Базові правила кібербезпеки для користувачів

Базові превентивні міри кібербезпеки при роботі з електронною поштою

1. Не зберігайте дані для автентифікації (логін та пароль) в легкодоступних місцях (наприклад, на робочому столі).

2. ***Використовуйте стійкі паролі***, зокрема такі що: містять не менше 8 символів, містять щонайменш одну літеру та один спецсимвол (“_” або “-” або “!” тощо) не містять персоніфікованої інформації (дати народження, номерів телефонів, номерів та серій документів, автотранспорту, банківської картки, адреси реєстрації тощо), не використовуються в будь-яких інших аккаунтах.

   Рекомендація:
   Ознайомтесь з ефективною методикою легкого створення складних паролів
   https://bit.ly/2H4nnVO

1. ***Не відкривайте листи, які надійшли з невідомих та незвичайних*** електронних адрес наприклад santorin@abrgv.com тощо.

2. Не відкривайте ***листи в яких у темі присутні фрази типу “Ви виграли 500 тисяч…”***, “Відкрийте, та отримайте свій приз…” тощо.

3. Якщо в листі присутні вкладені ***файли з потенційно небезпечним розширенням*** (послідовність символів, що додаються до назви файлу і призначені для ідентифікації типу (формату) файлу), наприклад “Додаток 2.exe” або “Протокол 245 від 25 числа.bat” тощо НЕ відкривайте їх.

   До ***потенційно небезпечних розширень файлів*** у вкладеннях електронної пошти слід віднести: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js та будь-які інші невідомі розширення.

4. У разі, якщо є потреба відкрити той чи інший файл, але у вас є сумніви відносно його безпечності або безпечності його джерела, необхідно скористатися онлайн-сервісом перевірки файлів (файл перевіряється більш ніж 50 антивірусними програмами з актуальними антивірусними базами) - **VirusTotal**. Для цього достатньо перейти на сайт **virustotal.com** та слідувати інструкціям сервісу.

   Звертаємо вашу увагу на те, що, навіть якщо перевірка на VirusTotal не дала результату, це не виключає того, що файл може бути шкідливим.

Базові превентивні міри кібербезпеки при роботі в мережі інтернет (робота з інтернет-браузером)

1. Під час користування Інтернет-ресурсами ***не відкривайте підозрілі посилання (URL)***, особливо ті, що вказують на веб-сайти, які ви зазвичай не відвідуєте.

2. ***Звертайте особливу увагу на назву Інтернет-ресурсу***, що запитує автентифікаційні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати назву, щоб воно виглядало знайомим (замаскована назва: facelook.com, правильна назва: facebook.com; замаскована назва:gooogle.com, правильна назва: google.com тощо) . В іншому разі є велика ймовірність перейти на фішингову сторінку, ззовні ідентичну справжній, та самостійно «віддати» власні автентифікаційні дані.

3. Шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів та/або роздруковані на папері, у тому числі у формі скорочених URL, згенерованих спеціальними сервісами, такими як tinyurl.com, bit.ly, ow.ly тощо. ***Не вводьте ці посилання до браузера та не скануйте QR-коди вашим смартфоном якщо ви не впевнені у їх вмісті та походженні.***

4. ***Використовуйте VirusTotal для перевірки підозрілих посилань*** так само, як для сканування файлів.

5. ***Будьте обережні щодо випливаючих*** вікон та повідомлень у вашому браузері, програмах, операційній системі та мобільному пристрої. Завжди читайте вміст цих вікон та не "схвалюйте" і не "приймайте" нічого необдумано.

Резервне копіювання

1. Здійснюйте ***регулярне резервне копіювання важливих даних*** (не рідше ніж раз на тиждень), зберігайте резервні копії на зовнішніх носіях інформації (флеш та/або зовнішній жорсткий диск (або SSD).

2. Для більш надійного ефективного збереження важливих даних бажано проводити ***резервне копіювання в хмарне середовище***, наприклад у сервіс Google Drive.

   Відеоінструкція зі створення акаунту Gmail (необхідно, щоб розпочати роботу з google drive (займає не більше трьох хвилин) та базових функцій Google Drive
   https://youtu.be/JZCLESm1Ltg

Інструкція по роботі з Google Drive
https://bit.ly/2LECU3h

Інші застереження та рекомендації

1. Не підключайте флешки та зовнішні диски, не вставляйте CD та DVD тощо у ваш комп'ютер, якщо ви не довіряєте повністю їх джерелу.

2. Якщо є ймовірність, що флеш-носій скомпрометований (використовувався на інфікованому комп’ютері), не вставляйте його до ПК, та зверніться до співробітників відділу АСУ.

3. Не виключайте автоматичне оновлення операційної системи.

4. Не виключайте вбудований брандмауер Windows (за винятками, коли цю функцію бере на себе зовнішній антивірусний продукт).