МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий гуманітарний інститут

Кафедра прикладної лінгвістики

«Допущений до захисту»

Завідувач кафедри

_____Ніна Філіппова

«25» ____06____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття першого (бакалаврського) рівня вищої освіти

на тему:

«Нейролінгвістичні техніки в заголовках фішингових повідомлень»

Виконав: студентка групи 4521

_____Довга М. Ю.

Керівник роботи: д-р. філол. наук, доц.

_____Гогоренко О. В.

(підпис)

Миколаїв – 2024 р.

ЗМІСТ

Анотація. Дипломна робота присвячена дослідженню використання нейролінгвістичних технік у заголовках фішингових повідомлень. В роботі було проведено аналіз фішингових повідомлень, їх структури та лексико-граматичних особливостей. Також було проаналізовано вплив нейролінгвістичних технік на ефективність фішингових повідомлень та їх впізнавання користувачами.
Ключові слова: фішингові повідомлення; фішинг; нейролінгвістичні техніки; кібератаки.

Abstract. The diploma work is devoted to the study of the use of neuro-linguistic techniques in the headers of phishing messages. The paper analyzed phishing messages, their structure and lexical and grammatical features. The influence of neuro-linguistic techniques on the effectiveness of phishing messages and their recognition by users was also analyzed.

Key words: phishing messages; phishing; neuro-linguistic techniques; cyber attacks.

ВСТУП

Актуальність дослідження. Дослідження є дуже актуальним у сучасному цифровому світі, оскільки фішинг-атаки є одним з найбільш поширених та ефективних методів шахрайства в Інтернеті.

Фішинг-атаки полягають у тому, що зловмисники намагаються використовувати підроблені повідомлення, щоб залучити людей до надання конфіденційної інформації або отримання доступу до комп'ютерних систем. Один з ключових елементів фішингового повідомлення - це заголовок, який повинен бути привабливим та запрошуючим для потенційної жертви.

Нейролінгвістичні техніки можуть бути використані зловмисниками для того, щоб зробити фішингові повідомлення більш переконливими та ефективними. Ці техніки включають в себе використання слів та фраз, які сприяють виробленню емоційної реакції у людей, таких як страх, обурення або зацікавленість.

Тому дослідження в галузі нейролінгвістичних технік в заголовках фішингових повідомлень є дуже важливим, оскільки воно допоможе виявити та розробити методи захисту від фішингу, а також надати корисні поради та рекомендації для того, щоб люди могли впізнати та уникнути фішингових атак.

Фішинг – це вид кібератак, при якому злочинці намагаються отримати конфіденційну інформацію, таку як паролі, номери кредитних карток, за допомогою шахрайських повідомлень, що містять посилання на підроблені веб-сайти або зловмисний код.

Заголовки таких повідомлень відіграють важливу роль, оскільки вони привертають увагу користувачів та стимулюють їх до відкриття листа та подальшої взаємодії зі злочинцями.

Дослідження застосування нейролінгвістичних технік у заголовках фішингових повідомлень може допомогти розкрити нові методи та техніки, які використовуються злочинцями. Наприклад, застосування психологічних

технік у заголовках може збільшити ефективність фішингових атак, оскільки злочинці можуть пристосувати повідомлення до певної цільової аудиторії.

Об'єкт - нейролінгвістичні техніки.

Предмет - використання нейролінгвістичних технік в заголовках фішингових повідомлень.

Методи роботи було обрано з урахуванням специфіки предмета, об'єкта, цілей та завдань дослідження. Для вирішення поставлених завдань використовуються такі методи як: метод прагма-комунікативного аналізу; метод лінгвістичного спостереження та опису; метод контекстуального аналізу

Теоретичною базою послужили роботи вітчизняних та зарубіжних дослідників у галузі персуазивної комунікації та теорії мовного впливу (І.А. Стернін, А.В. Голоднов, Є.В. Шелестюк, H. Halmari, T. Virtanen, R.T. Lakoff, D. Tannen), судового дискурсу (Т.В. Дубровська, О.В. Климович, І.В. Палашевська, J. Cotterill, A. Wagner, L. Cheng, Ch. Heffer), риторичної аргументації (Н.К. Пригаріна, Л .Ю.Василенко, Ch.W. .В.Кучеренко, S. Sorlin, Т.А. , R. Belli, K. E. Payment, V. Gold, G. D. Loftus).

