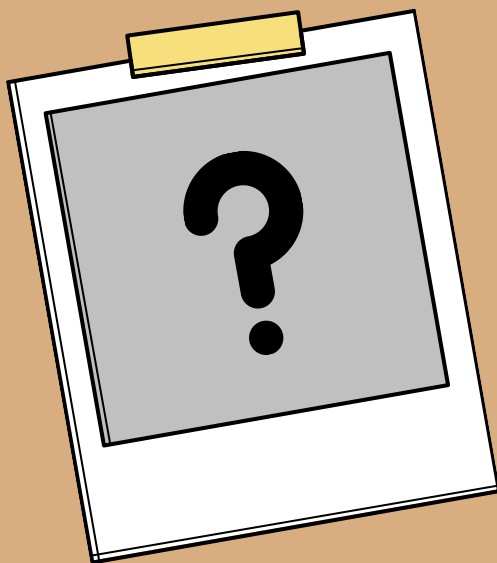




Відповіді на завдання за кейс-картками для педагога





Кейс-картка №1 "Тарифна пастка"

Короткий опис справи: жителю Чернігівщини запропонували змінити тарифний план. Чоловік повірив і повідомив код із SMS, який надійшов на його номер телефону. У результаті з його банківської картки зняли 64 000 грн.

1. Дії шахрая.

- Дзвонить невідомим абонентам і пропонує змінити тарифний план для поліпшення мобільного зв'язку.
- Просить надати код із SMS для підтвердження.
- Вимагає конфіденційну інформацію для отримання доступу до рахунку.

2. Потерпілий.

- Чоловік середнього віку, який користується мобільним зв'язком.
- Мешканець Чернігівщини.
- Втратив 64 000 грн.
- Довіряє незнайомцям по телефону.

3. Емоції / психологічні тригери.

- **Ілюзія офіційності.** Шахрай видає себе за представника мобільного оператора, використовуючи авторитет відомої компанії. Це знижує недовіру і підсилює впевненість у правдивості його слів.
- **Грає на страху залишитися без зв'язку.** Шахрай апелює до базової потреби людини — бути на зв'язку з близькими, особливо в часи, коли перебої зв'язку сприймаються як серйозна загроза.
- **Відчуття турботи.** Незнайомець ніби дбає про потерпілого, пропонуючи вигідні умови. Це створює ілюзію, що оператор піклується про клієнта.
- **Створення відчуття контролю та вигоди.** Потерпілому здається, що він отримає додаткову перевагу — завжди буде зв'язок. Це спричиняє позитивне очікування і підштовхує до дії.

4. Гачок / як шахрай заманює жертву.

- Надає пропозицію змінити тарифний план, щоб залишатися завжди на зв'язку, навіть у разі перебоїв у мережі.
- Подає інформацію як офіційне повідомлення від мобільного оператора.
- Просить код із SMS як підтвердження.

5. Запобігання / як уникнути шахрайства.

- Нікому не повідомляти SMS-коди від банків та мобільних операторів.
- Слід завжди перевіряти інформацію через офіційний контактний центр мобільного оператора.
- Не потрібно передавати конфіденційну інформацію через телефон.
- Слід прив'язати фінансовий номер телефону до своїх паспортних даних або укласти контракт із мобільним оператором.





Кейс-картка № 2 "Ваш родич у біді"

Короткий опис справи: пенсіонеру зателефонував шахрай, видавши себе за сина після ДТП. Унаслідок стресу чоловік передав незнайомці постіль та заощадження — 500 доларів і 200 євро. Згодом з'ясувалося, що з сином усе гаразд.

1. Дії шахрая.

- Зателефонував і представився сином потерпілого.
- Повідомив неправдиву інформацію про ДТП.
- Попросив посередника (незнайомку) забрати гроші та речі.

2. Жертва шахрая.

- Чоловік старшого віку, 70 років.
- Мешканець Чернігівщини.
- Втратив заощадження — 500 доларів і 200 євро, а також особисті речі (постіль).
- Легко піддається емоційному впливу та довіряє незнайомцям.

3. Емоції / психологічні тригери.

- **Страх за близьку людину.** Шахрай повідомляє про ДТП, спричиняючи сильне хвилювання за життя і здоров'я сина. Це паралізує критичне мислення.
- **Почуття терміновості.** Шахрай змушує реагувати негайно (потрібні гроші на лікування зараз), позбавляючи потерпілого часу на роздуми чи консультацію з іншими.
- **Ілюзія довіри.** Використання образу сина автоматично знижує рівень підозри та викликає бажання допомогти.
- **Емоційний шантаж через провину.** Потерпілий відчуває, що від його дій залежить здоров'я і навіть життя близької людини.

