

Соціальна інженерія

Що таке соціальна інженерія (CI)?

CI – це наука, що вивчає людську поведінку та фактори, які на неї впливають.

Мета CI: - дослідження причин тієї чи іншої поведінки людини;
- вивчення обставин та середовища, що впливають на формування системи цілей та цінностей індивіду, і як наслідок – його поведінки;
- розробка та застосування методів впливу на людину та захисту від них

У контексті інформаційної безпеки, CI – це психологічне маніпулювання людьми, з метою змусити їх вчинити певні дії, наприклад повідомити свої персональні дані, перейти та завантажити файл за посиланням тощо, які особа не вчинила б, якщо б нею не маніпулювали.

Все своє життя кожна людина є об'єктом та суб'єктом психологічного маніпулювання.

Ми все життя розмовляємо прозою)

Зараз - і у кіберпросторі.

Чому хакери використовують СІ?

- **Це дешево.** СІ не вимагає таких значних затрат, як на розробку ШПЗ чи експлойтів; [?]
- **Це ефективно.** СІ до сьогодні вважається одним із найефективніших методів хакерських атак. Атаки із використанням СІ є передумовою та відправною точкою атак із використанням ШПЗ. Хакери застосовують СІ для отримання первинного доступу до мережі, а вже потім застосовують складне ШПЗ, щоб надійно «засісти» в системі, викрасти дані тощо. Розробити ШПЗ чи знайти вразливість у програмному забезпеченні – це тільки частина атаки, важливо «переконати» жертву перейти за посиланням та завантажити ШПЗ; [?]
- **Це універсально.** СІ ефективна проти будь-якої операційної системи та версії програмного забезпечення, від неї не захистять антивіруси.

Популярні технічні вектори атак

Атаки на програму



Вразливості



Вразливості

Атаки на людину

Популярні технічні вектори атак



Фішинг



Вішинг

спам

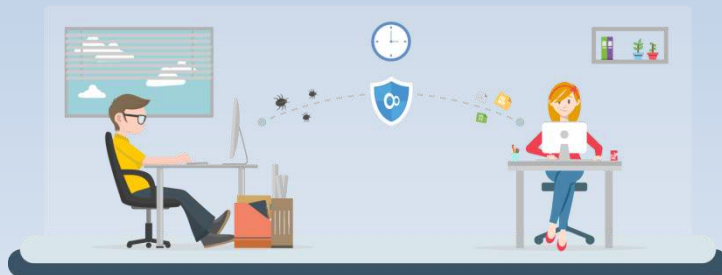


Спам

Спливаючі вікна

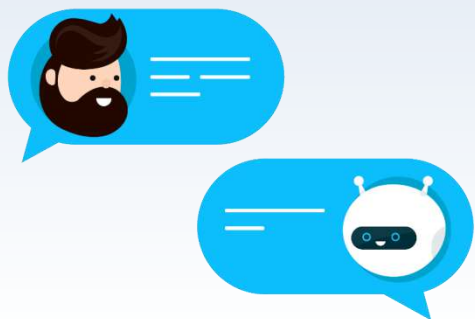


Популярні технічні вектори атак



Інсайдерські атаки

Завантаження
програм



Месенджери

Популярні соціальні вектори атак



Підглядання та
підслуховування



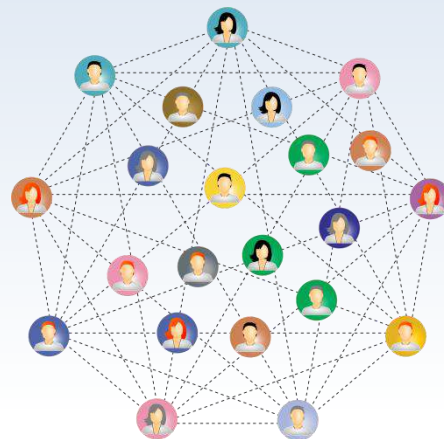
Аналіз сміття



Імперсонація

Популярні соціальні вектори атак

Зворотна соціальна
інженерія



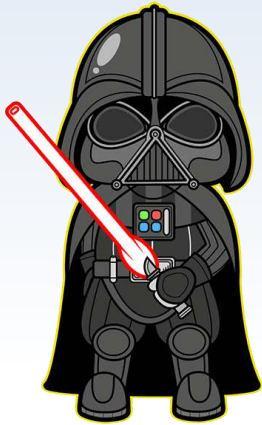
OSINT

Популярні соціальні вектори атак



Посередник

Дорожнє яблуко



?



