**Полтавська академія неперервної освіти**

**ім. М.В. Остроградського**

**Випускна робота**

**Тема «Розробка уроку з інформатики»**

**Виконала: Масенко Світлана Анатоліївна, Лубенський район, ОЗ "Хорольський ЗЗСО І-ІІІ ст. №1", учитель математики та інформатики**

**ПОЛТАВА – 2025**

**Клас:** 6  
**Тема:** *Безпечна поведінка в Інтернеті. Як розпізнати фішинг та інтернет-шахрайство*  
**Тип уроку:** Вивчення нового матеріалу (з елементами практики та рефлексії)

**📌 Очікувані результати навчання:**

**Після уроку учень/учениця:**

* пояснює, що таке фішинг та які є види інтернет-шахрайства;
* розпізнає ознаки небезпечних повідомлень/листів;
* аргументовано пояснює, як діяти в ситуаціях кіберзагроз;
* застосовує правила безпечної поведінки онлайн;
* працює в групі, бере участь в обговоренні, оцінює власну участь у роботі.

**🔧 Необхідне обладнання:**

* Презентація
* Картки з прикладами листів (справжні/фейкові)
* Онлайн-дошка (Padlet, Jamboard)
* Інтернет (за можливості)
* Маркери, стікери

**Структура уроку**

**1. Організаційний момент (1–2 хв)**

* Привітання
* Налаштування на тему
* Коротка проблемна ситуація: “Чому люди продовжують втрапляти в пастки шахраїв в Інтернеті, навіть знаючи про них?”

**2. Актуалізація знань (5 хв)**

**Інтерактивна вправа “Правда чи міф” (так/ні):**

* Усі сайти в Інтернеті безпечні.
* Пароль можна повідомляти лише друзям.
* Якщо лист виглядає офіційно — йому можна довіряти.
* Шахраї можуть прикидатися знайомими в месенджері.

🔁 **Формувальне оцінювання:** обговорення відповідей, короткий зворотний зв’язок.

**3. Опрацювання нового матеріалу (10 хв)**

**Міні-лекція з демонстрацією:**

* Що таке фішинг?
* Як працюють інтернет-шахраї (приклади месенджерів, сайтів, листів).
* Які “ознаки небезпеки” варто запам’ятати.

**Метод “Знайди ризик”** — учитель демонструє лист/повідомлення на екрані, учні називають ризиковані елементи. Мета: навчити учнів уважно аналізувати контент (листи, повідомлення, сайти, акаунти) та виявляти потенційні загрози або ознаки шахрайства.

**1) фронтальна робота (на екрані):**

* Учитель демонструє один приклад на дошці/екрані.
* Учні по черзі/за бажанням виходять і позначають маркером (або називають), **де саме бачать ознаку небезпеки**.

**2) робота в парах/групах:**

* Кожна група отримує власний приклад.
* Завдання — знайти **усі можливі “червоні прапорці”** (ознаки ризику), виписати або виділити їх.

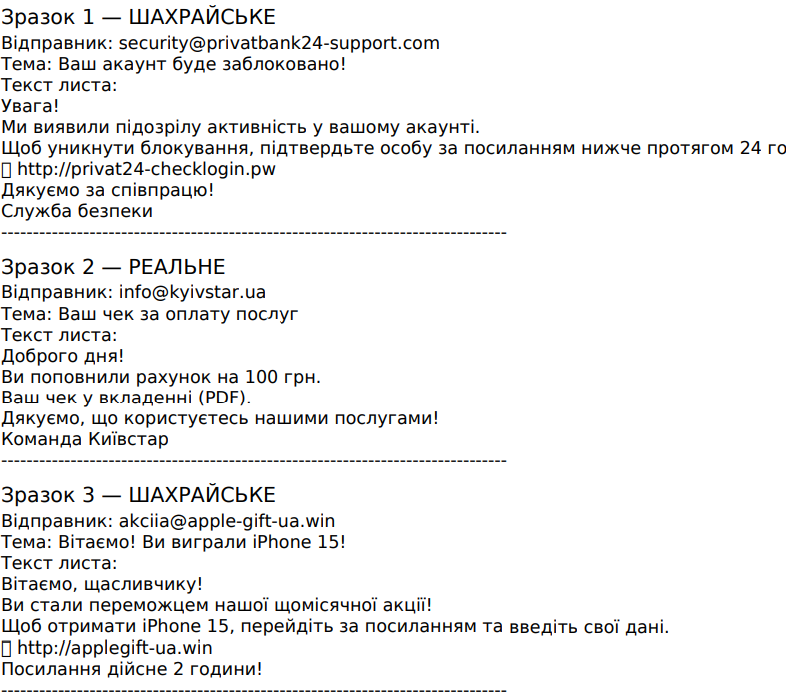
| **Ознака** | **Приклад** |
| --- | --- |
| Підозріла адреса відправника | info@notbank.com.ua |
| Орфографічні чи граматичні помилки | “Ваш акаунт заблокований!” |
| Заклики до термінових дій | “Натисни зараз, інакше втратиш доступ” |
| Вкладення або посилання без пояснення | “Дивись прикріплений файл” |
| Збіг зовнішнього вигляду сайту з відомими брендами, але інша URL-адреса | http://bank.ukrainiia.net |
| Вимога надати особисті дані | “Введіть номер карти” |

