|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | |  | |  |
| **ПРЕЗИДІЯ НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ**  **РОЗПОРЯДЖЕННЯ № 643** | | | | |
| м. Київ |  | | “ 17 ” 12 2020 р. | |

Про заходи щодо кіберзахисту   
електронних інформаційних ресурсів

З метою недопущення завдання шкоди державним інтересам та відповідно до листа Головного управління контррозвідувального захисту інтересів держави у сфері економічної безпеки Служби безпеки України від 13.11.2020 №7047 щодо кіберзахисту державних електронних інформаційних ресурсів, а також враховуючи надані у згаданому листі Рекомендації щодо виявлення можливих загроз безпечній роботі в інформаційно-комунікаційних мережах та недопущення використання в роботі фішингових сайтів (далі – Рекомендації щодо захисту від фішингу):

1. Установам, організаціям і підприємствам НАН України з залученням відповідних фахівців вжити заходів щодо ознайомлення працівників, які використовують персональні комп’ютери при виконанні службових обов’язків, з Рекомендаціями щодо захисту від фішингу (додаються), способами використання їх на практиці та перевагами від їхнього дотримання.

2. Керівникам установ, організацій і підприємств НАН України забезпечити обов’язкове дотримання Рекомендацій щодо захисту від фішингу під час роботи на персональних комп’ютерах з інформацією (даними), викрадення або знищення якої може створювати небезпеку життєво важливим інтересам України.

3. Центру практичної інформатики НАН України надавати уповноваженим представникам наукових установ, організацій і підприємств НАН України, підрозділів апарату Президії НАН України консультаційно-методичну допомогу щодо виявлення можливих загроз безпечній роботі в інформаційно-комунікаційних мережах та недопущення використання в роботі фішингових сайтів.

4. Контроль за виконанням цього розпорядження покласти на Науково-організаційний відділ Президії НАН України.

Президент

Національної академії наук України

академік НАН України **А.Г.Загородній**

В.о.головного вченого секретаря

Національної академії наук України

академік НАН України **В.Л.Богданов**

Букало В.П.

239-65-72

Рекомендації щодо виявлення можливих загроз безпечній роботі в інформаційно-комунікаційних мережах та недопущення використання в роботі фішингових сайтів

1. Обов’язково перевіряти URL-адресу, на яку рекомендується перейти, на наявність незначних помилок у написанні.

2. Використовувати тільки безпечні https–з’єднання (відсутність літери "s" у адресі сайту є однією з ознак фішингу).

3. Здійснювати перевірку усіх листів із вкладеннями та гіперпосиланнями (навіть у разі надходження зі знайомої адреси).

4. При отриманні підозрілого листа повідомити про це відправника.

5. Використовувати двофакторну автентифікацію у всіх акаунтах (профілях) користувача.

6. Регулярно здійснювати оновлення веб-переглядача (браузера) та антивірусного програмного забезпечення (більшість браузерів мають функцію визначення фішингових сайтів).

7. Перевіряти усі вкладення в електронних листах за допомогою антивірусного програмного забезпечення з актуальним оновленням та, у разі підозри, використовувати динамічний аналіз файлів у так званій "пісочниці" (бажано офлайн, наприклад Sandboxie).

Довідково: безкоштовна утиліта Sandboxie – це засіб для контролю за роботою різних програм, а також підвищення рівня безпеки, у тому числі при роботі в мережі Інтернет. Програма надає користувачам можливість запуску додатків у захищеній оболонці ("пісочниця"). Додаток, який працює у "пісочниці", не може вносити будь-які записи у дані системного реєстру, отримувати доступ до системних файлів або вносити зміни у систему чи вплинути на її працездатність.

Зазначене програмне забезпечення підвищує захист операційної системи від встановлення небажаного програмного забезпечення під час веб-серфінгу в мережі Інтернет, а також слідкує за роботою електронної пошти, використовуючи власну "пастку" для шкідливого програмного забезпечення, прикріпленого до листа.

Кількість таких віртуальних "пісочниць" не обмежується. При цьому користувач має змогу самостійно скласти перелік програм, які будуть автоматично запускатися у них, а також налаштовувати для кожної з них рівні дозволу до різних ресурсів.

Слід зазначити, що онлайн сервіси (VirusTotal, Hybrid Analysis, JOE Sandbox та інші) надають користувачам можливість завантажувати файли, що проходили аналіз з їх використанням, а також здійснювати пошук таких файлів за ключовими словами.

8. Усі підозрілі вкладення у листах рекомендується пересилати до ГУ КЗЕ Служби безпеки України та Ситуаційного центру забезпечення кібербезпеки ДКІБ Служби безпеки України (incident@dis.gov.ua).

9. У разі надходження підозрілого листа здійснювати перевірку його службового заголовку на предмет наявності підміни адреси відправника.