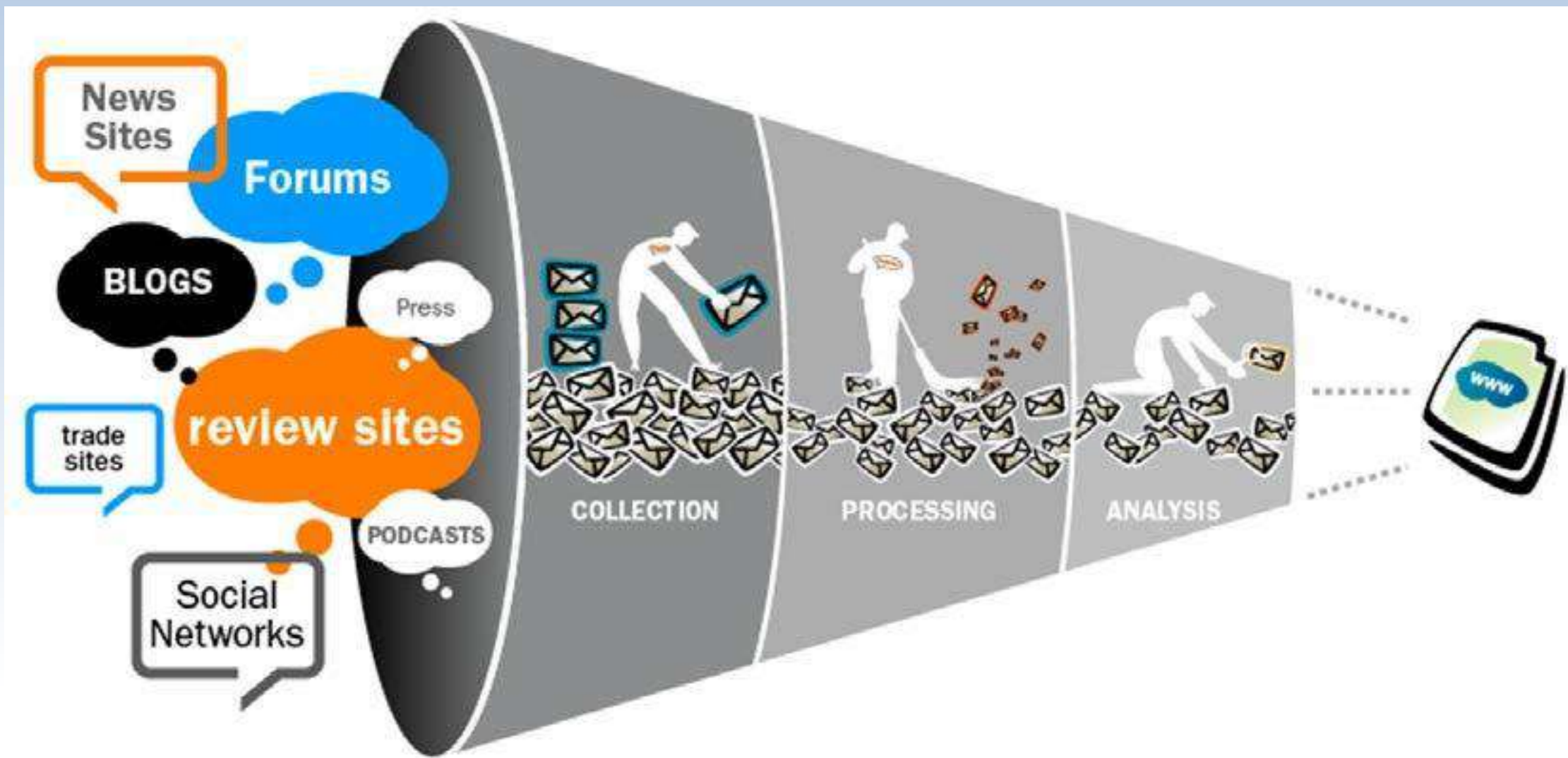
Етапи атаки з використанням СІ

1. Розвідка та збір інформації.

Щодо конкретної особи: акаунти в соціальних мережах; емейли, номери телефонів та адреси інтернет-месенджерів; деталі щодо сімейного стану, дітей, дружини/чоловіка, батьків тощо; місце роботи, заняття, хобі, як проводить вільний час, відпустку; деталі щодо посади, як давно працює у компанії/установі, чи задоволений місцем праці, посадою тощо; наявність автотранспорту, нерухомості, іншого майна; соціальна та громадська діяльність.

Щодо компанії чи державної установи:

- як побудована мережева інфраструктура ,
- яким чином здійснюється доступ до мережі «Інтернет»;
- чи використовують (яке?) антивірусне програмне забезпечення;
- версія операційної системи;
- як побудований бізнес, партнери компанії та підрядні організації;
- адреси головного офісу та філіалів



2. Легендування та планування атаки

Підготовка всього необхідного інструментарія:

- створення фішингового листа,
- написання тексту,
- створення та розкрутка (або придбання) фейкового акаунту у соцмережі,
- придбання бази даних емейлів державних установ та ін.

3. Атака

Жертве дзвінок з банку з підміною номера, лист від доброго знайомого, повідомлення у месенджер и т.п.

Найпоширеніші стандартні схеми обману

- **SMS-вікторина**

Пришліть якомога більше SMS на номер “XXX” і виграйте телевізор (машину, поїздку і т.д.). Як правило, внизу дрібними літерами прописано, що кожне смс коштує певну, доволі велику суму грошей, а шанси на перемогу мінімальні.

- **SMS-піддавки**

Як правило, приходить SMS наступного змісту: “Системне повідомлення. Акція! Перекажіть гроші на номер “XXX” і отримайте вдвічі більше!”.

- **“Поверніть гроші!”**

Приходить SMS, що повідомляє Вас про надходження коштів на мобільний рахунок, а через кілька секунд відбувається вхідний дзвінок. Голос повідомляє, що тільки що помилково переказав гроші не на той номер, і просить повернути їх за допомогою послуги “Мобільний переказ”.

- **Дзвінок від працівника банку**

Стався технічний збій в програмі банку, в результаті чого Ви може втратити усі свої заощадження. Телефонний співрозмовник запевняє Вас, що проблему можна вирішити прямо зараз, але для цього від Вас вимагається повідомити додаткову інформацію у вигляді ПІН-коду та номеру банківської карти.

- **Родич потрапив у біду (затриманий поліцією, скоїв ДТП...)**

На мобільний телефон “жертви” дзвонять з невідомого номера і, як правило, представляються працівником поліції, далі повідомляють, що хтось із близьких родичів потрапив у біду (ДТП, затриманий поліцією, скоїв напад і т.д.) і для “вирішення” питання потрібно заплатити певну суму грошей, але зробити це слід негайно та не повідомляти нікого.

- **Оголошення**

Коли Ви щось втратили, загубили і даєте оголошення в газету або, можливо, розклеюєте їх в місті. Будьте пильні, тому що Вам можуть зателефонувати шахраї, у яких немає загубленої речі, але вони намагатимуться видурити у Вас гроші за повернення.

- **Несподіваний виграш**

Типовий варіант розвитку подій: неочікуваний виграш у лотереї чи в акції (в тому числі від мобільного оператора, якихось фірм тощо).

