Вебінар на тему: ***«Інтернет-павутина: ризики, шахрайство та способи захисту»***

•Презентацію підготувала:

•Христина Плюта

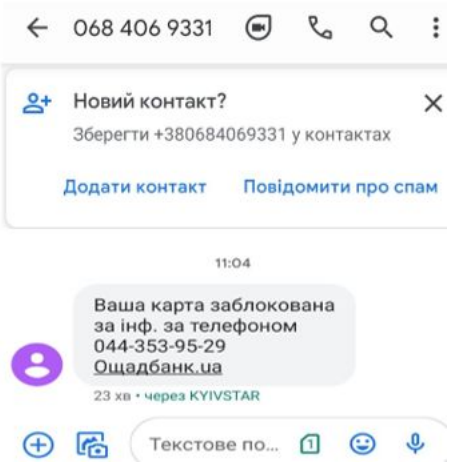
•Менеджер відділу протидії електронному та картковому шахрайству

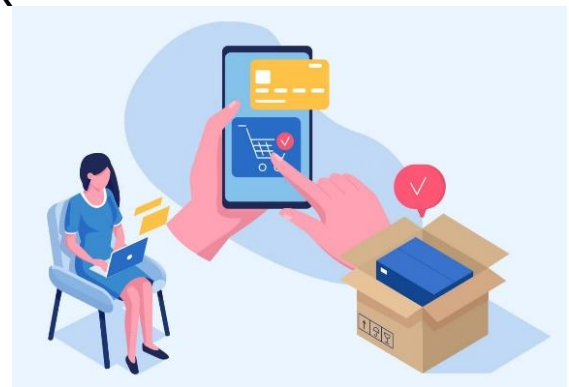
•Департаменту банківської безпеки

•АТ «Кредобанк»

План вебінару

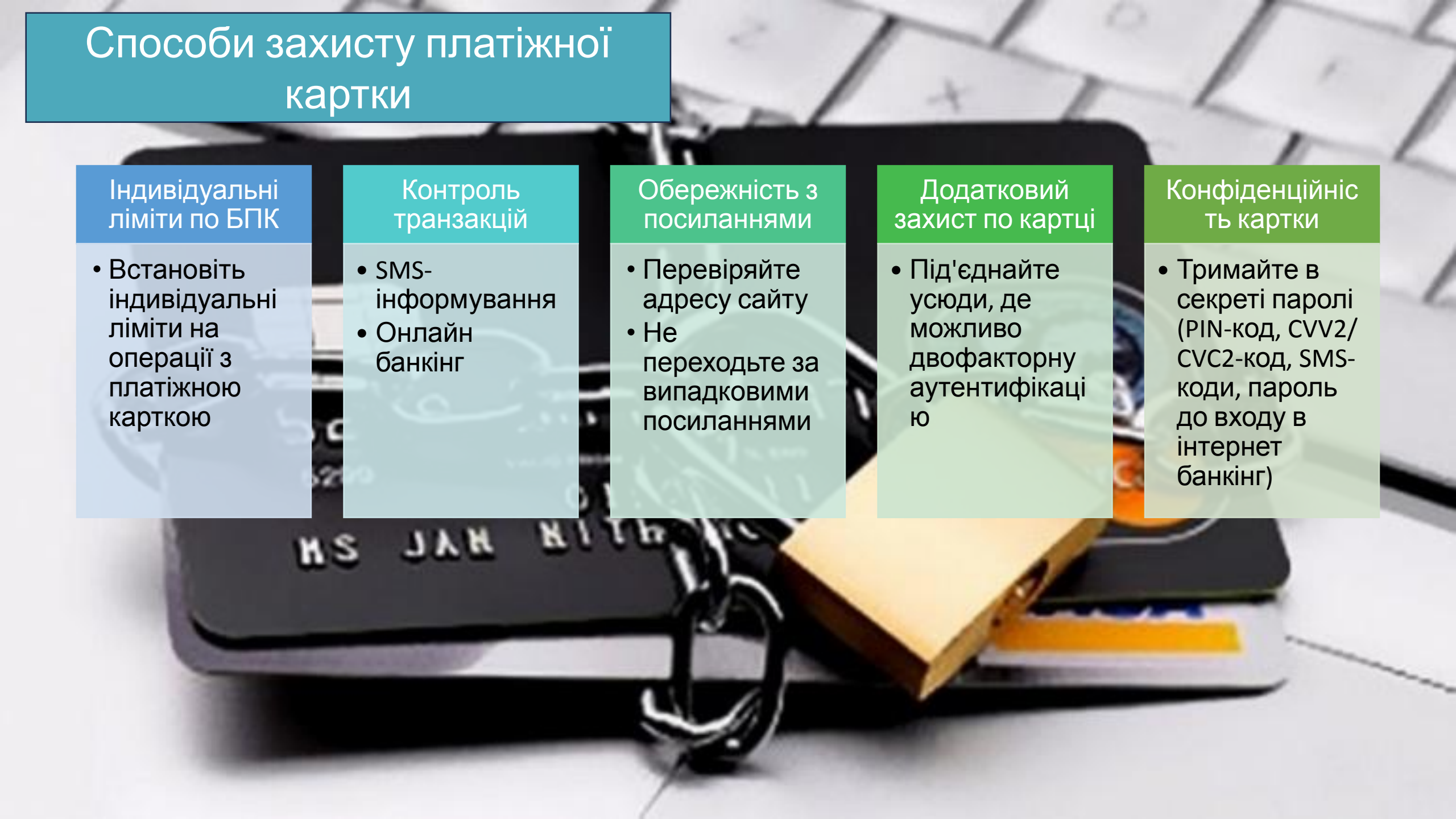
- Інтернет і гроші: як безпечно користуватися банківськими картками та онлайн-платежами
- Онлайн-покупки без ризику: як розпізнати фейкові магазини та оголошення
- Небезпечні програми та застосунки: чому «безкоштовне» може коштувати дорого
- Чат-боти та штучний інтелект: що можна і чому не варто їм довіряти
- Фінансовий номер телефону: як його використовують шахраї
- Соціальна інженерія: як маніпулюють довірою в соцмережах і месенджерах





