Co-funded by the European Union

АКТИВУЮЧИЙ СЦЕНАРІЙ УРОКУ
розроблений в рамках проєкту

„ІННОВАЦІЇ В ШКІЛЬНІЙ ОСВІТІ"

Тема:

Phishing і фальшиві сторінки

1. Цілі уроку

Учень:

- розуміє, що таке phishing і фальшива інтернет-сторінка,
- може вказати найпоширеніші методи кіберзлочинців,
- знає, як фальшиві повідомлення і fake news використовуються для шахрайства,
- знайомиться з основними правилами безпеки в мережі,
- розвиває вміння аналізувати онлайн-контент і критичне мислення.

2. Цільова група

Учні початкових шкіл

3. Методи навчання

- Мозковий штурм
- Міні-лекція з прикладами
- Аналіз випадків (case study)
- Групова вправа – „Справжня чи фальшива сторінка?”
- Скерована дискусія
- Індивідуальна рефлексія

4. Навчальні матеріали / джерела

- Комп’ютер, проектор, інтерактивна дошка
- Скріншоти фіктивних phishing-листів та фальшивих сайтів
- Картка „10 попереджувальних сигналів phishing-у” (для роздачі учням)
- Список освітніх та фактчекінгових сторінок:
  - Польща: https://niebezpiecznik.pl, https://demagog.org.pl
  - Чехія: https://manipulatori.cz
  - Словаччина: https://hoax.sk

Проєкт спільно профінансований Європейським Союзом

- Україна: https://www.stopfake.org/en/news/
- ЄС: https://edmo.eu, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

5. Перебіг уроку (45 хв)

1. Вступ – чи завжди в інтернеті безпечно? (5–7 хв)

1. Мозковий штурм – досвід учнів (2–3 хв)

- Учитель просить учнів навести приклади ситуацій, коли:
  - отримали дивне повідомлення e-mail або SMS,
  - хтось надіслав їм підозріле посилання у соцмережах,
  - з'явилась сенсаційна інформація про виграш чи лотерею, яка спонукала натиснути на лінк.
- Відповіді учнів можна записати на дошці у дві колонки: „здавалося правдивим" / „викликало підозру", щоб показати, що не всі повідомлення відразу виглядають як шахрайство.

2. Навідні запитання (2–3 хв)

- Чи траплялося вам отримати повідомлення з обіцянкою виграшу, супер-акції або швидкого заробітку, але воно виглядало підозріло?
- Чи кожне повідомлення, яке ми отримуємо в інтернеті, є правдивим і безпечним?
- Які загрози можуть критися за натисканням на невідомий лінк?
- Чи може фальшиве повідомлення призвести до крадіжки грошей, пароля від онлайн-гри чи захоплення акаунта у соцмережах?
- Чому кіберзлочинці хочуть, щоб ми діяли швидко й без роздумів?

(Учитель заохочує учнів коротко ділитися історіями – без подання приватних даних чи імен осіб.)

3. Пояснення вчителя – розширена інформація (2 хв)

- **Phishing** – це інтернет-шахрайство, метою якого є виманювання конфіденційної інформації (паролі, логіни, номери платіжних карток, особисті дані).
- Шахраї використовують:
  - фальшиві e-mail чи SMS, видаючи себе за банк, кур'єрську компанію, торговельну платформу чи знайомого з контактів,
  - fake news або сенсаційні заголовки, що викликають емоції – страх, поспіх, надію на виграш,

    - фальшиві сайти, які виглядають майже так само, як справжні сторінки банків, магазинів чи соціальних мереж.
- Основна мета phishing-у – змусити жертву натиснути на лінк, завантажити файл, ввести дані входу чи підтвердити оплату, думаючи, що це безпечна сторінка.
- Натискання на фальшиве посилання може призвести до:
    - крадіжки грошей з банківського рахунку,
    - захоплення акаунтів у іграх, застосунках чи соцмережах,
    - поширення вірусів і шпигунського ПЗ на комп'ютері чи телефоні.

(Важливо підкреслити: жертви phishing-у не винні – винні шахраї. Кожен може стати жертвою маніпуляції, якщо не буде обережним.)

2. Міні-лекція: Phishing, фальшиві сторінки і дезінформація (10–12 хв)

1. Вступ – загрози в мережі (1 хв)

- Учитель питає учнів:
    - „Чи траплялося вам отримати повідомлення від невідомої особи з лінком або проханням ввести дані?"
    - „Як ми розпізнаємо, чи повідомлення безпечне?"
- Вводить тему, підкреслюючи, що phishing і фальшиві сторінки – це найпоширеніші інструменти кіберзлочинців, які використовують дезінформацію та емоції, щоб нас ошукати.