- **Дзвінок на “дорогий” номер з вакансією роботи**

Часто на сайтах з пошуку роботи можна натрапити на пропозиції, що у порівнянні з іншими здаються набагато вигіднішими,. Як правило, під такими смачними оголошеннями контакти “відділу кадрів” починаються з 090 та 070. Це не код міста або оператора мобільного зв'язку, як може здатися на перший погляд. 090 та 070 – це код платного номера, який з космічною швидкістю “з'їдає” всі гроші

- **Терміново погасіть заборгованість!**

Також можуть приходити смс з вимогою негайно погасити заборгованість: мовляв, більш детально про суму уточніть за таким-то номером телефону.

- **Фейковий приз**

До Вас телефонує радіоведучий відомої програми та вітає з виграшем цінного призу. Щоб його отримати, потрібно протягом хвилини зателефонувати на такий-то номер радіостанції, де Вас ще раз вітають з перемогою.

- **Дзвінок від “служби підтримки”**

Як інтернет-магазини маніпулюють покупцями

Власники інтернет-магазинів вибирають такий дизайн сайту, який примушує покупців здійснювати певні дії або прямо їх обманює.

Кінцева мета - зробити так, щоб покупці ненавмисно приймали потенційно шкідливі для себе рішення.

Такі інтерфейси інтернет-магазинів отримали назву "темний шаблон", тому що вони застосовують типові методи маніпуляцій покупцями.

Існує не менше **15 способів**, за допомогою яких інтернет-магазини примушують покупців витратити більше грошей під час шопінгу. До такого висновку прийшла команда з семи студентів, доцентів і професорів в сфері комп'ютерних наук Принстонського університету і Університету Чикаго в результаті наукового дослідження.

Було проаналізовано 53 тис сторінок 11 тис інтернет-магазинів. З 11 тис просканиваних інтернет-магазинів "темні шаблони" були виявлені на 1 254 (11,1%) торгових сайтах. Чим популярніший сайт, тим, як правило, вище шанс, що він використовує "темний шаблон".

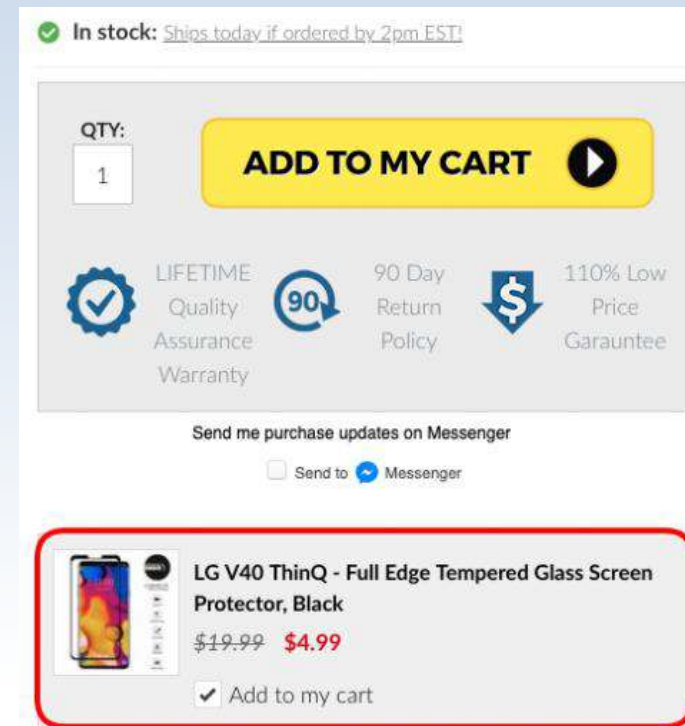
Категорія 1. Підлість

Власники інтернет-магазинів намагаються спотворити дії користувача або не надали інформацію, яка, ймовірно, змусить його змінити своє рішення.

- Проникають в кошик.

Сайти додають товари в кошик покупця без його згоди.

Поширеність - сім випадків на семи сайтах.



- Приховують фінальні витрати. Незазначені платежі показують перед здійсненням покупки. Поширеність - п'ять випадків на п'яти сайтах.

Order Subtotal	\$50.98
Standard Delivery	\$14.99
Care & Handling	\$2.99
Tax	\$4.56
Total	\$73.52
Savings Today ⓘ	\$9.00

Get a Delivery Rebate up to \$15 for your Proflowers purchase! [Learn More](#)

- Приховують підписку. Стягують з покупця періодичну плату під приводом одноразової плати або безкоштовної пробної версії. Поширеність - 14 випадків на 13 сайтах.

Monthly Specials Wine Clubs New Arrivals Your Guide Customer Service My Wine Cellar

Summer in One Case – SAVE over \$100 

The Ultimate Summer Collection:

★★★★☆ 4.2 Average bottle rating ⓘ

[Case Summary >](#)



15 bottles for JUST \$13.29 each

\$199.35

Reg. \$306.35

SAVE \$107.00

Shipping Rates

☐ Enjoy **FREE shipping** with WSJwine Advantage [Learn More](#)

Add to Cart

Item No. A07897

Monthly Specials Wine Clubs New Arrivals Your Guide Customer Service My Wine Cellar

Your Shopping Cart [Proceed to Checkout](#)

[Log in](#) for faster checkout (and to view other items you've saved for later).