Інтернет і гроші: як безпечно користуватися банківськими картками та онлайн-платежами

Способи захисту платіжної картки



Індивідуальні ліміти по БПК

- Встановіть індивідуальні ліміти на операції з платіжною карткою

Контроль транзакцій

- SMS-інформування
- Онлайн банкінг

Обережність з посиланнями

- Перевіряйте адресу сайту
- Не переходьте за випадковими посиланнями

Додатковий захист по картці

- Під'єднайте усюди, де можливо двофакторну аутентифікацію

Конфіденційність картки

- Тримайте в секреті паролі (PIN-код, CVV2/CVC2-код, SMS-коди, пароль до входу в інтернет банкінг)

Переваги покупок в інтернеті

- Зручність
- Великий асортимент
- Можливість економити
- Доставка додому або до поштомату
- Можливість читати відгуки

Ризики покупок в інтернеті

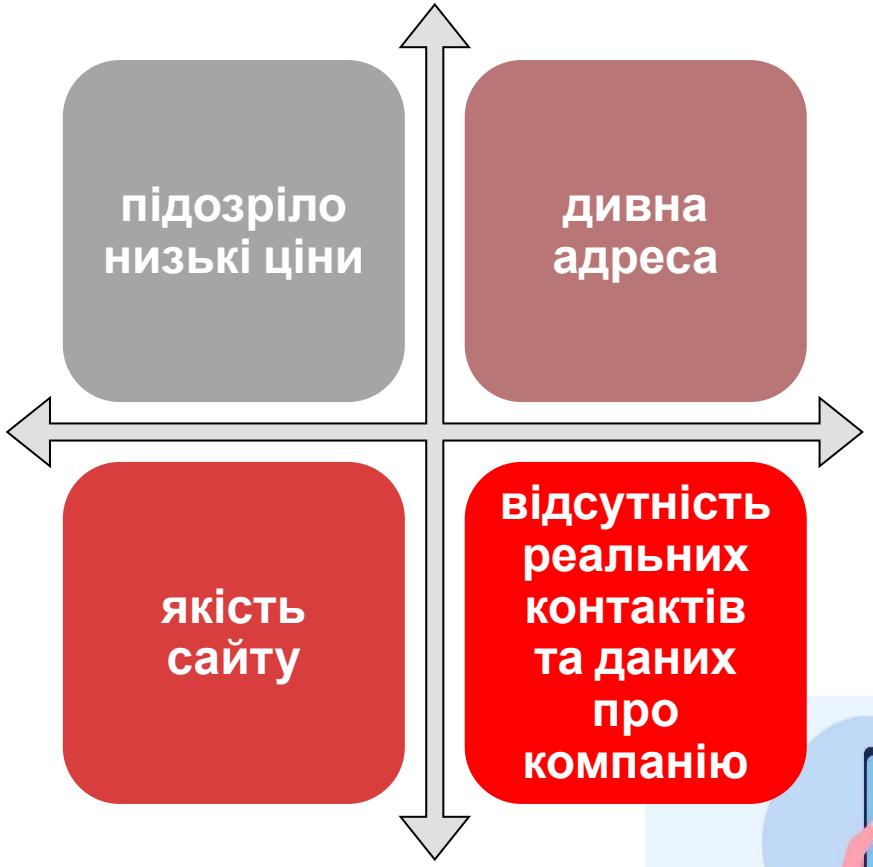
- Шахрайство
- Отримання неякісного товару
- Крадіжка персональних чи платіжних даних
- Схеми із завищеною ціною доставки
- Довга або проблемна доставка