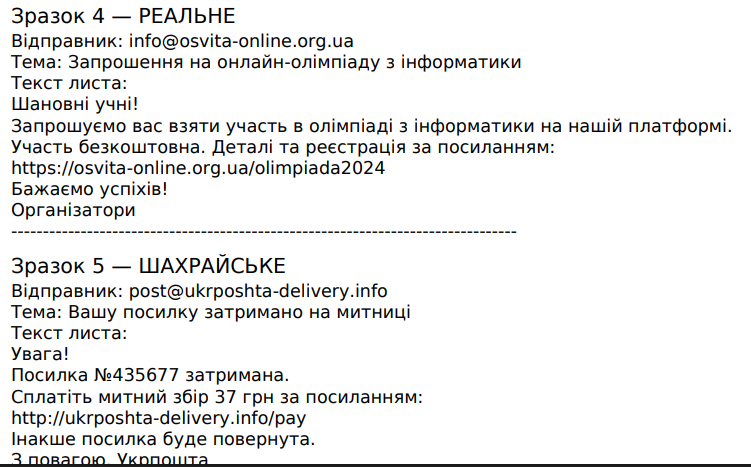
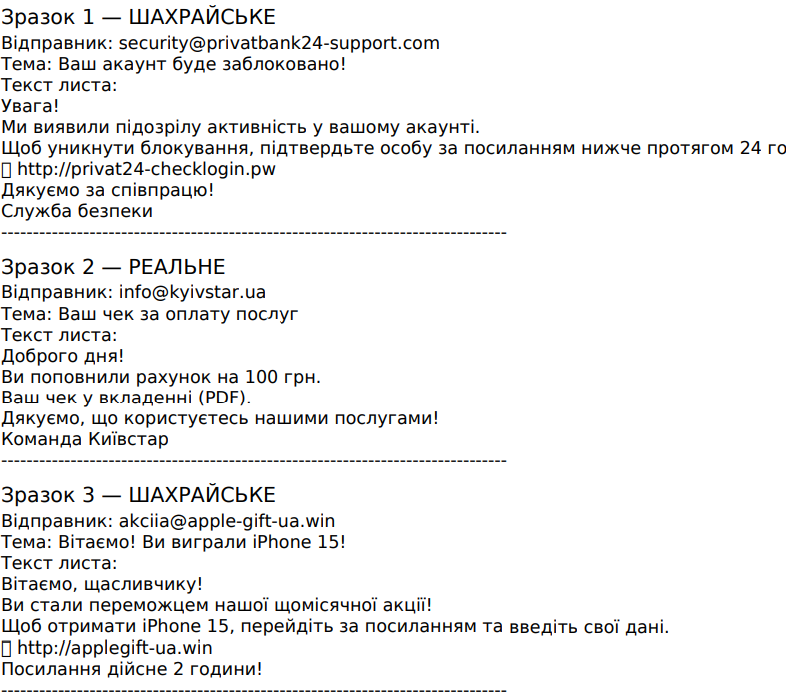
**4. Інтерактивна діяльність (15 хв)**

**Групова гра “Реальне чи шахрайське?”**

* Групи отримують по 2–3 картки з імітацією листів або повідомлень.
* Завдання — визначити, які з них фішингові, аргументувати чому.
* Відмічають у таблиці:

| **№** | **Повідомлення** | **Це фішинг?** | **Чому?** |
| --- | --- | --- | --- |

ЗРАЗКИ: 



✅ **Формувальне оцінювання**: презентація результатів, взаємне оцінювання: “Я згоден, бо…”, “А я думаю інакше, тому що…”

**5. Рефлексія та узагальнення (5–7 хв)**

**Вправа “Мікрофон” або “3 речення”**  
Учні завершують фрази:

* Я дізнався/дізналася, що…
* Тепер я точно не буду…
* Найбільше мене здивувало…

🔁 **Формувальне оцінювання:**  
**Сходинки розуміння:**  
Учні ставлять “галочку”:

* 🔲 Я зрозумів(ла) тему уроку
* 🔲 Мені було цікаво
* 🔲 Я зможу пояснити це іншим

**6. Домашнє завдання (на вибір):**

🖍 **Креативне завдання:** Створити пам’ятку або постер "Як не стати жертвою фішингу".  
📷 **Медіа завдання:** Знайти приклад фішингового листа (зображення, скрін, стаття) і пояснити його ознаки (усно/письмово).