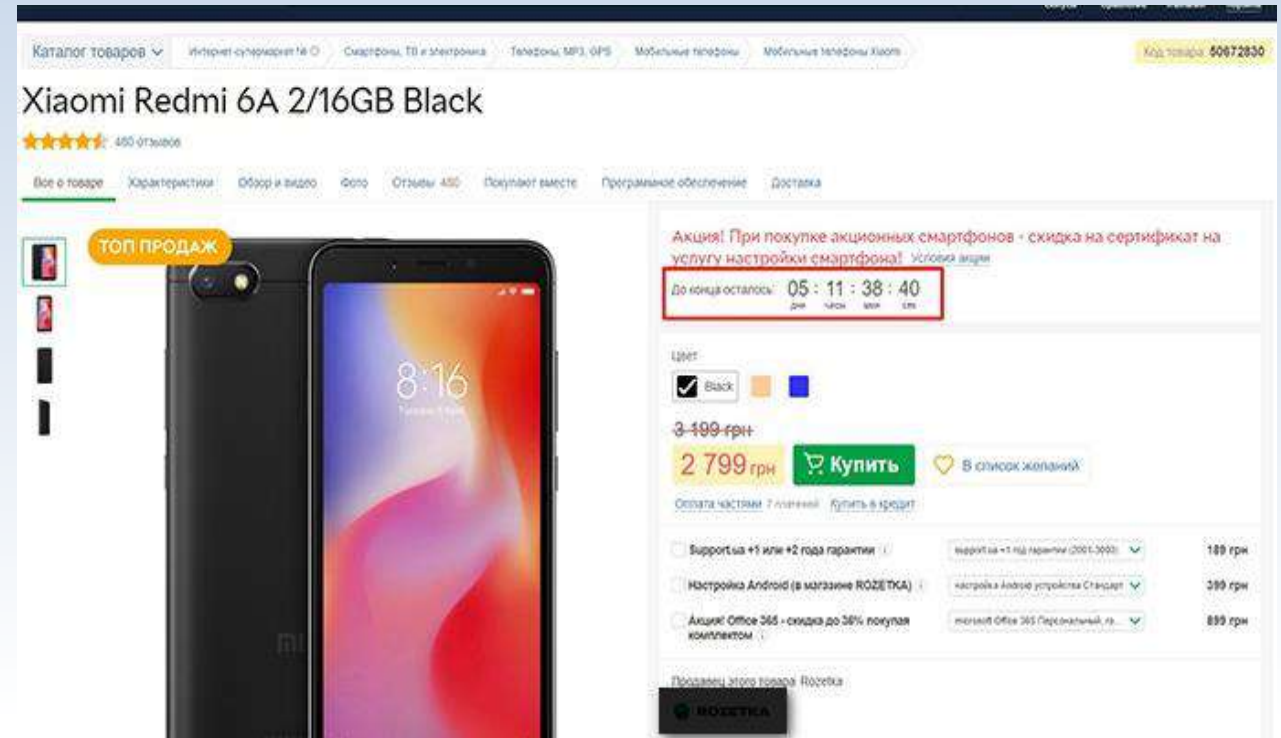
Item Description	Qty	Remove	Price	Subtotal
The Ultimate Summer Collection Item #: A07897 - 15 btl's	1 update		\$306.35 \$199.35	\$306.35 \$199.35
WSJwine 1 Year Advantage Delivery Membership Item #: 1524SQL	1 update		\$89.00	\$89.00

Категорія 2. Терміновість

Встановлюють крайній термін продажу або укладання угоди, щоб прискорити прийняття рішення покупцем про придбання товару або послуги.

- Таймер зворотного відліку.

За допомогою таймера зворотного відліку вказують користувачеві, що термін дії угоди або знижки закінчується. Поширеність - 393 випадки на 361 сайті.

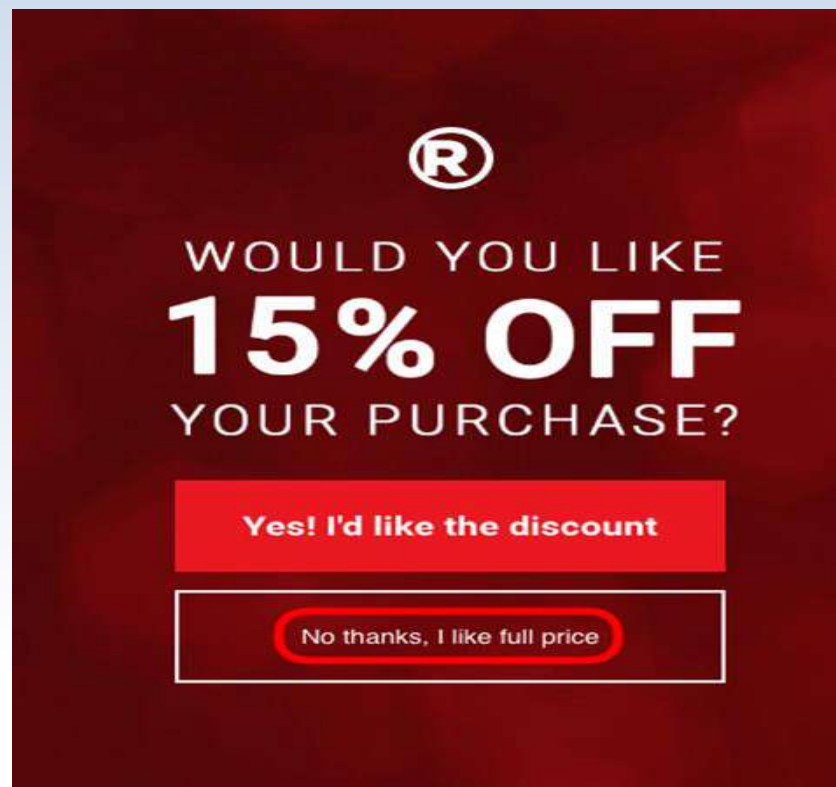


Категорія 3. Помилковий шлях

Використовують візуальні ефекти, маніпулятивні фрази з емоційним забарвленням, щоб змусити покупця зробити певний вибір або відмовитися від не вигідного для продавця рішення.

- Підтвердження.

Маніпулятивні фрази, що викликають негативні емоції, щоб змусити покупця відмовитися від певного вибору. Поширеність - 169 випадків на 164 сайтах.



- Візуальне підроблення.

Оформлення, яке підштовхує покупця до певного вибору.

Поширеність - 25 випадків на 24 сайтах.

CONTACT PREFERENCES

Please select **Yes** below if you are happy to receive email notifications of **exclusive member offers** from M8 Group companies. You will always have the option to unsubscribe from any emails you decide you would rather not receive.

☐ YES I do want to hear about exclusive offers & discounts	☐ NO I'd rather NOT hear about exclusive offers & discounts
--	---

Don't worry, we will never sell or rent your personal information, it's part of our [privacy policy](#). Also, you can update your preferences and unsubscribe from 'My Account' at any time.

- Складні для сприйняття повідомлення.