2. Визначення phishing-у (2 хв)

- **Phishing** – це інтернет-шахрайство, метою якого є виманювання особистих даних або грошей, найчастіше через:
    - e-mail, SMS, повідомлення в месенджерах,
    - фальшиві сайти, що видають себе за банки, магазини, соцмережі,
    - фальшиві сповіщення у браузері або застосунках („Ваш телефон заражено – натисніть, щоб виправити").
- Ціль кіберзлочинців:
    - отримання логінів і паролів,
    - крадіжка грошей із рахунків,
    - захоплення акаунтів у соцмережах,
    - розсилання нових шахрайських повідомлень друзям жертви.

3. Фальшиві інтернет-сторінки (2 хв)

- Це сайти, що видають себе за справжні:
    - мають схожу адресу (наприклад, „paypa1.com" замість „paypal.com"),
    - копіюють дизайн банку чи магазину,

  - просять ввести дані входу, номер картки, особисті дані.
- Кіберзлочинці часто розсилають посилання на такі сторінки у phishing-повідомленнях, використовуючи залякуючі або сенсаційні заголовки (напр. „Ваш акаунт буде видалено, якщо не підтвердите дані").

4. Техніки, які використовують шахраї (3 хв)

Учитель пояснює типові методи маніпуляції з прикладами:

1. **Шокуючі повідомлення:**
   - „Ваш акаунт буде негайно заблокований, якщо ви не натиснете на посилання!"
   - Використовують страх і поспіх, щоб жертва діяла імпульсивно.
2. **Обіцянки виграшу чи супер-пропозиції:**
   - „Ви виграли новий телефон!", „Отримай безкоштовний купон – тільки сьогодні!"
   - Викликають надію на виграш або прибуток.
3. **Видавання себе за установи:**
   - Повідомлення, схожі на ті, що від банку, кур'єрської служби, знайомого з контактів.
   - Часто мають підроблене лого, схожу e-mail адресу, але насправді це шахраї.
4. **Посилання на фальшиві сторінки:**
   - Імітують панель входу до банку, соцмереж чи інтернет-магазину.
   - Після введення даних злочинці отримують повний доступ до акаунта.
5. **Дезінформація і fake news:**
   - Фальшиві новини про катастрофи, небезпеку або „таємні акції", які заохочують перейти за підозрілим лінком.
   - Приклад: „Терміново! У вашому місті буде евакуація – подивись список місць!" (посилання веде на сайт для виманювання даних).

5. Зв'язок phishing-у з fake news (2 хв)

- Fake news можуть бути інструментом кіберзлочину, коли:
  - створюють фальшиве відчуття небезпеки чи сенсації, щоб змусити клікнути,
  - імітують повідомлення від надійних інституцій чи інформаційних порталів,
  - використовують поширення у соцмережах для масового розповсюдження шахрайства.
- Ефективний phishing часто поєднує елемент брехні (fake news) і фальшиві сторінки, створюючи враження автентичності та тиску часу.

6. Наслідки для жертв (1–2 хв)

- **Фінансові:** крадіжка грошей із банківських рахунків, несанкціоновані платежі.
- **Приватності:** захоплення особистих даних, які можуть бути використані в інших шахрайствах.
- **Соціальні:** захоплення акаунтів у соцмережах, розсилання шахрайських повідомлень друзям.
- **Психологічні:** стрес, почуття сорому або провини, зниження довіри до справжніх установ.

7. Підсумок міні-лекції (1 хв)

- Phishing – це поєднання шахрайства, маніпуляцій емоціями та дезінформації.
- Жертвою може стати кожен – навіть обережні люди.
- Основні правила захисту:
    1. Не натискати на підозрілі лінки і не відкривати вкладення від невідомих відправників.
    2. Перевіряти адреси сайтів і e-mail (помилки у словах, дивні домени).
    3. Ніколи не надавати конфіденційні дані, якщо є хоча б тінь сумніву щодо джерела повідомлення.

(Учитель демонструє на слайді приклад фіктивного phishing-листа, щоб учні могли вказати, що в ньому підозріле.)