Сайти, які приймають онлайн-платежі, мають бути захищеними: в адресному рядку повинно бути

Використовуйте лише перевірені ресурси та переконайтеся у правильності назви необхідного сайту

Онлайн-покупки без ризику: як розпізнати фейкові магазини та оголошення

Ознаки фейкового інтернет-магазину



Фейкові оголошення в соцмережах та на маркетплейсах

Як безпечно здійснювати покупки в Інтернеті?

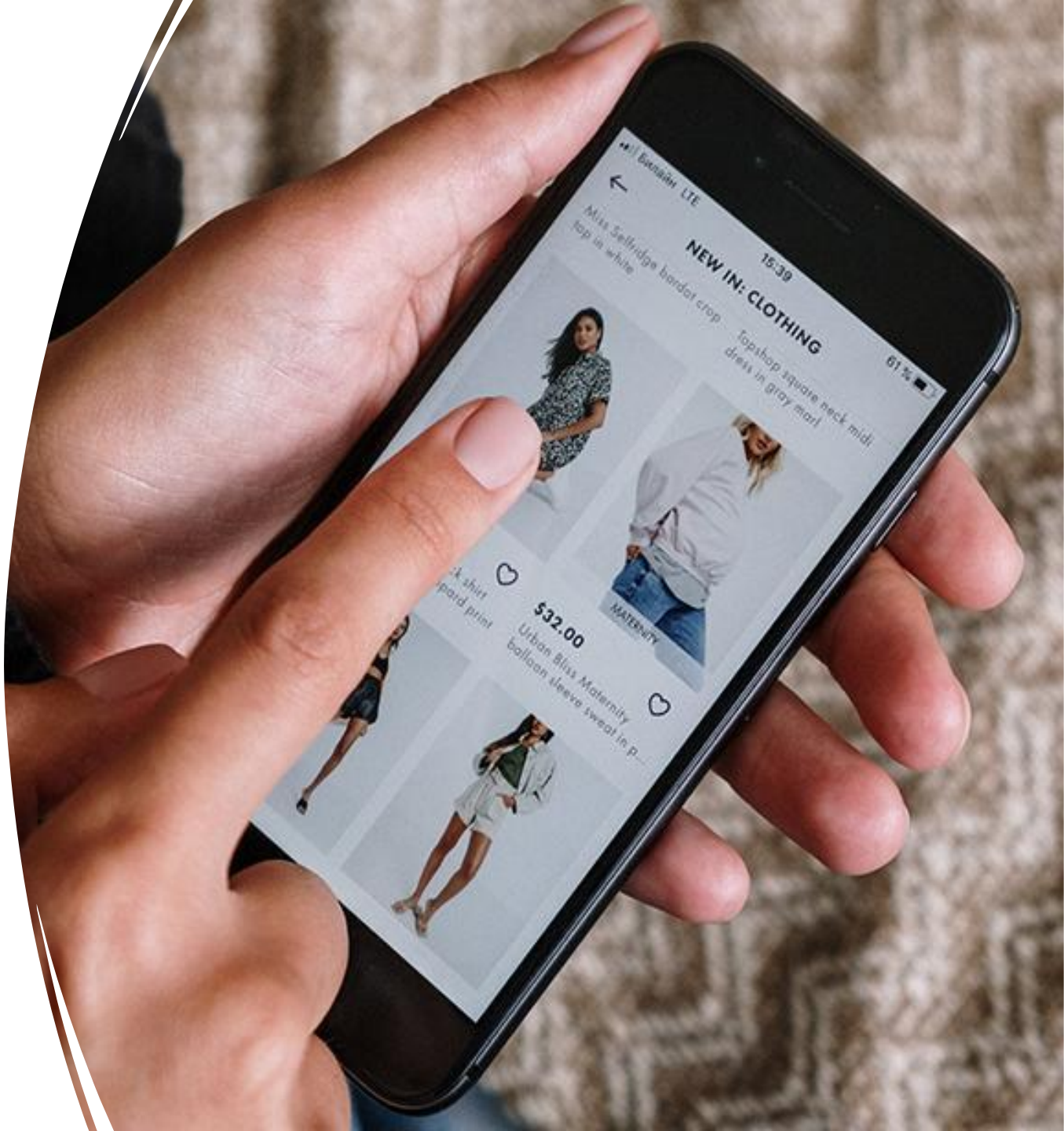
Використовуйте віртуальну/діджитал картку для розрахунків в Інтернеті

