Додаток до наказу
від «28» 02.2024 № 12

ПАМ'ЯТКА
з правил кібергігієни в Головному управлінні Держпродспоживслужби в Луганській області

1. Публічні мережі

Уникайте підключення до публічних (відкритих) Wi-Fi мереж. Завжди використовуйте VPN для шифрування вашого інтернет – трафіку, уникайте використання чутливої інформації на публічних мережах, завжди перевіряйте правильність назви точки доступу і уникайте відкритих мереж безпосередньо для важливих операцій.

2. Антивірусне програмне забезпечення

Використання антивірусного програмного забезпечення (ПЗ) важливе з кількох причин:

- Захист від вірусів і шкідливих програм: Антивірусне ПЗ виявляє та блокує віруси, черв'яки, троянці, шпигунське ПЗ та інші види шкідливих програм, що можуть пошкодити ваші файли, використовувати ваші дані або навіть пошкодити операційну систему.
- Захист особистої інформації: Антивірусне ПЗ допомагає захистити ваші особисті дані, такі як паролі, фінансові дані та конфіденційну інформацію від крадіжки або зламу.
- Захист від онлайн загроз: Воно також може захищати вас від онлайн загроз, таких як шкідливі посилання, фішингові атаки та інші спроби шахрайства, забезпечуючи безпечніше переглядання веб-сторінок та електронної пошти.
- Виявлення та блокування нових загроз: Багато антивірусних програм мають функцію "проактивного виявлення", яка допомагає виявляти нові загрози, навіть якщо вони ще не були визначені як віруси або інші види шкідливих програм.
- Оновлення баз даних: Більшість антивірусних програм оновлюють свої бази даних регулярно, щоб вони могли розпізнавати найновіші загрози. Такі оновлення забезпечують вашу систему захистом від найсучасніших атак.

3. Зберігання файлів

Архівуйте та зберігайте важливі документи, додатки, файли на з'ємних носіях. Це зменшує ризик втрати важливих даних та підвищує ефективність використання вільного простору пам'яті ваших пристроїв.

4. Оновлення

Слідкувати за оновленнями вкрай важливо, і ось чому:

- Безпека: Оновлення програмного забезпечення, операційних систем, антивірусних програм і т.д. часто містять виправлення для виявлених вразливостей. Невстановлені оновлення можуть залишити ваші пристрої вразливими перед шкідливими програмами та кібератаками.
- Функціональність: Часті оновлення можуть додавати нові функції або покращувати існуючі. Це може поліпшити продуктивність та зручність користування вашими пристроями чи програмами.
- Сумісність: Оновлення можуть вирішувати проблеми з сумісністю програмного забезпечення. При випуску нових версій операційних систем або програм вони можуть стати несумісними з певними версіями старіших програм, і оновлення можуть вирішити цю проблему.
- Відмова від підтримки: Розробники час від часу припиняють підтримку старих версій програмного забезпечення або операційних систем. Це означає, що без оновлень ви можете залишитися без необхідних патчів безпеки та інших важливих оновлень.

5. Надійний пароль

Створюйте надійні паролі, уникайте використання одного і того ж самого пароля для декількох систем.
Ознаками надійного пароля є:

- Мінімум 12 символів.
- Вміст спеціальних символів, цифр, великих та маленьких літер.
- Уникати використання легких шаблонів, серед яких дата народження, ім'я або місто.
- Уникати очевидних паролів по типу «0123456789», «password», «qwerty».

6. Перевіряйте вміст листів

Перевіряйте вміст листів електронної пошти які отримуєте. Не зберігайте вміст листів, якщо сталось так що ви зберегли файли то перед відкриттям скористайтесь сервісом «Virustotal» для перевірки вмісту таких файлів. Пам'ятайте що адреса з якої вам надсилають листи може бути скомпрометована.

7. Джерело відправки

Перевіряйте та аналізуйте адресу відправника підозрілих листів. Шахраї все частіше підроблюють відомі сервіси (наприклад системні повідомлення від поштових сервісів), та розповсюджують фішингові посилання ніби від

відомих вам ресурсів для «перевірки актуальності даних», або повідомлень на електронну пошту з текстом що «ваша пошта заблокується через 12 годин, перейдіть за посиланням щоб уникнути втрати важливих даних». Також звертайте увагу на орфографічні помилки, імена та номери телефонів які додають до листів для підвищення довіри та автентичності.

8. Особиста інформація

Не зберігайте файли які несуть в собі чутливу інформацію, корпоративні, особисті документи, інформацію щодо ваших акаунтів, банківських додатків тощо. В разі втрати пристрою, крадіжки, інформація може бути втрачена та використана проти вас.

9. Ліцензійне програмне забезпечення

Використовуйте ліцензійні програмні засоби, системи. При використанні неліцензійного програмного забезпечення підвищується ризик вразливостей до кібератак, використання такого програмного забезпечення порушує авторські права та ліцензійні угоди.

10. Довіряйте офіційному

Перевіряйте актуальну інформацію на офіційних веб порталах про:

Номери телефонів.
Електронні адреси (в тому числі електронні адреси окремих відділів).
Посадових осіб.