3. Групова вправа – „Справжня чи фальшива сторінка?" (15–20 хв)

Ціль вправи

- Розвиток умінь розпізнавати спроби phishing-у.
- Навчання учнів аналізу підозрілих повідомлень і сайтів.
- Усвідомлення того, як кіберзлочинці маніпулюють емоціями (страх, поспіх, виграш), щоб змусити ввести дані чи натиснути на лінк.
- Створення власних правил безпеки в інтернеті.

1. Поділ на групи (1 хв)

- Клас ділиться на команди по 3–4 особи.
- Кожна група отримує 3 приклади (надруковані або показані на екрані):
    1. Справжня сторінка банку або магазину (наприклад, офіційна панель входу).
    2. Фальшива phishing-сторінка, дуже схожа на справжню.
    3. Phishing-повідомлення (SMS/e-mail від „кур'єрської компанії" чи „банку") із проханням натиснути на лінк або ввести дані.

Co-funded by the European Union

1. Справжня сторінка банку/магазину

(Офіційна панель входу – приклад)

Заголовок: „Bank Polska Online – Увійти”
Адреса сторінки (URL): https://secure.bankpolska.pl

Вигляд:

- Лого банку у верхньому лівому куті.
- Праворуч – опція зміни мови (PL / EN).
- Поля входу: „Ідентифікатор” + „Пароль”.
- Іконка замка у браузері (зелена або сіра).
- Нижній колонтитул із юридичною інформацією та лінками: „Правила”, „Політика конфіденційності”.

Елементи автентичності:

- Адреса у домені банку.
- SSL-сертифікат (https:// + замок).
- Відсутність помилок, правильна мова.

2. Фальшива phishing-сторінка

(Дуже схожа на справжню)

Заголовок: „Bank Polska – Вхід”
Адреса сторінки (URL): https://bankpolska-login.secure-info.net

Вигляд:

- Схоже лого банку (трохи розмите, гірша якість).
- Сторінка майже ідентична, але немає опції зміни мови.
- Поля входу такі ж, але кнопка „Увійти” іншого кольору.
- Відсутній SSL-сертифікат або замок перекреслений/червоний.
- У нижньому колонтитулі немає лінків на правила чи політику конфіденційності.

Ознаки фальшивості:

- Домен відрізняється від офіційного (додаткові слова, незвичне закінчення).
- Часто прихована помилка у назві домену (наприклад, „banlkpolska.pl”).
- Іноді спливає вікно з проханням „оновити дані”.

3. Phishing-повідомлення

(SMS або e-mail від „кур’єрської компанії” чи „банку”)

Приклад SMS:
„Ваша посилка чекає на отримання. Доплатіть 1,99 zł, щоб її отримати: https://inpost-paczka-secure.net”

Приклад e-mail від „банку”:
Тема: „Терміново! Ваш акаунт заблоковано”
Текст:
„Шановний Клієнте,
ми виявили незвичну активність на вашому акаунті. Щоб розблокувати доступ, натисніть посилання нижче і увійдіть:
Увійти зараз
Якщо ви не підтвердите дані протягом 24 годин, акаунт буде остаточно заблокований.”

Ознаки підозрілості:

- Тиск часу („протягом 24 годин”).
- Лінк веде на інший домен.
- Мовні помилки або дивні формулювання.
- Неочікувані прохання ввести дані.

2. Допоміжний інструмент – „Картка 10 попереджувальних сигналів phishing-у” (2 хв)

Кожна група отримує картку з переліком найчастіших сигналів:

№	Попереджувальний сигнал
1	Помилки у словах, дивна адреса сторінки (наприклад, „paypa1.com” замість „paypal.com”).
2	Відсутність „https://” і замка в адресному рядку.
3	Адреса e-mail відправника виглядає підозріло (наприклад, випадкові символи).

Co-funded by the European Union

№	Попереджувальний сигнал
4	Повідомлення містить мовні помилки, незвичний шрифт або дивне форматування.
5	Погрози або тиск часу („Якщо не натиснеш, акаунт буде заблоковано!”).
6	Обіцянка виграшу, подарунку чи супер-акції без причини.
7	Лінки ведуть на невідомі домени або сайти без контактів.
8	Прохання ввести паролі, номер картки або особисті дані.
9	Вкладення у невідомому форматі, особливо .exe, .zip.
10	Незвичне лого чи графіка, інший вигляд сайту, ніж зазвичай.