Тексти складені таким чином, щоб змусити покупця зробити певний вибір. Поширеність - дев'ять випадків на дев'яти сайтах.

The screenshot shows a checkout form with two input fields: 'Phone' and 'Email'. Below the 'Phone' field is a small circular icon with a question mark. Below the 'Email' field is a checkbox. The text next to the checkbox reads: 'We'd love to send you emails with offers and new products from New Balance Athletics, Inc. but if you do not wish to receive these updates, please tick this box. [View Privacy Policy.](#)' The phrase 'if you do not wish to receive' is circled in red. At the bottom of the form is a red button labeled 'CONTINUE TO BILLING'.

- Продаж під тиском.

За замовчуванням інтернет-магазин вибирає дорожчі варіанти продукту. Поширеність - 67 випадків на 62 сайтах.



ТОВАРЫ И УСЛУГИ

МАГАЗИНЫ

UA | RU

Покупки

Все цены

Харьков

Найти товар в каталоге Мобильные телефоны, смартфоны

НАЙТИ

Главная » Электроника » Мобильные устройства » Мобильные телефоны, смартфоны в Харькове (всего 3 094 товара)

Как выбрать мобильный телефон?

Сравнить

MYPHONE

Samsung M32

1

2

3

4

5

...

65

Фильтры

Сортировка

Популярность

☒ С доставкой из других городов

Цена, грн

от 120 до 404643 грн

ОК

Скидки

Условия оплаты

Популярные производители

Alcatel 28

Asus 34

Blackview 117

Doogee 100

Fly 8

Honor 51

Apple 337

Bentley 2

Bravis 11

Ergo 45

Google 43

HTC 22

Xiaomi Redmi Note 10 Pro 6/128Gb Onyx Gray

8 702 грн по ценам 8 145 ... 10 150 грн, в 53 магазинах

Смартфон · 2021 год · 6.67" Super AMOLED, 2400x1080 · камера 108 Мп, 4 объектива · фронтальная 16 Мп · Qualcomm Snapdragon 732G, 2.3 ГГц, 8 ядер · 6 Гб/128 Гб · Android 11.0 · 2x SIM · NFC · Wi-Fi, Bluetooth · стереодинамики · 5020 мАч, быстрая зарядка · 193 г

в сравнение

★★★★★ 2 отзыва

Сравнить цены

Xiaomi Redmi 9 4/64Gb Carbon Gray

4 104 грн по ценам 3 745 ... 4 768 грн, в 27 магазинах

Смартфон · 2020 год · 6.53" IPS, 2340x1080 · камера 13 Мп, 4 объектива · фронтальная 8 Мп · MediaTek Helio G80, 2 ГГц, 8 ядер · 4 Гб/64 Гб · Android 10.0 · 2x SIM · NFC · Wi-Fi, Bluetooth · 5020 мАч, быстрая зарядка · 198 г

в сравнение

★★★★★ 3 отзыва

Сравнить цены

Xiaomi Poco X3 Pro 6/128Gb Phantom Black

7 138 грн по ценам 6 599 ... 8 055 грн, в 47 магазинах

Смартфон · 2021 год · 6.67" IPS, 2400x1080 · камера 48 Мп, 4 объектива · фронтальная 20 Мп ·

Сравнить цены

ОБСЕ

Організація з безпеки та співробітництва в Європі

Координатор проєктів в Україні

UKaid

from the British people

Die Bundesregierung

УКРАЇНСЬКА ШКОЛА УРЯДУВАННЯ

Категорія 4. Соціальний доказ

Вплив на поведінку користувачів шляхом опису досвіду і поведінки інших користувачів.

- Повідомлення про активність. Інформування користувача про активність інших користувачів на сайті, наприклад, кількість скоєних покупок, переглядів, відвідувань. Поширеність - 313 випадків на 264 сайтах.

Тип размещения	Вмещает	Цена за 7 ночей	На ваш выбор	Количество	
Семейный номер с видом на озеро 1 односпальная кровать и 1 двуспальная кровать Семейный номер, Балкон с видом Балкон, Вид на озеро Телевизор с плоским экраном Кондиционер Ванная комната в номере Принадлежности для барбекю Бесплатный Wi-Fi Цена за номер за 7 ночей	3	UAH 9 800 + налоги и сборы (UAH 175,28)	Завтрак UAH 40 (по желанию) Стоимость возвращается частично Последний шанс! Остался 1 номер!	0	Я бронирую - Моментальное подтверждение - Регистрация не обязательна - Отсутствие сборов за бронирование и использование кредитной карты! Кредитная карта не требуется!
Бунгало с видом на сад (для 2 взрослых) Цена за бунгало за 7 ночей	2	Чуть-чуть не успели! Продано за UAH 2 766			Еще 2 человека просматривали на ваши даты за последние 10 минут
Бунгало с видом на сад (для 3 взрослых) Цена за бунгало за 7 ночей	3	Чуть-чуть не успели! Продано за UAH 3 459			
Двухместный номер «Комфорт» с 1 кроватью Цена за номер за 7 ночей	2	Чуть-чуть не успели! Продано за UAH 7 399			
Семейный номер с балконом Цена за номер за 7 ночей	3	Чуть-чуть не успели! Продано за UAH 8 087			

База Отдыха Озерки может взимать дополнительные сборы, не указанные выше. Посмотрите ["Примечания"](#) для более подробной информации об этом варианте размещения.

Количество свободных мест в Затоке ограничено: 4 курортных отеля, похожих на Recreation Center Ozerki, уже недоступны!

Ориентиры поблизости - Великолепное расположение — показать на карте

Гости понравились прогулки в этом районе!

Рестораны, магазины и рынки * Природа *

Кафе Лагуна, бар Кафе/бар 0 км На территории базы отдыха Озерки Озеро 0 км

- Відгуки про продукт або послугу невстановленого походження.

Відгуки на сторінці продукту, походження яких невідоме. Поширеність - 12 випадків на 12 сайтах.

