АЛГОРИТМ
дій працівників при отриманні фішингових та інших підозрілих електронних листів

1. Первинна оцінка.

Ознаки підозрілого (фішингового) листа:

- **терміновість та тиск:** лист вимагає негайних дій («Терміново сплатити», «Ваш рахунок заблоковано», «Остання вимога суду»);
- **запит персональних даних або ресурсів:** лист містить вимоги надати списки працівників (ПІБ, адреси, номери телефонів), відомості про техніку, майно або ресурси установи. Офіційні запити від державних органів надходять через системи електронного документообігу (з використанням кваліфікованого електронного підпису) або з пошти, що закінчується на .gov.ua та завжди мають вихідний номер та дату;
- **невідомий або підроблений відправник:** адреса виглядає підозріло або не відповідає офіційній (наприклад, замість court.gov.ua - court-gov-ua.com). Державні установи не використовують публічні поштові сервіси (@meta.ua, @gmail.com, @ukr.net) для службового листування;
- **неочікуваний лист:** не чекали жодних документів або повідомлень;
- **підозрілі вкладення:** лист може містити архіви (.zip, .rar, .7z), файли з подвійними розширеннями (наприклад, Договір_2026.pdf.exe) або виконувані файли (.exe, .scr, .msi, .bat, .cmd, .vbs, .js, .ps1). Будьте обережні навіть зі стандартними форматами: PDF та DOCX - можуть містити посилання для завантаження;
- **документи Office** з вимогою «Увімкнути вміст» (макроси);
- **підозрілі посилання:** ведуть на невідомі сайти (можна перевірити, навівши курсор на посилання, не натискаючи);
- **помилки та дивний текст:** граматичні помилки, автоматичний переклад, незрозумілий зміст.

2. Дії при отриманні підозрілого листа.

Якщо лист викликає підозру, ЗАБОРОНЯЄТЬСЯ:

- відкривати вкладення;
- переходити за посиланнями;
- відповідати на лист та запити;
- пересилати його іншим працівникам;
- вводити будь-які паролі або службову інформацію.

У разі підозри НЕОБХІДНО:

- перевірити інформацію самостійно:
  - через офіційні сервіси (наприклад, Дія, електронний кабінет);
  - через офіційні сайти або відомі контакти;
- зв’язатися з відправником через офіційні канали (НЕ через контакти з листа);
- повідомити відповідальну особу з інформаційної безпеки та керівника;
- не видаляти лист до перевірки спеціалістами.

3. Інформування.

Негайно повідомте про підозрілий лист відповідальну особу з інформаційної безпеки та керівника. Не видаляйте підозрілий лист, це збереже технічні заголовки листа, необхідні для аналізу.

4. ЕКСТРЕНИЙ АЛГОРИТМ.

Якщо ви відкрили файл або перейшли за посиланням:

– негайно відключіть комп'ютер від мережі (витягніть кабель або вимкніть wi-fi);
– не вимикайте комп'ютер та не перезавантажуйте комп'ютер;
– негайно повідомте відповідальну особу з інформаційної безпеки та керівника;
– припиніть роботу за комп'ютером;
– не видаляйте лист і файли.

Головне правило: не панікувати і не намагатися приховати помилку. Чим швидше повідомите, тим меншої шкоди буде завдано установі. Якщо є сумнів —**НЕ відкривайте, НЕ натискайте, ПОВІДОМТЕ.**

Важливо пам'ятати:

1) жоден державний орган або банк не вимагає паролі електронною поштою та не використовують публічні поштові сервіси (@meta.ua, @gmail.com, @ukr.net) для службового листування;

2) навіть знайомий відправник може бути зламаний;

3) відкриття одного файлу може призвести до зараження всієї мережі установи.