

# 1

## Інформація, яку безпечно повідомляти стороннім особам

Шахраї виманюють у людей конфіденційну інформацію, щоб привластити чужі кошти. Потрібно тримати язик за зубами, думати двічі перед тим, як ділитися з кимось інформацією про себе.

Визначте, яку інформацію повідомляти стороннім особам безпечно, а яку – ні. Там, де можна повідомляти інформацію, поставте (+), де не можна – (-).

тризначний номер  
на звороті картки

логін до інтернет-  
банкінгу

смс-коди  
від банків

адресу  
електронної пошти

пароль  
до інтернет-  
банкінгу

16-значний номер  
картки

пін-код  
до картки

пароль  
до сторінки  
в TikTok

смс-коди  
від мобільних  
операторів

назву банку,  
зазначену  
на картці

## 2

# Спілкування в соціальних мережах

**2.1.** Шахраї вміють маскуватися твоїми друзями в соціальних мережах та просити в борг від їхнього імені.



Бувають ситуації, що друзі дійсно потрапляють у скрутне становище та просять про допомогу. Як зрозуміти, хто пише, друг чи шахрай? **Опишіть** ваші дії.

---

---

---

---

---

## 2.2. Спочатку думай – потім клікай

Шахраї під маскою твоїх друзів можуть прислати і такі повідомлення в соціальних мережах.



Опишіть ваші дії. Чому не можна клікати за цим посиланням?

---

---

---

---

---

---

---

---





**3.2.** Які з описаних ситуацій схожі на шахрайство, а які на правильну поведінку?

В тих ситуаціях, які схожі на шахрайство, напишіть одну пораду, як вберегтися від шахрайства.

Продавець на майданчику оголошень (наприклад, OLX) пропонує обговорити деталі покупки в месенджері

Схоже на шахрайство

Все ок

---

---

---

---

Покупець просить надати 16-значний номер платіжної картки, щоб переказати гроші за покупку

Схоже на шахрайство

Все ок

---

---

---

---

Працівник мобільного оператора телефону  
та просить назвати СМС-код

Схоже на шахрайство

Все ок

---

---

---

---

Покупець на майданчику оголошень (наприклад, OLX) надсилає  
продавцю посилання в менеджер та просить ввести всі карткові  
реквізити для отримання оплати продавцем

Схоже на шахрайство

Все ок

---

---

---

---

Пропонують взяти участь у голосуванні в конкурсі, для цього  
просять ввести логін та пароль до сторінки в Facebook

Схоже на шахрайство

Все ок

---

---

---

---

Телефонує працівник банку та просить встановити програму віддаленого доступу для посилення заходів безпеки

Схоже на шахрайство

Все ок

---

---

---

---

**3.3.** Однією з найрозповсюдженіших схем шахрайства є продаж неіснуючих товарів. На жаль, у сфері онлайн-покупок можуть зустрітися шахраї.

Перерахуйте правила безпечних онлайн-покупок.

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_



# 4

## Ситуація: шахраї викрали фінансовий номер телефону

До яких ресурсів шахраї можуть отримати доступ, присвоївши фінансовий номер телефону?

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Перегляньте перелік, який ви зазначили. Доступ до якого ресурсу дасть шахраю більше шансів викрасти гроші з рахунків, **оцініть балами від 1 до 5**, де 5 балів – це найвищий ризик, що шахрай зможе викрасти кошти, отримавши доступ до цього ресурсу.

Обговоріть свої оцінки в класі/групі, а саме ті випадки, де ви поставили найвищий бал. Чи погоджуються вони з вашою оцінкою.





# 5

## Що робити, коли стикнувся з шахрайством?

**5.1.** Розгляньте описані нижче ситуації та зазначте, куди потрібно звертатися насамперед, щоб захистити свої кошти.

1. Перестав працювати фінансовий номер телефону

---

2. Викрали смартфон

---

3. Випадково повідомили телефоном шахраю секретні реквізити картки

---

4. Зняли готівку з банкомата, де було встановлене скімінгове обладнання

---

5. На фішинговому сайті вказали логін та пароль до інтернет-банкінгу

---

6. Помітили, що з вашого рахунку зникають кошти

---

**5.2.** Тепер ви знаєте, скільки пасток розставляють шахраї.

Подумайте, як ви можете захистись від аферистів. Яких заходів безпеки потрібно вжити для кожного інструменту.

**Сторінка в соціальних мережах**

---

---

---

**Фінансовий номер телефону**

---

---

---

**Смартфон**

---

---

---

**Ігровий акаунт**

---

---

---

**Яких ще правил потрібно дотримуватися, щоб не потрапити до рук шахраїв?**

*(Напишіть 5 порад)*

---

---

---

---

---

# 6

## Тести

**Перевіримо, як ви засвоїли тему заняття.**  
Яка з відповідей правильна?

1. Що таке фінансовий номер телефону?

- Так називають банківський рахунок
- Номер, з якого телефонує банк
- Номер, який прив'язаний до банківського рахунку
- Видуманий термін

2. Які реквізити картки можна розголошувати стороннім особам?

- 16-значний номер та термін дії картки
- Пін-код та термін дії картки
- 16-значний номер картки
- Жодних реквізитів повідомляти не можна

3. На якому онлайн-сервісі можна перевірити потенційного шахрая за номером телефону та посиланням на сайт?

- STOP FRAUD, CheckMyLink
- "Дія"
- Кабінет електронних сервісів
- Шахрай онлайн

4. Як часто рекомендується змінювати пін-код до платіжної картки?

- 1 раз на 3 місяці
- пін-код до картки змінити неможливо
- Щороку
- Немає сенсу змінювати пін-код

5. Банкомат "зажував" платіжну картку, які ваші дії?

- *Напишу заяву в поліцію*
- *Спробую дістати картку з банкомата*
- *Не відходячи від банкомата, зателефоную до кол-центра банку*
- *Одразу піду до відділення банку писати заяву*

6. Під час введення пін-коду в банкоматі виникла підозра, що хтось у черзі позаду дізнався ваш пін-код. Які ваші дії?

- *Зміню пін-код до картки*
- *Повідомлю в поліцію*
- *Проігнорую, пін-код – це не таємниця*
- *Звернуся до відділення, щоб перевипустити картку*