Відгуки покупців



Євген 35 років м. Біла Церква

Що я можу сказати, телефон суперський, не натішуся! Кращий андроїд телефон на ринку. Красивий екран - по яскравості, чіткості, передачі кольору всякі Ксяомі, хуавей і вже тим більше iphone і поруч не стояли. Це просто твір інженерної думки і дизайнерських рішень. Покупкою задоволений дуже сильно. Мені його вистачить на дуже і дуже довго!



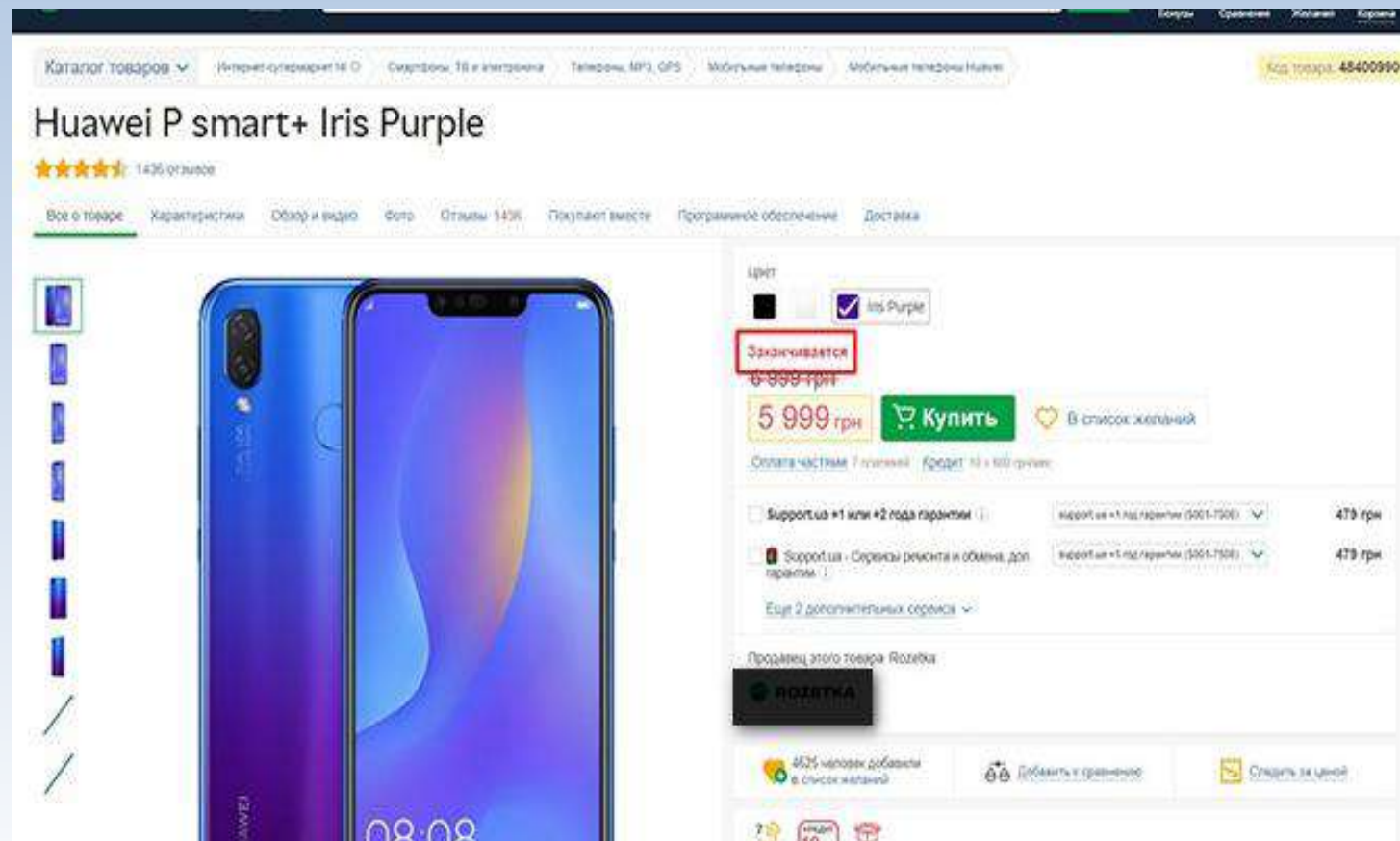
Денис 35 років м. Київ

Чудовий флагманський телефон, втілені найновіші технології. Камера з активною обробкою у процесі знімання це щось. Той випадок коли не пошкодуєш витрачених грошей. Батарею тримає довго, заряджається швидко. Звук чіткий, динамік гарний. Усі основні додатки просто "літають" - фейсбук, інстаграм, ютуб. Повністю виправдав мої очікування!

Категорія 5. Брак

- Попередження про те, що продукт може стати недоступним, що підвищує його цінність в очах покупця.
- Повідомлення про високий попит.

Попередження про великий попит, що підвищує цінність товару. Поширеність - 47 випадків на 43 сайтах.

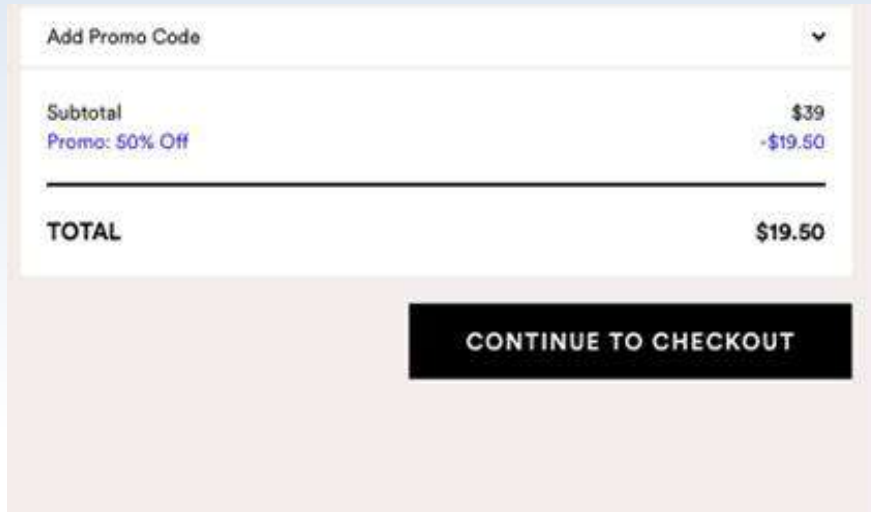


Категорія 6. Перешкоди

Покупцеві легко потрапити в певну ситуацію, але складно з неї вийти.