3. Завдання для груп (8–10 хв)

Кожна група аналізує три приклади та:

1. Визначає, які повідомлення/сторінки справжні, а які phishing.
2. Позначає на роздруківці або у таблиці попереджувальні сигнали (за номерами з картки).
3. Вказує емоції, які намагається викликати шахрай (страх, поспіх, виграш, відчуття обов’язку).
4. Формулює правило захисту, яке допомогло б уникнути цього шахрайства (наприклад, „завжди перевіряю адресу сайту”, „не переходжу за лінками з SMS”).

Таблиця для заповнення:

Приклад повідомлення/сторінки	Справжня чи фальшива?	Попереджувальні сигнали (№ з картки)	Як захиститися?

Проєкт спільно профінансований Європейським Союзом

Co-funded by the European Union

Приклад повідомлення/сторінки	Справжня чи фальшива?	Попереджувальні сигнали (№ з картки)	Як захиститися?

4. Презентація результатів (4–5 хв)

- Кожна група презентує один приклад, який здалася їй найцікавішим або найскладнішим для розпізнавання.
- Учитель записує на дошці найчастіше згадувані попереджувальні сигнали, створюючи спільний „список правил онлайн-безпеки”.

5. Підсумок вправи (1–2 хв)

- Phishing часто виглядає професійно і достовірно, тому легко потрапити в пастку.
- Основні правила захисту:
    1. Ніколи не вводжу паролі чи номери карток після натискання на лінки з повідомлень.
    2. Перевіряю адресу сайту і відправника повідомлення.
    3. Не дію під тиском часу – завжди можна перевірити справу іншим способом (наприклад, зателефонувавши до банку).
    4. Якщо щось виглядає підозріло – краще не натискати.

4. Дискусія: Як захищатися від phishing-у та шахрайств у мережі? (8–10 хв)

1. Ціль дискусії

Проєкт спільно профінансований Європейським Союзом

- Усвідомити, чому навіть обережні люди можуть стати жертвами phishing-у.
- Зрозуміти, як емоції, поспіх і відсутність перевірки інформації допомагають кіберзлочинцям.
- Виробити практичні правила безпечного користування лінками, повідомленнями і сайтами.

2. Базові запитання до учнів

- Чому багато людей натискають на фальшиві повідомлення, навіть якщо вони виглядають підозрілими?
- Які емоції найчастіше використовують кіберзлочинці (страх, цікавість, поспіх, бажання виграти)?
- Чи всі лінки від „друзів" безпечні? Чому навіть акаунти друзів іноді можуть надсилати фальшивий контент?
- Як можна перевірити, чи сайт справжній (наприклад, https, сертифікат, відсутність помилок у назві, офіційний домен)?
- Чи можуть fake news бути першим кроком до шахрайства (наприклад, фальшиві новини про катастрофи, лотереї, акції)? Як працює цей механізм?

3. Поглиблюючі запитання для дискусії

- Чи завжди безпечно натискати на лінк, якщо повідомлення надійшло від знайомого? (наприклад, зламаний акаунт надсилає заражені повідомлення).
- Чому кіберзлочинці часто додають „термінові попередження" або „акції з обмеженим часом", щоб ми натискали швидко й без роздумів?
- Чи кожен виграш в інтернеті справжній? Які „червоні прапорці" вказують на шахрайство?
- Як відрізнити справжнє повідомлення від банку чи кур'єрської компанії від фальшивого?
- Що робити, якщо випадково натиснули на лінк чи передали дані шахраям? Хто може допомогти у такій ситуації?

4. Міні-аналіз – короткі приклади для обговорення

Учитель може показати 2–3 фіктивні повідомлення (роздруківки або слайди):

1. „Терміново! Ваш акаунт буде заблоковано протягом 24 годин, натисніть тут і підтвердьте свої дані!"

2. „Гей, подивись це відео – це ти? 😂 [лінк]” (повідомлення від акаунта знайомого)
3. „Ви виграли смартфон! Отримайте приз, натиснувши на посилання нижче.”

Запитання:

- Які емоції викликає це повідомлення?
- Що в ньому виглядає підозріло?
- Як правильно відреагувати у такій ситуації?

5. Висновки дискусії – „Золоті правила безпеки”

На основі відповідей учнів і аналізу прикладів учитель створює список правил (на дошці або фліпчарті), наприклад:

1. Завжди перевіряю відправника – навіть якщо повідомлення від знайомого.
2. Не натискаю на лінки з невідомих джерел та не відкриваю підозрілі вкладення.
3. Перевіряю адресу сайту – справжні сервіси мають правильний домен і замок „https://”.
4. Не довіряю „несподіваним акціям” чи „виграшам без причини” – нічого не приходить безкоштовно.
5. Не дію у поспіху – шахраї хочуть, щоб ми натискали без роздумів.
6. У разі сумнівів питаю дорослого, банк, спеціаліста або перевіряю повідомлення на офіційному сайті.