Теоретичне значення дослідження полягає в розумінні того, як фішери використовують нейролінгвістичні техніки для підвищення ефективності своїх атак. Дослідження може допомогти зрозуміти, які саме техніки найчастіше використовуються в фішингових повідомленнях, та дозволить розробляти більш ефективні методи протидії таким атакам.

Практичне значення дослідження полягає в тому, що на його основі можна розробити нові методи виявлення та запобігання фішинговим атакам. Наприклад, можна розробити системи, які будуть аналізувати текст повідомлення та виявляти нейролінгвістичні техніки, використані в ньому, щоб зменшити успішність таких атак. Такі системи можуть бути корисними для захисту користувачів від шахраїв та зловмисників, які намагаються вкрасти їхні конфіденційні дані та гроші.

У цілому, дослідження нейролінгвістичних технік в заголовках фішингових повідомлень може мати значний вплив на практику боротьби зі шахрайством та злочинністю в Інтернеті.

Метою дослідження є дослідження використання нейролінгвістичних технік у заголовках фішингових повідомлень з метою підвищення ефективності захисту користувачів від інтернет-шахраїв.

Основні завдання дослідження:

1. Аналіз літератури щодо нейролінгвістичних технік та їх використання в мовленні.

2. Збір фішингових повідомлень та аналіз їх структури та лексико-граматичних особливостей.

3. Вивчення впливу нейролінгвістичних технік на ефективність фішингових повідомлень та їх впізнавання користувачами.

4. Розробка та валідація методики для виявлення фішингових повідомлень з використанням нейролінгвістичних технік.

5. Розробка рекомендацій щодо підвищення ефективності захисту користувачів від фішингових атак з використанням нейролінгвістичних технік.

6. Проведення експериментального дослідження та аналіз результатів для підтвердження ефективності запропонованих методів та рекомендацій.

7. Розроблення електронного довідника.

Наукова новизна. Нейролінгвістичні техніки є важливим інструментом у сфері кібербезпеки, зокрема, в боротьбі з фішинговими атаками. Проте, дослідження використання нейролінгвістичних технік в заголовках фішингових повідомлень є досить новим напрямком.

Дослідження може включати аналіз зразків фішингових повідомлень, що містять шкідливі посилання або вкладення. Зокрема, можна дослідити застосування нейролінгвістичних технік, таких як аналіз семантики, вживання заголовків зі складними структурами або використання емоційно заряджених слів у фішингових повідомленнях.

Також, можна провести дослідження ефективності застосування нейролінгвістичних технік виявлення фішингових повідомлень, порівнюючи їх з іншими методами виявлення фішингових атак.

Отже, дослідження використання нейролінгвістичних технік в заголовках фішингових повідомлень є важливим напрямком у сфері кібербезпеки і може допомогти у покращенні захисту користувачів від шкідливих атак.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. Загальна кількість сторінок – 80. Загальна кількість використаних джерел -70.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ПОНЯТТЯ «ФІШИНГ»

1.1. Суть поняття «фішинг» та його механізм

Знаходження фішингових сайтів є складною та часоємною задачею, що включає в себе багато різних факторів та критеріїв. Зараз більшість комерційних та фінансових послуг надається через інтернет, що робить користувачів більш вразливими до викрадання особистої інформації та фішингу. Фішинг передбачає отримання користувачем листа з посиланням на зловмисний веб-сайт, який призначений для збору інформації та персональних даних користувача. Це створює значні збитки для фінансових та кредитних установ.

Історія виникнення фішингу пов'язана з еволюцією Інтернету та зловмисниками, які намагаються шахрайством здобути незаконний доступ до конфіденційної інформації користувачів [1].

У 1990-х роках, коли з'явилися перші онлайн-банки, зловмисники розробили методи шахрайства, використовуючи фішинг-технології. У той час, вони відправляли електронні листи (e-mail) з вимогою підтвердити дані свого банківського акаунту. Лист виглядав так, ніби його надіслала банківська установа, і мав вигляд аутентичного повідомлення від цієї організації. У листі також містилися посилання на фальшивий сайт банку, на якому користувач повинен був ввести свої дані входу до свого банківського акаунту, такі як ім'я користувача і пароль.