Купуйте онлайн на перевірених сайтах

Не відправляйте передоплату, не перевіривши дату реєстрації акаунту на ресурсі, як часто змінювалось ім’я продавця

Остерігайтеся занадто низьких цін

Обговорюйте деталі угоди лише в межах сайту – не переходьте в месенджери (Viber, Telegram, WhatsApp тощо)



Небезпечні програми та застосунки: чому «безкоштовне» може коштувати дорого

Ознаки ризику небезпечних програм чи застосунків

Основні правила безпеки

Небезпечні програми та застосунки: як уникнути ризиків

Поведінка користувача

• Якщо програма виглядає «безкоштовною, але чудовою» — варто задуматися.
• Не встановлюйте програми/ не завантажуйте файли із невідомих джерел та за порадою від незнайомих відправників
• Не переходьте за посиланнями зі спливаючих вікон чи реклами
• Уважно вивчайте всі умови підписок, що оформлюються

Пам’ятка для учасників

• Якщо ви не платите грошима — ви платите своїми даними, безпекою, продуктивністю пристрою, фінансами
• Якщо підписка активувалася через магазин додатків — скасуйте її в налаштуваннях акаунту (App Store / Google Play) та попросіть повернення коштів
• Якщо встановлено програмне забезпечення - відключіть інтернет-з’єднання та видаліть ці програми.
• За необхідності перезавантажте телефон, включіть інтернет-з’єднання, зателефонуйте до банку та повідомте про шахрайство

Пам’ятайте

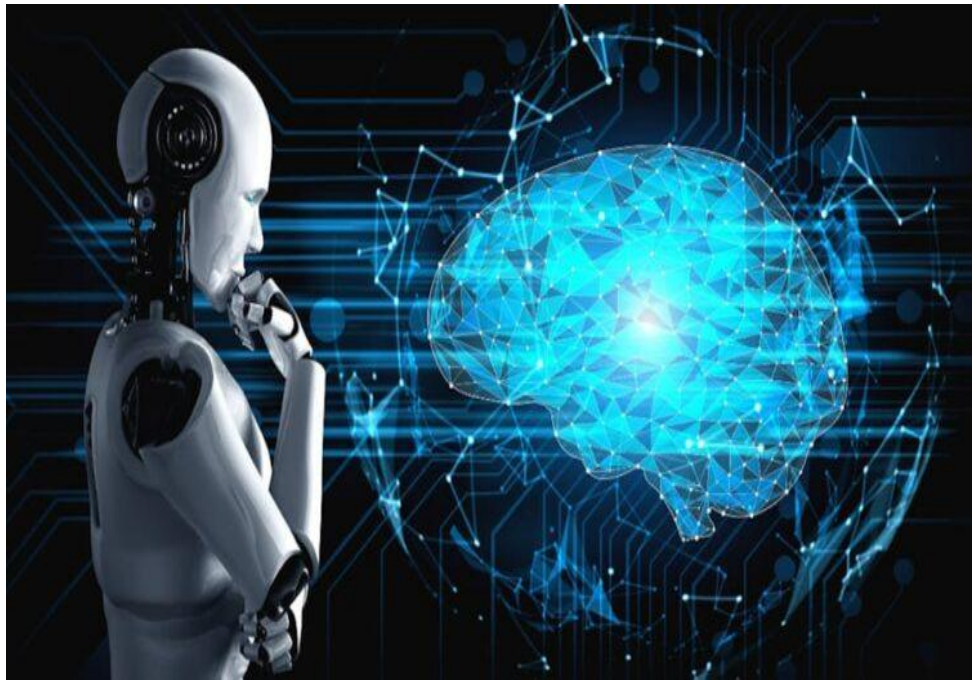
Інтернет пропонує зручність, але й відкриває можливості для шахраїв.