6. Підсумок учителя (1–2 хв)

- Кіберзлочинці використовують емоції та довіру, щоб нас ошукати – phishing працює не тому, що хтось „неуважний”, а тому, що він добре спланований.
- Жертвою може стати кожен, але завдяки обережності, перевірці інформації та униканню випадкових кліків ми можемо себе захистити.
- Fake news часто є першим кроком до шахрайства, бо створюють сенсацію, що заохочує натиснути й веде на фальшиві phishing-сторінки.

5. Підсумок і рефлексія (7–10 хв)

1. Індивідуальна рефлексія – закінчи речення (3–4 хв)

Кожен учень отримує аркуш або користується зошитом і завершує речення:

- „Я зрозумів/зрозуміла, що phishing…”
- „Найбільш підозрілим у фальшивих повідомленнях є…”
- „Перш ніж натиснути на лінк, я перевірю…”
- „Щоб захистити свій акаунт, я буду…”
- (опціонально) „Якщо випадково натисну на підозрілий лінк, я повинен…”

Учитель підкреслює, що немає неправильних відповідей – вправа допомагає перевести знання у практичні звички.

2. Короткий обмін досвідом (2–3 хв)

- Учні, які хочуть, читають свої відповіді (або вчитель збирає анонімні картки та зачитує вибрані приклади).
- Дискусія за допомогою запитань:
  - Чи повторювалися ваші відповіді?
  - Яке правило захисту від phishing-у згадувалося найчастіше?
  - Чи з’явилися нові ідеї, які варто запам’ятати?

3. Спільний список – „5 (або більше) правил безпечного користування лінками і сайтами” (3 хв)

На дошці або фліпчарті створюється спільний список правил безпеки. Приклади:

1. Ніколи не вводжу паролі чи номери карток у підозрілих лінках або після переходу з e-mail/SMS.
2. Перевіряю точну адресу сайту (відсутність помилок у словах, правильний домен, „https://” і значок замка).
3. Не натискаю на несподівані пропозиції виграшу, лотереї, „термінові попередження” – спочатку перевіряю їх в офіційних джерелах (наприклад, входжу в банк вручну, телефоную у кур’єрську компанію).
4. Не дію поспіхом – шахраї хочуть, щоб ми клікали імпульсивно.
5. Консультую підозрілі повідомлення з батьками, учителем або спеціалістом.
6. (опціонально) Використовую антивірус, оновлюю систему та паролі – це додатковий захист від атак.

(Список можна сфотографувати або переписати в зошити як „Правила безпечного користування лінками і сайтами”).

4. Підсумок учителя – фінальне повідомлення (1–2 хв)

- Phishing – це шахрайство, що базується на емоціях і довірі – навіть дорослі, які добре знаються на технологіях, іноді стають жертвами.
- Найважливіше правило: якщо щось виглядає підозріло чи надто добре, щоб бути правдою – не клікай, не передавай дані, перевір джерело.
- Безпека в мережі залежить від уважності кожного з нас – краще запитати, перевірити чи зачекати, ніж втратити дані або гроші.

(Урок можна завершити коротким усним квізом або запитанням: „Яке одне правило ви запам'ятаєте на майбутнє?" – учні відповідають одним словом чи фразою.)

6. Словник понять

Поняття	Визначення
Phishing	Спроба виманювання даних (логіни, паролі, банківські дані) через фальшиві повідомлення, видавання себе за надійні установи.
Фальшива сторінка	Вебсайт, що імітує офіційний сайт банку, магазину, сервісу з метою крадіжки даних або грошей.
Дезінформація у phishing-у	Використання фальшивих повідомлень або fake news для того, щоб змусити жертву натиснути на лінк чи завантажити файл.
Кіберзлочинець	Особа або група, що використовує методи шахрайства в інтернеті для отримання даних чи грошей.
Безпечні лінки	Сайти й адреси, що починаються з „https", мають правильний домен і походять із перевірених джерел.

7. Методичний посібник для вчителя

1. Підготовка матеріалів

- **Приклади:**
  - Використовуй лише фіктивні повідомлення і phishing-сторінки, створені спеціально для занять, щоб уникнути ризику натиснути на справжні лінки чи розкрити дані.