4. Гачок / як шахрай заманює жертву.

- Дзвінок із повідомленням про нібито ДТП за участю сина.
- Використання образу близької людини для встановлення довіри.
- Наголошення на терміновості (потрібні кошти на лікування негайно).
- Пропозиція передати гроші через довірену особу.

5. Запобігання / як уникнути шахрайства.

- Перед тим, як діяти, слід обов'язково зателефонувати родичу.
- Не потрібно впускати незнайомців у дім і віддавати їм гроші.
- У разі виникнення підозри слід одразу телефонувати в поліцію.



Кейс-картка № 3

"Фейковий працівник банку. Захист рахунку"



Короткий опис справи: жительці Заліщиків зателефонував псевдопрацівник банку, який повідомив про те, що хтось нібито спробував увійти до її кабінету онлайн-банкінгу. Під приводом захисту рахунку жінка надала реквізити платіжної картки та коди з SMS. У результаті з її рахунку зникло 113 000 грн.

1. Дії шахрая.

- Зателефонував жінці та представився працівником банку / служби безпеки банку.
- Повідомив неправдиву інформацію про несанкціонований вхід та оформлення кредиту.
- Виманив у жертви дані платіжної картки (номер, термін дії, CVV-код) та коди з SMS.
- Використав отримані дані для переказу грошей на невідомі рахунки.

2. Жертва шахрая.

- Жінка, 32 роки.
- Жителька міста Залішки, Тернопільщина.
- Повірила в легенду про захист рахунку.

3. Емоції / психологічні тригери.

- **Страх втратити гроші.** Повідомлення про спробу входу до кабінету онлайн-банкінгу та оформлення кредиту спричиняє сильне хвилювання, ніби кошти ось-ось зникнуть. Це блокує критичне мислення.
- **Почуття терміновості.** Шахрай змушує реагувати негайно (щоб захистити рахунок саме зараз), позбавляючи часу, щоб перевірити інформацію чи звернутися до банку самостійно.
- **Ілюзія довіри.** Використання образу працівника служби безпеки банку автоматично знижує рівень підозри та викликає довіру до сказаного.
- **Емоційний тиск через відповідальність.** Потерпіла відчула, що саме від її швидких дій залежить збереження грошей, і погодилася надати конфіденційні дані.

4. Гачок / як шахрай заманює жертву.

- Легенда про спробу входу до онлайн-кабінету та оформлення кредиту.
- Використання авторитету банку (служби безпеки банку).
- Створення враження, що потрібна допомога самої жертви для захисту рахунку.

5. Запобігання / як уникнути шахрайства.

- Якщо телефонує працівник банку, потрібно сказати, що ви зараз перетелефонуєте самостійно на офіційний номер банку, зазначений на платіжній картці. Працівники банку ніколи не телефонують і не просять дані картки чи коди з SMS.
- Не слід розголошувати дані платіжної картки: PIN-код, CVV-код, логін та пароль до інтернет-банкінгу, SMS-коди від банків або іншу конфіденційну інформацію.
- У разі виникнення підозри потрібно відразу повідомляти поліцію та банк.





Кейс-картка № 4 "Фейковий працівник банку. Невикористання кредитної картки"

Короткий опис справи: жительці Чернігова зателефонувала псевдопрацівниця банку та залякала штрафом за невикористання картки. На підставі авторизації картки вона змусила жінку переказати кошти на зазначені рахунки. Потерпіла втратила понад 125 000 грн.

1. Дії шахрайки

- Зателефонувала й представилася працівницею банку.
- Повідомила неправдиву інформацію про штраф через невикористання картки.
- Надала інструкції переказувати кошти між картками, знімати готівку та надсилати на зазначені рахунки.

2. Потерпіла.

- Жінка, 63 роки.
- Жителька міста Чернігова.
- Довірилася псевдопрацівниці банку.
- Розгубилася через можливий штраф.

3. Емоції / психологічні тригери.

