Головне управління Держпродспоживслужби в Донецькій області

Пам’ятка щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет.

Основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації.

РЕКОМЕНДАЦІЇ

І. Щодо користування електронною поштою (службовою і приватною):

1. Не використовувати приватну електронну пошту для цілей службової діяльності та службову електронну пошту в приватних цілях.
2. Не використовувати в браузерах можливість запам’ятовувати паролі.
3. Не використовувати паролі, що були встановлені «за замовчанням».
4. Використовувати виключно надійні (стійкі) паролі.

Під надійними паролями слід розуміти такі, що:

- складаються з не менше 8 символів;
- включають літери (у верхньому і нижньому регістрі), цифри та спеціальні символи;
- не містять персональної інформації (наприклад: дати народження своєї та своїх близьких, номерів телефонів, номерів та серій документів, що посвідчують особу, номерів власного автотранспорту, банківської картки, адреси реєстрації);
- не використовуються в будь-яких інших акаунтах.

5. Перевіряти всі файли, отримані електронною поштою, на предмет відсутності вірусів та шкідливого програмного забезпечення.
6. Не відкривати вкладень у підозрілих повідомленнях, листах від адресатів, щодо авторства яких виникають сумніви (наприклад: автор з невідомих причин змінив мову спілкування; тема листа є нетиповою для автора; спосіб, у який автор звертається до адресата, є нетиповим) у повідомленнях з нестандартним текстом, що спонукають до переходу на підозрілі посилання або до відкриття підозрілих файлів - архівів, виконуваних файлів та вкладень з виконуваними файлами, які мають, зокрема, розширення «.exe», «.bat», «.cmd», «.vbs», «.docm», «.xlsm». При отриманні таких листів на службову електронну пошту негайно повідомляти про такі листи адміністратора безпеки або відповідний підрозділ.
7. Не використовувати точки публічного доступу до Інтернету для входу до службової електронної пошти.

II. Щодо користування особистими пристроями (знімними/зовнішніми носіями інформації, комп'ютерами, планшетами, ноутбуками, смартфонами):

1. Установити паролі на всі пристрої, що перебувають в особистому користуванні (PIN-коди, паролі на вхід до всіх облікових записів) та блокувати пристрої щоразу після закінчення роботи з ними.

2. Налаштувати на усіх WIFI-пристоях використання технології WPA2 та періодично змінювати паролі доступу.

3. З метою унеможливлення завантаження на особистий пристрій програм-шпигунів та іншого шкідливого програмного забезпечення дотримуватися таких правил:
установлювати додатки лише з офіційних та перевірених сервісів (Chrome Store, Add-ons та Play Market для Android, App Store для IOS);
здійснити налаштування пристрою таким чином, щоб унеможливити автоматичне встановлення (оновлення) додатків з невідомих джерел;
періодично видаляти з особистих пристроїв додатки (програми), які не використовуються.

4. Постійно здійснювати оновлення операційних систем та іншого програмного забезпечення.

5. Використовувати антивірусне програмне забезпечення.

6. Регулярно створювати резервні копії важливої інформації. Для збереження резервних копій використовувати зовнішні носії інформації.

7. Не використовувати особисті пристрої (знімні/зовнішні носії інформації, комп'ютери, планшети, ноутбуки, смартфони) для обробки, зберігання та обміну інформацією, яка обробляється під час виконання службових обов'язків.

III. Щодо користування соціальними мережами (обов'язково для службових профілів, рекомендовано для особистих профілів)
Заборонено використовувати російські мобільні додатки, соціальні мережі «ВКонтакте» та «Одноклассники» та сервіси «Mail.ru» (відповідно до Указу Президента України від 15.04.2017 № 133).

IV. Щодо підключення до мережі Інтернет:
Одним із найпоширеніших способів входу до мережі Інтернет у публічних місцях є підключення до відкритих точок Wi-Fi. Зазвичай вони є безкоштовними та вхід до них здійснюється без введення паролів. Саме відсутність паролю робить їх вразливішими для злому з боку зацікавлених осіб, які мають на меті отримати доступ до персональних даних та відомостей, що зберігаються на телефоні, планшеті, комп'ютері.

1. Під час здійснення входу до мережі використовувати лише ті точки доступу до Wi-Fi, які мають протоколи безпеки для захисту бездротового з'єднання WPA чи WPA-2.

2. У публічних місцях найкраще користуватися особистим Wi-Fi модемом або здійснювати вхід до мережі Інтернет з мобільного пристрою за передплаченим пакетом послуг мобільного оператора та/або використовувати шифроване VPN-з’єднання до корпоративного чи особистого проксі-серверу.

V. Щодо убезпечення від фішингових атак

Фішинговий сайт – це шахрайський веб-ресурс, який розташовано за максимально схожою з офіційним сайтом доменною адресою (наприклад, statevvebsite.org.ua замість statewebsite.gov.ua) і який копіює його зовнішній вигляд (дизайн). Метою такого ресурсу є отримання персональних даних громадян, у тому числі їх паспортних даних або реквізитів платіжних карток, для подальшого використання в злочинних цілях.

Кіберзлочинці, використовуючи засоби соціальної інженерії, надсилають на електронні адреси громадян листи від імені державних установ та пропонують їм перейти за зазначеним посиланням для отримання «важливої» інформації або її «уточнення». Перейшовши за таким посиланням, громадянин потрапляє на копію реальної сторінки держустанови, де йому пропонують «зареєструватись» або будь-яким іншим чином внести необхідні шахраям дані.

1. Ставтеся з підозрою до листів з вкладеннями й посиланнями. Краще уточніть у відправника за телефоном, зазначеним на офіційному сайті державної установи, чи був надісланий Вам такий лист. Можливо, що адресу електронної пошти відправника могли підмінити або зламати.

2. Якщо Ви все ж таки вирішили перейти за будь-яким посиланням, що надійшло Вам на адресу електронної пошти, переконайтеся в правильності написання URL-адреси, за якою Вам пропонують перейти, у відсутності незначних помилок (відмінностей) у доменному імені державної установи. Усі державні установи в Україні мають єдине ім’я – gov.ua та вигляд statewebsite.gov.ua. Усі інші доменні розширення є ознакою фішингового ресурсу.

3. Якщо обраний Вами сайт не підтримує безпечне https-з'єднання, не вводьте свої персональні дані, реквізити кредитних карток, логіни та паролі електронної пошти або акаунтів у соціальних мережах.

4. Не ігноруйте попередження браузера про перехід на підозрілий сайт.

5. Якщо є потреба відвідати ресурс, краще ввести його адресу вручну, щоб запобігти переспрямуванню на шкідливий сайт.

6. На акаунтах, де є можливість, налаштуйте двофакторну аутентифікацію.