- Важко скасувати.

Покупцеві легко підписатися на повторювану підписку, але для її скасування потрібно писати лист або звертатися в службу підтримки клієнтів. Поширеність - 31 випадок на 31 сайті.



The screenshot shows a checkout interface. At the top, there is a field labeled 'Add Promo Code' with a dropdown arrow. Below this, a summary table displays the following:

Subtotal	\$39
Promo: 50% Off	-\$19.50
TOTAL	\$19.50

Below the table is a large black button with the text 'CONTINUE TO CHECKOUT' in white capital letters.

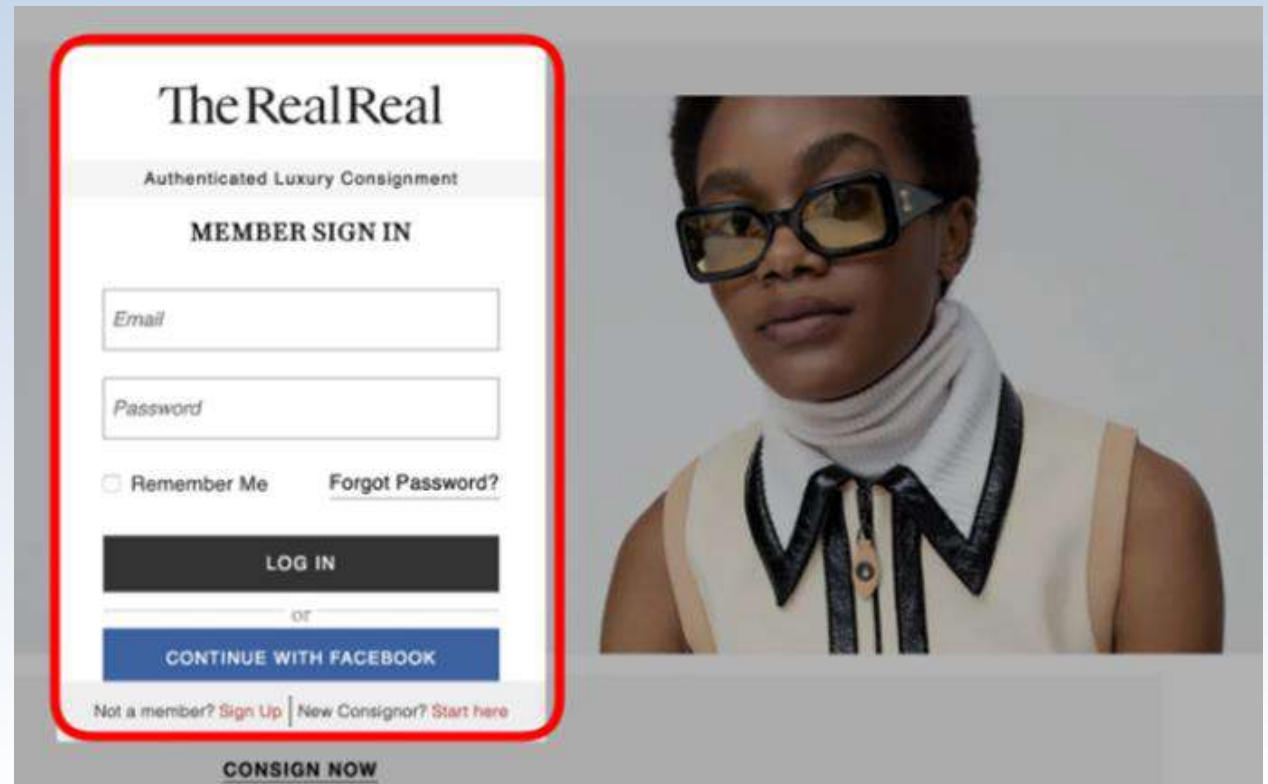
To the right of the checkout area, there is a list of terms and conditions. The first item is 'No Commitment to Buy', which states: 'Shop or "Skip the Month". Skip as many months as you want; it's always your choice. Cancel your membership any time by calling (855) SAVAGEX (open 24/7)'. This entire paragraph is circled in red. The second item is 'Earn VIP Member Credits', which states: 'If you don't shop or "Skip the Month" by the 5th of each month, your payment method will be charged \$49.95 on the 6th until you cancel your membership. That charge becomes a member credit you can use to shop or save.'

Категорія 7. Примус до дії

Примус покупця вчинити певну дію, перш ніж він зможе виконати свою основну задачу.

- Примусова реєстрація.

Примус користувачів створювати облікові записи або ділитися інформацією для виконання своїх завдань. Поширеність – шість випадків на шести сайтах.

A screenshot of the 'The Real Real' website's login page. The page is titled 'The Real Real' and 'Authenticated Luxury Consignment'. Below this, it says 'MEMBER SIGN IN'. There are two input fields: 'Email' and 'Password'. Below the password field, there is a checkbox for 'Remember Me' and a link for 'Forgot Password?'. A black 'LOG IN' button is present, followed by an 'OR' separator and a blue 'CONTINUE WITH FACEBOOK' button. At the bottom of the login section, there are links: 'Not a member? Sign Up' and 'New Consignor? Start here'. A red rectangle highlights the entire login section. To the right of the login form is a portrait of a woman with short dark hair, wearing large black-rimmed glasses, a white turtleneck, and a black and white patterned vest.

Практична вправа.