Ідея використання фішингу на той час була дуже нова і дещо революційна, оскільки зловмисники використовували довіру людей до банків і інших фінансових установ для того, щоб шахрайсько отримати доступ до їхніх грошей. З тих пір методи фішингу значно вдосконалилися і поширилися на більшість галузей Інтернету, таких як соціальні мережі, електронна пошта, інтернет-магазини і т.д. Зараз фішинг є одним з найпоширеніших видів

шахрайства в Інтернеті, і користувачам потрібно бути дуже обачними і уважними, щоб захистити свої дані і гроші від зловмисників.

Аналіз розсилки спаму та фішингових атак показує наявність деяких шаблонів проведення атаки, але їх важко відразу розпізнати. Знаходження прихованих шаблонів фішингових атак є ефективним методом при розробці програмного забезпечення для запобігання атакам цього типу. Для цього використовуються різні методи збору та аналізу даних, отриманих від попередніх атак, щоб ідентифікувати типові шаблони атак та запобігти майбутнім вторгненням [7].

Основні ознаки фішингу включають:

1. Відправник повідомлення намагається здобути від вас конфіденційну інформацію, таку як пароль, номер кредитної картки, номер соціального страхування або іншу особисту інформацію.

2. Надсилання непередбачуваних повідомлень від імені компаній або організацій, які ви не очікуєте отримати. Наприклад, повідомлення від банку, з яким ви не маєте діла.

3. Швидкий термін відповіді або обмежений час, щоб ви відповіли на повідомлення. Наприклад, повідомлення, що попереджає про блокування вашого акаунту, якщо ви не надішлете свої реєстраційні дані протягом години.

4. Несподіваний запит на оплату чогось, на що ви не розраховували. Наприклад, повідомлення від онлайн-магазину про замовлення товару, який ви не здійснювали.

5. Повідомлення містить посилання на сторінку, яку вам потрібно відвідати, але воно виглядає підозріло або ненадійно.

6. Граматичні помилки або орфографічні помилки в повідомленні.

Якщо ви отримали повідомлення з однією або кількома з перерахованих ознак, будьте обережні та не надавайте конфіденційну інформацію, не відправляйте гроші та не натискайте на посилання в повідомленні, доки не переконаєтеся в його справжності.

За останні 10 років кількість користувачів Інтернету значно збільшилася, що пояснюється віддаленим доступом до мережі за допомогою смартфонів та їх популярністю в різних версіях. Запровадження фінансових послуг через Інтернет, також набуває все більшої популярності серед банків та інших бізнес-організацій. Проведення фінансових операцій в Інтернеті має свої переваги, такі як зменшення забруднення повітря, скорочення трафіку, збереження часу та грошей тощо [8].

У сучасному світі, з розвитком технологій, комп'ютер та смартфон стали невід'ємною частиною життя кожної людини. За допомогою комп'ютера та Інтернету, людина, не виходячи з дому, може легко отримувати різну інформацію, контролювати свої фінанси, виконувати різні операції. Інтернет – це безмежний світ інформації, який дає широкі можливості для спілкування, навчання, організації роботи та відпочинку і в той же час є величезною базою даних, що щодня поповнюється, яка містить цікаву для зловмисників інформацію про користувачів. Існує два основні види загроз, яким можуть наражатися користувачі: технічні та соціальна інженерія. Технічна інженерія являє собою, як правило, роботу різних шкідливих програм, соціальна інженерія-це в першу чергу фішинг-атаки.

Фішинг, у перекладі з англійської, означає ловити рибу, рибалити. Якщо розібратися в суті цього виду шахрайства, воно нагадує саме свого роду рибалку, де здобиччю будуть люди, їх особиста інформація та фінанси. [21].

Фішинг-атаки організовуються так: зловмисники створюють фальшивий сайт, який виглядає абсолютно таким же, як і необхідний сайт банку або будь-якої іншої організації. Наступний етап - залучення потенційних жертв на підроблений сайт, щоб останні, відвідавши сайт-клон, залишили персональні дані: логін, пароль, PIN-код. Використовуючи отримані дані, кібер-шахраї крадуть гроші з рахунків користувачів [1].