Навіть звичайний тест або «чудодійна програма» може обернутись реальною втратою грошей.

Будьте уважні, не передавайте дані картки невідомим сайтам і довіряйте лише перевіреним сервісам.

Навіть «безкоштовний тест» може коштувати дорого.

Чат-боти та штучний інтелект: що можна і чому не варто їм довіряти



Що ШІ справді вміє добре

Чому не варто довіряти ШІ на 100%

- ШІ може помилятися
- Він не розуміє контексту так, як учитель
- Може містити упередження
- Конфіденційність і безпека
- Підміна мислення

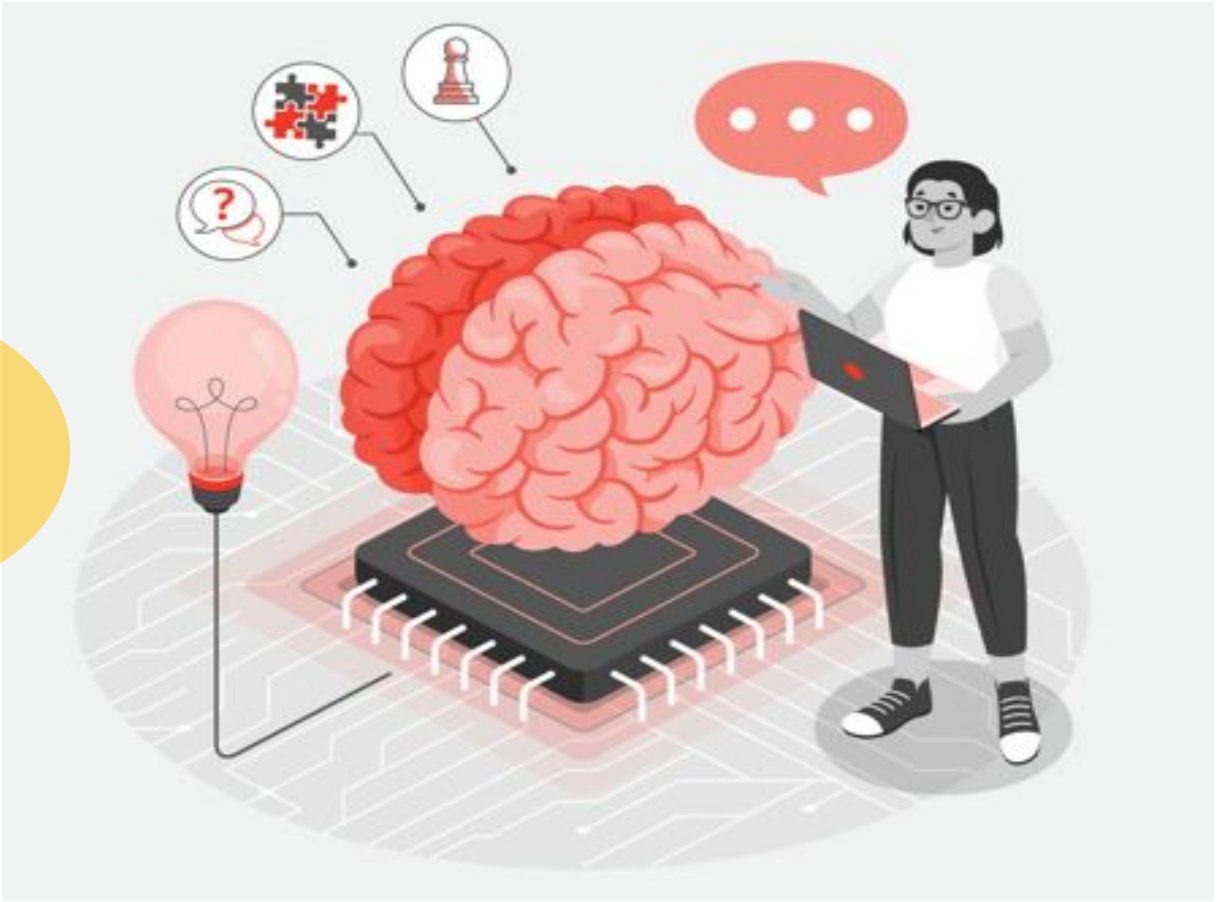
Довіра — обережна.