Яки методи впливу на покупців використовують сайти:

1. <http://mobila.v-magazine.com.ua/s21ultra/>
2. <https://enot.in.ua/en-003725-samsung-galaxy-a72-8256gb-awesome-violet-ua-ucrf-sm-a725flvhsek.html>
3. <https://www.citrus.ua/smartfony/redmi-note-10-pro-6128-glacier-blue-685083.html?app=ssr>

Деякі з ознак, які допоможуть виявити соціальну інженерію:

- Погана граматика або занадто офіційна лексика
- Дивна адреса відправника
- Почуття терміновості
- Запит на конфіденційну інформацію
- Щось звучит занадто добре, щоб бути правдою (безкоштовний сир і дуже багато)

Як протидіяти атакам із використанням СІ?

- Не повідомляйте свої персональні дані чи дані про установу, де ви працюєте
- Уникайте або обмежуйте публікування своїх персональних даних, фотографій в соціальних мережах, на сайтах чи порталах
- Якщо сам емейл чи телефонний дзвінок, який Ви отримали, а також саме прохання телефонуючого чи автора емейлу викликає у Вас підозру, перевірте легітимність емейлу чи самого запиту

- Не повідомляйте персональні дані, не переказуйте кошти, не повідомляйте дані платіжної картки **НИКОМУ.**
Навіть дружині)
- Ігноруйте запити та повідомлення в соціальних мережах від підозрілих акаунтів
- Користуйтесь антивірусами, ліцензійним програмним забезпеченням
- На всіх сервісах, де це можливо, активуйте двохфакторну аутентифікацію

- Не довіряйте підозрілим повідомленням та предметам
- Підтверджуйте особу
- Утилізуйте сміття належним чином
- Навчіться розрізняти працівників своєї установи
- Не робіть фотознімки та відеозаписи на робочому місці
- Перевіряйте інформацію з різних джерел

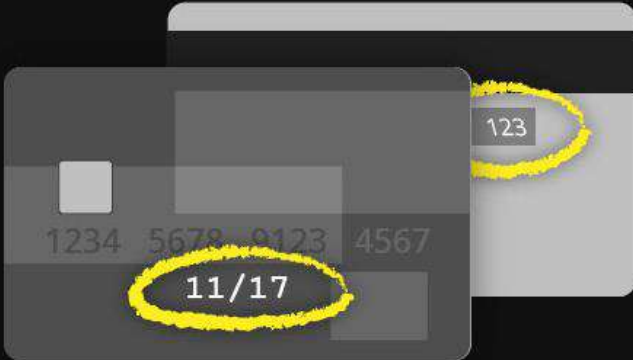
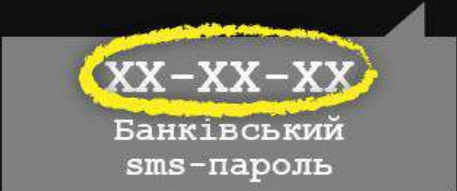
Поради від Департаменту кіберполіції



ВІШИНГ
телефонне
шахрайство

#Cashless

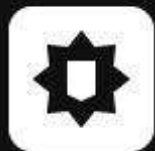
**ЗА ЖОДНИХ УМОВ
НЕ РОЗКРИВАЙТЕ ЦІ
РЕКВІЗИТИ СВОЇХ КАРТОК!**



ШАХРАЙ МОЖЕ ПРЕДСТАВИТИСЯ ЯК:



**СПІВРОБІТНИК
БАНКУ**



**СПІВРОБІТНИК
ПОЛІЦІЇ**



**СПІВРОБІТНИК
ПЕНСІЙНОГО ФОНДУ
АБО ПОДАТКОВОЇ**



**ВОЛОНТЕР
АБО БЛАГОДІЙНИК**



**СПІВРОБІТНИК
СБУ**



**ПОКУПЕЦЬ
ВАШОГО ТОВАРУ**

ЯК РОЗПІЗНАТИ?



Телефонують та запитують реквізити картки

Термін дії, тризначний код зі звороту картки або банківський SMS пароль запитують лише шахраї!



Легкі гроші

Обіцяють гроші, на які ви не очікували (несподіваний виграш у лотерею, перерахунок пенсії тощо).



Наполегливість та поспіх

Наполегливо переконують зробити те, що ви ще хвилину тому робити не збирались.



Телефонують та спрямовують Вас до банкомату чи терміналу

Аргументи та приводи можуть бути різними, а результат один — переказ Ваших грошей на рахунок шахрая.



Тривожна тема

Лякають тим, що ваша картка заблокована, злочинці зламали ваш рахунок.



Запит всіх реквізитів

Для будь-яких зарахувань на вашу картку достатньо її номеру, — жодних інших даних не потрібно.

ЯК ЗАХИСТИТИСЯ?



Давати тільки номер картки

Для отримання будь-якого переказу на вашу картку — достатньо надати покупцеві лише номер картки.



Припинити розмову

Якщо телефонують з приводу блокування вашої картки, — припинити розмову і самостійно зателефонувати до банку.



Не розголошувати ці реквізити:

термін дії картки, тризначний код безпеки з її звороту та банківський sms-пароль.



Не виконувати сторонні команди

Не виконувати в банкоматі чи платіжному терміналі команди, які надають телефоном.

ЯК ДІЯТИ?

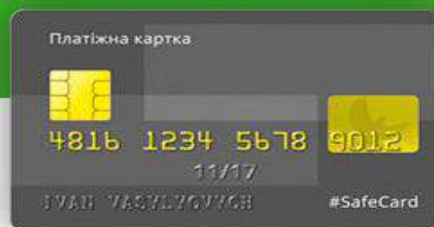
ЯКЩО ВИ ПІДДАЛИСЯ ШАХРАЙСЬКІЙ ПРОВОКАЦІЇ ТА ПОВІДОМИЛИ ШАХРАЯМ РЕКВІЗИТИ СВОЄЇ КАРТКИ, ПОТРІБНО:



Негайно заблокувати вашу картку



Звернутися із заявою до Кіберполіції онлайн
www.cybercrime.gov.ua



Організація з безпеки та співробітництва в Європі
Координатор проектів в Україні



Die Bundesregierung



УКРАЇНСЬКА
ШКОЛА
УРЯДУВАННЯ

Підсумки

Практичні вправи