. Доцільно обмежити фізичний доступ до персональних комп'ютерів, на яких здійснюється підготовка та відправка документів у банк (надавати доступ виключно відповідальним працівникам, які безпосередньо уповноважені та мають право проводити роботи з програмним забезпеченням системи ДБО).

- Використовуйте сучасне антивірусне забезпечення, оновлюйте та проводьте антивірусну перевірку на комп'ютерах. Наголошуємо, що шкідливе програмне забезпечення здатне перехоплювати будь-які дані з банків, персональних комп'ютерів клієнтів та/або особистих даних держателів ЕПЗ та зберігати/поширювати таку інформацію для подальшого несанкціонованого використання сторонніми особами злочинним шляхом.

- Забезпечуйте своєчасне встановлення оновлень безпеки операційної системи, браузерів та програмного забезпечення комп'ютерів. Необхідно встановити надійні паролі доступу на вхід до персонального комп'ютера, забезпечити періодичну зміну цих паролів.

- Не допускайте несанкціонованого використання ключів електронного цифрового підпису, зберігайте ключові носії у спосіб, що виключає несанкціонований доступ до них. Генерацію секретних ключів слід виконувати тільки самостійно. Нікому (у тому числі працівникам банку) не повідомляти та не передавати паролі до особистих секретних ключів. Не записувати і не зберігати паролі разом з носієм ключа."