- **Страх покарання.** Повідомлення про штраф за невикористання картки спричиняє виникнення тривоги та бажання уникнути негативних наслідків. Це блокує критичне мислення.
- **Почуття терміновості.** Шахрайка створює відчуття, що діяти потрібно негайно, інакше штрафу не уникнути. Це позбавляє часу на перевірку інформації в банку.
- **Ілюзія довіри.** Використання ролі працівниці банку знижує рівень підозри та викликає впевненість у правдивості її слів.
- **Емоційний тиск через відповідальність.** Потерпіла відчула, що від її швидких дій залежить, чи уникне вона фінансових проблем, і погодилася виконувати вказівки шахрайки.

4. Гачок / як шахрайка заманила жертву.

- Представляється працівницею банку, створюючи ілюзію офіційності.
- Залякує штрафом за невикористання кредитної картки.
- Пропонує просте рішення — пройти авторизацію, виконуючи її інструкції.
- Дає вказівки, як переказувати кошти та надсилати їх, прикриваючись турботою про клієнта.

5. Запобігання / як уникнути шахрайства.

- Якщо телефонує працівник банку, потрібно сказати, що ви зараз перетелефонуєте самостійно на офіційний номер банку, зазначений на платіжній картці.
- Слід припинити розмову, якщо в телефонній розмові керують вашими діями (просять зробити трансакцію, встановити програму на ваш пристрій);
- Не потрібно розголошувати дані платіжної картки: PIN-код, CVV-код, логін та пароль до інтернет-банкінгу, SMS-коди від банків або іншу конфіденційну інформацію.
- У разі виникнення підозри слід одразу повідомити поліцію та банк.



Кейс-картка № 5 "Фейкові працівники банку. Захист мобільного застосунку"

Короткий опис справи: 40-річній жительці Чернігова зателефонували псевдопрацівники банку та переконали "поставити захист на мобільний додаток банку". Жінку змусили переказати власні кошти й оформити кредит, після чого гроші переказали на рахунки шахраїв. Загальна сума збитків — 162 000 грн.

1. Дії шахраїв

- Чоловік зателефонував і представився працівником служби безпеки банку.
- Повідомив неправдиву інформацію про потребу "поставити захист на мобільний додаток банку".
- Переконав потерпілу переказати власні кошти на зазначений номер банківської картки.
- Пізніше інша шахрайка, представившись працівницею банку, вмовила жінку оформити кредит у додатку.
- Дала інструкції переказати кредитні кошти на рахунок незнайомки.
- Після проведення трансакцій шахраї зникли й перестали виходити на зв'язок.

2. Потерпіла.

- Жінка, 40 років.
- Жителька міста Чернігова.
- Довірилася працівникам банку.
- Вірила, що захищає свої гроші від сторонніх.

3. Емоції / психологічні тригери.

- **Страх втратити контроль.** Повідомлення про небезпеку доступу сторонніх до акаунту спричиняє паніку та бажання негайно "поставити захист". Це відключає критичне мислення.
- **Почуття терміновості.** Шахраї переконували діяти негайно, щоб "захистити додаток", не залишаючи часу для перевірки інформації в банку.
- **Ілюзія професійності.** Використання образів "працівника служби безпеки банку" та "працівниці банку" автоматично знижувало підозру й створювало довіру.
- **Маніпуляція допомогою.** Шахраї видавали свої вказівки за "турботу про клієнта", змушуючи потерпілу виконувати їхні інструкції.
- **Емоційний тиск через відповідальність.** Жінка повірила, що від її дій залежить безпека грошей, і погодилася навіть оформити кредит, щоб "врятувати рахунок".



4. Гачок / як шахрай заманює жертву.

- Шахраї представилися працівниками служби безпеки банку, створюючи ілюзію офіційності.
- Використали аргумент про захист додатку від сторонніх осіб.
- Дали псевдотурботливі інструкції, які виглядали як допомога клієнту.
- Запропонували нібито єдиний спосіб уникнути загрози — переказати гроші та оформити кредит.

5. Запобігання / як уникнути шахрайства.

- Якщо телефонує працівник банку, потрібно сказати, що ви зараз перетелефонуєте самостійно на офіційний номер банку, зазначений на платіжній картці.
- Слід припинити розмову, якщо в телефонній розмові керують вашими діями (просять зробити трансакцію, встановити програму на ваш пристрій);
- Не потрібно розголошувати дані платіжної картки: PIN-код, CVV-код, логін та пароль до інтернет-банкінгу, SMS-коди від банків або іншу конфіденційну інформацію.
- У разі виникнення підозри слід одразу повідомляти поліцію та банк.