Використовуйте для навчання та творчості.

Як правильно користуватися ШІ?

Не пишіть особисті дані.

Сприймайте ШІ як *помічника*, а не *вчителя*.



Чат-боти

ПЕРЕВАГИ

- Доступність 24/7
- Стандартизація відповідей
- Швидкість реакції

НЕДОЛІКИ

- Обмежене розуміння контексту
- Ризики конфіденційності
- Залежність і зниження самостійності


Користуйтеся лише офіційними контактами банку зазначеними на його сайті та дізнайся чи використовує банк офіційно чат-бот
Не завантажуйте застосунки/ файли та не відкривайте посилання, які отримуєте через чат-боти або в месенджерах від сумнівних джерел
Чат-боти
Ніколи не вводьте конфіденційну інформацію в чат-боти
Перейдіть на офіційний сайт відповідної організації, від імені якої пропонується грошова допомога

Фінансовий номер телефону: як його використовують шахраї

Підміна SIM-картки

Метою підміни SIM-картки є доступ до банківських рахунків, BankID, Apple/ Google акаунта, пошти, облікових записів у соцмережах та месенджерах, фото та відео із подальшою крадіжкою коштів або шантажу

Як відбувається?

шахрай перевипускає SIM-карту, звернувшись до мобільного оператора з повідомленням про крадіжку телефону

Варіанти підміни SIM-картки:

- відповівши на ідентифікаційне питання про «останні дзвінки», які шахрай попередньо сам і зробив, або надавши PUK-код
- через особистий кабінет мобільного оператора, який шахрай реєструє сам, одночасно виманюючи у жертви SMS-код оператора
- надавши скан-копію або підроблений паспорт жертви у магазині оператора

Як захиститися?

Перейдіть на контрактне обслуговування фінансового номеру

Ідентифікуйтеся у свого мобільного оператора, зареєструйтеся в персональному кабінеті мобільного оператора

Негайно реагуйте на ознаки заміни SIM-картки

Відключіть можливість віддаленого перевипуску SIM-картки

Не використовуйте цей номер в соц.мережах, оголошеннях

Соціальна інженерія: як маніпулюють довірою в соцмережах і месенджерах

Соціальна інженерія — це метод маніпуляції людиною з метою отримання конфіденційної інформації, наприклад, персональних даних, реквізитів банківських карток, кодів підтвердження з SMS, облікових даних інтернет-банкінгу з подальшим використанням для вчинення шахрайства.

Фішинг	створення шахрайських сайтів, схожих на легітимні, та розсилання листів з шкідливими файлами або посиланнями
Смішинг (SMS-фішинг)	шахрайство через SMS із повідомленнями про виграші, блокування акаунтів, що спонукає перейти за посиланням або завантажити шкідливі програми
Вішинг (телефонний фішинг)	телефонне шахрайство з метою отримання конфіденційної інформації або спонукання до дій
Квішинг (QR-фішинг)	шахрайські QR-коди, що ведуть на підмінні сайти


Погана граматика або занадто офіційна лексика
Дивна адреса відправника
Запит на конфіденційну інформацію
Почуття терміновості
Ознаки соціальної інженерії
Щось звучить занадто добре, щоб бути правдою

Як уберегтися від соціальної інженерії?

НЕ ВІР!

- Банки не запитують код зі зворотного боку картки

НЕ БІЙСЯ!

- Якщо картку справді заблоковано, жодні операції з нею неможливі

НЕ СПІШИ!

- Самостійно зателефонуй до банку за номером, зазначеним на платіжній картці, та спокійно з’ясуй усі деталі

Серіал "Школа платіжної грамотності"

Корисні QR-коди офіційних сторінок державних установ, вартих уваги

Центр фінансових знань ТАЛАН

Платіжна безпека від НБУ

Кіберполіція

ДЯКУЮ ЗА УВАГУ!

БЕРЕЖІТЬ СЕБЕ ТА РІДНИХ