  - Можна брати за основу реальні атаки phishing, але змінюй назви, логотипи, адреси URL так, щоб вони були нейтральні й освітні.
  - Не показуй реальних даних користувачів, навіть як приклад – зберігай повну анонімність.
- **Різноманітність матеріалів:**
  - Підготуй скріншоти сторінок входу, e-mail сповіщень, SMS, реклами у соцмережах.
  - Можна додати елемент інсценізації – розіграти ситуацію, коли хтось отримує підозріле повідомлення, а інші шукають правильну реакцію.
  - Покажи різні форми phishing-у: класичний e-mail, фальшиві акції, лінки від „друзів", пости у соцмережах, фальшиві застосунки.

2. Проведення занять

- **Відправна точка:**
  - Почни урок із відкритого запитання, наприклад: „Чи хтось із вас коли-небудь отримував повідомлення, яке виглядало підозріло? Що в ньому вас насторожило?"
  - Переконайся, що розмова не призводить до висміювання – phishing може торкнутися кожного.
- **Міні-лекція:**
  - Подай короткі блоки інформації (макс. 2–3 хв) з перервами на запитання учням, щоб утримувати їхню увагу.
  - Використовуй прості приклади й зрозумілу мову – уникай надлишкової технічної термінології.
- **Практичні вправи:**
  - Аналіз фальшивих сторінок і повідомлень має бути безпечним (без активних лінків).
  - Учні повинні мати можливість позначати сигнали небезпеки (наприклад, маркером на роздруківках або на інтерактивній дошці).
  - Дай час на обмін висновками, щоб учні могли порівняти свої спостереження.

3. Модерування дискусії

- Заохочуй учнів наводити приклади з власного життя або історії, почуті від родини й знайомих.
- Підкреслюй, що ніхто не захищений на 100% від шахрайства – жертвами phishing-у стають навіть IT-фахівці з безпеки.
- Правило: „Не висміюємо, а аналізуємо" – реагуй, якщо у класі з'являються насмішки над ситуаціями інших.

- Можна застосувати техніку „Запитання до класу”: замість оцінювання відповіді, питати „Чи хтось думає інакше?”, „Чи є інший спосіб вирішення?”.

4. Забезпечення безпечної атмосфери

- Підкреслюй, що phishing – це злочин, а не вина людини, яка потрапила у пастку.
- Якщо хтось поділиться досвідом бути жертвою шахрайства, вислови підтримку та визнання за сміливість розповісти історію.
- Поясни учням, що найкращий захист – це знання, а не сором: чим більше ми знаємо про шахрайства, тим краще можемо себе захистити.

5. Виховна мета уроку

- Формування:
  - усвідомлення цифрових загроз, пов’язаних із phishing-ом і фальшивими сторінками,
  - звички перевіряти лінки й відправників повідомлень перед тим, як натискати чи вводити дані,
  - стійкості до маніпуляцій емоціями (страх, поспіх, раптові нагороди),
  - позиції відповідального користувача інтернету, який дбає не лише про власну безпеку, але й попереджає інших про шахрайства.

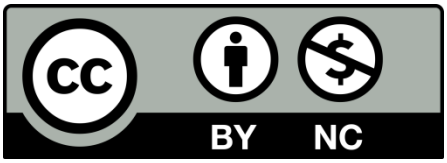
6. Додаткові пропозиції для розширення уроку

- **Домашнє завдання:** учні збирають 3 приклади фальшивих повідомлень (з інтернету або вигадують власні фіктивні) і на наступному уроці аналізують їх у групах.
- **Міні-проєкт класу:** створення плаката „10 попереджувальних сигналів phishing-у” або „Як перевірити, чи сайт безпечний?”, який можна розмістити у школі.
- **Симуляція phishing-атаки (безпечна):** учитель готує коротке „фальшиве повідомлення”, а учні мають вказати всі сигнали, що це шахрайство.

8. Освітні та фактчекінгові джерела

Co-funded by the European Union

- **EDMO – European Digital Media Observatory**
  https://edmo.eu
- **Europol – Cybercrime**
  https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
- **EUvsDisinfo**
  https://euvsdisinfo.eu
- **Niebezpiecznik.pl (PL)**
  https://niebezpiecznik.pl
- **Demagog.org.pl (PL)**
  https://demagog.org.pl
- **Manipulátoři.cz (CZ)**
  https://manipulatori.cz
- **Hoax.sk (SK)**
  https://hoax.sk
- **StopFake.org (UA)**
  https://www.stopfake.org/en/news/



Проєкт спільно профінансований Європейським Союзом