МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ

ДЕРЖАВНЕ ПІДПРИЄМСТВО
«НАЦІОНАЛЬНІ ІНФОРМАЦІЙНІ СИСТЕМИ»
ДНІПРОПЕТРОВСЬКА РЕГІОНАЛЬНА ФІЛІЯ

пр. Дмитра Яворницького, 104А, м. Дніпро, 49038 тел.: (056) 720-90-81
E-mail: inbox_dp@nais.gov.ua

Південно-Східне міжрегіональне управління Міністерства юстиції (м. Дніпро)

Начальнику управління Лєгостаєву І.М.

пр. Д.Яворницького, 21-А,
м.Дніпро, 49027

Шановний Іване Миколайовичу!

Державне підприємство «Національні інформаційні системи» повідомляє про зафіксовані непоодинокі розсилки зловмисниками листів різного контексту на електронну пошту нібито від імені державних установ, зі вкладенням шкідливого програмного забезпечення, що встановлює на комп'ютер користувача віддалений прихований доступ та відправляє документи на підконтрольні їм сервери.

Для запобігання можливому доступу сторонніх осіб до інформації Єдиних та державних реєстрів Міністерства юстиції України за особистими атрибутами доступу, користувачам також пропонуємо дотримуватися наведених нижче рекомендацій, а саме:

1. Не завантажувати зашифровані архіви або архіви під паролем. За необхідності зверніться до відправника для уточнення факту відправлення листа із вкладенням. Рекомендовано взагалі заблокувати отримання таких файлів через електронну пошту.

2. Перш ніж відкрити вкладення в електронних листах чи повідомленнях, звертайте увагу на деталі. Краще утриматися від завантаження вкладень електронних листів від сумнівних відправників. Також звертайте увагу на зміну мови спілкування, нетипової для автора теми листа, а також на повідомлення, що спонукають перейти за підозрілими посиланнями або відкрити підозрілі файли.

3. Обмежте можливість запуску виконуваних файлів.

4. Для проведення реєстраційних дій у Реєстрах використовувати окремий спеціально налаштований комп'ютер за можливості з фіксованою IPадресою та без доступу до публічних мереж WI-FI.

5. Для роботи з Реєстрами використовувати захищений носій особистих ключів з вбудованими програмно-апаратними засобами, що має позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації та виданий акредитованим центром сертифікації.

6. Не використовувати нештатні носії інформації (флеш-носії, карти пам'яті, диски, мобільні телефони, смартфони, планшети, MP3/MP4 – плеєри тощо) на комп'ютері, призначеному для роботи з Реєстрами, у тому числі, з метою заряду акумуляторів.

7. Не розголошувати ідентифікатори доступу до системи, а також пароль доступу до особистого ключа, не залишати без нагляду та не передавати захищений носій ключової інформації іншим особам. За необхідності фіксування паролів на паперових носіях, зберігати останні у сейфі (сховищі).

8. Використовувати різні паролі для доступу до Реєстрів та особистого ключа ЕЦП.

9. Регулярно змінювати паролі доступу до особистого ключа ЕЦП з використанням багатосимвольних комбінацій з прописних і строкових літер, цифр та спеціальних символів. Здійснювати негайну зміну у разі підозри щодо їх компрометації.

10. Не використовувати в якості паролю власні ім'я, прізвище, номер телефону, дату народження тощо, сталі фрази зі щоденного вжитку, назв популярних літературних творів та пісень, поширених цитат та фрагментів текстів з них.

11. Використовувати виключно ліцензійне програмного забезпечення у мінімально необхідній кількості (операційна система, браузери, офісні програми тощо). Не встановлювати додаткових програмних засобів на комп'ютері, призначеному для роботи з Реєстрами, окрім тих, що необхідні для роботи. Не встановлювати додатки та «плагіни» розширення функціональності браузерів окрім тих, що необхідні для роботи з Реєстрами.

12. Встановлене програмне забезпечення повинно регулярно оновлюватись до останніх версій та включати всі останні оновлення та патчі, включаючи останні критичні оновлення та оновлення безпеки, від виробників цих програмних продуктів (операційна система, браузери, офісні програми тощо).

13. Обов'язково встановити пароль на вхід до операційної системи з дотриманням вимог у пункті 8.

14. Створити окремий обліковий запис в операційній системі Windows без прав адміністратора для роботи з Реєстрами та документами.

15. Вимкнути функції віддаленого доступу та автоматичного завантаження сторонніх програм, що дозволяють віддалене управління комп'ютером.

16. Відключити автоматичний запуск програм із змінних (зовнішніх) пристроїв та носіїв інформації, у тому числі в обліковому записі адміністратора.

17. Використовувати виключно ліцензійне антивірусне програмне забезпечення, що має чинний позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації, з актуальними антивірусними базами даних. Два рази на тиждень та при підозрі зараження здійснювати повну антивірусну перевірку комп'ютера.

18. Здійснювати антивірусну перевірку всіх змінних (зовнішніх) пристроїв та носіїв інформації перед кожним їх використанням.

19. Утримуватись від застосування на комп'ютері для доступу до Реєстрів рекомендацій про налаштування антивірусів, які примушують систему захисту комп'ютера ігнорувати будь-яку підозрілу активність. Такі рекомендації можуть поширюватись певними компаніями-розробниками ПЗ (зокрема бухгалтерського) або їх партнерами в мережі Інтернет та через технічну підтримку.

20. Не використовувати засоби електронного поштового листування, у тому числі, мобільні онлайн-додатки для дзвінків і обміну повідомленнями (месенджери), на комп'ютерному робочому місці, призначеному для роботи з Реєстрами. Під час користування електронною поштою з інших робочих місць та засобів комунікації, не відкривати електронні листи від невідомих адресатів, особливо з прикріпленими файлами, не переходити за наведеними в листах посиланнями.

21. Не залишати носії з ключами ЕЦП у комп'ютері, а також відкриті сесії роботи з Реєстрами у разі необхідності тимчасового залишення робочого місця.

22. Не залишати фахівця з налаштування комп'ютерної техніки сам на сам з комп'ютером, на якому встановлено програмне забезпечення для роботи з Реєстрами, та не надавати йому паролі і ключі (пункт 5).

З метою підвищення рівня безпеки та запобігання можливої компрометації, просимо довести до відома про зазначене приватним та державним нотаріусам, державним реєстраторам, державним та приватним виконавцям, а також співробітникам ВДРАЦ регіону.

З повагою

Директор філії **Вікторія САМОЙЛЕНКО**

Гвритишвілі 056 720 91 49