Як правило, для того, щоб залучити користувачів на фальшивий сайт, шахраї роблять поштове розсилання електронних повідомлень, які виглядають так, ніби листи надіслані саме з банку чи іншої фінансової організації, тобто

використовується логотип організації, його стиль листа, оформлення та навіть посилання у фішинг-повідомленнях схожі на реальну адресу банку в інтернеті. Крім того, повідомлення може містити ваше ім'я, ніби воно дійсно адресоване вам особисто. У листах шахраїв зазвичай наводиться правдоподібна причина, яка вимагає введення вами на сайті «банку» своїх даних. Зловмисник, який виступає від імені банку або іншого відомого сервісу (наприклад, PayPal або Facebook), вимагає від вас ввести конфіденційні дані нібито з метою перевірки та оновлення інформації про вчений запис. Інший варіант: зловмисник повідомляє, що від імені вашого облікового запису була помічена підозріла активність, і ви повинні "довести", що є власником облікового запису. Таким чином, атакуючий закидає "приманку" у величезне море Інтернет-користувачів, отримує особисту інформацію, добровільно (у більшості випадків) передану користувачем, і використовує її в зловмисних цілях: чи то крадіжка особистих даних, шахрайство з кредитними картками і т.д [9].

Найбільш поширена форма фішингу - масовий фішинг, оскільки в даному виді атаки відсутні конкретні цілі і використовується шахрайський метод соціальної інженерії проти багатьох людей. Таким чином, при даному виді фішингу немає необхідності в зборі інформації, оскільки атакуючий маскує своє повідомлення начебто від представника популярного, всесвітньо-відомого бренду [2].

Фактично, лише мала частина цих людей буде клієнтом банку, авіакомпанії, Інтернет-магазину або користуватиметься соціальними мережами чи будь-якою іншою службою, від імені якої надсилаються листи. Однак, невелика частина все ж таки відкриє надіслане повідомлення, пройде за посиланням або відкриє вкладення.

Сьогодні фішинг виходить за межі інтернет-шахрайства, а підроблені веб-сайти стали лише одним із багатьох його напрямків. Листи, які нібито надіслано з банку, можуть повідомляти користувачам про необхідність зателефонувати за певним номером для вирішення проблем із їхніми банківськими рахунками. Ця техніка називається вішінг (голосовий фішинг).

Зателефонувавши на вказаний номер, користувач заслуховує інструкції автовідповідача, які вказують на необхідність ввести номер свого рахунку та PIN-код. До того ж, вішери можуть самі дзвонити жертвам, переконуючи їх, що вони спілкуються з представниками офіційних організацій, використовуючи фальшиві номери. Зрештою, людину також попросять повідомити її облікові дані [3].

Набирає свої оберти та SMS-фішинг, також відомий як змішинг. Шахраї розсилають повідомлення, що містять посилання на фішинговий сайт, - входячи на нього та вводячи свої особисті дані, жертва аналогічним чином передає їх зловмисникам. У повідомленні також може говорити про необхідність зателефонувати шахраям за певним номером для вирішення проблем, що виникли [4].

Існує кілька простих правил, дотримуючись яких користувачі зможуть убезпечити себе від атак кібер-шахраїв:

1. Необхідно уважно ставитись до повідомлень, у яких вас просять пройти за посиланням та вказати особисті дані. Імовірність того, що банк запитуватиме таку інформацію електронною поштою, надзвичайно мала.

2. Не варто заповнювати сумнівні анкети, отримані електронною поштою. Таку інформацію можна вводити тільки на дійсно перевірених та безпечних сайтах. Також варто переконатися, що його адреса починається з https:// і знайдіть піктограму, схожу на замкнений висячий замок, в правому нижньому куті вікна браузера [20].

3. Якщо у вас виникли найменші підозри щодо повідомлення, яке надійшло з «банку», у вас завжди є можливість зв'язатися безпосередньо з банком та уточнити, чи проводилося розсилання електронних повідомлень тощо.

4. Не проходьте за посиланнями в електронних листах у форматі HTML: кіберзлочинці можуть сховати адресу підробленого сайту у засланні, яке виглядає як справжня електронна адреса банку. Натомість наберіть адресу вручну або скопіюйте посилання в адресний рядок браузера.

5. Варто також контролювати роботу антивірусних програм на вашому ПК, переконайтеся, що антивірусне рішення комп'ютера здатне блокувати перехід на фішингові сайти. Є можливість також встановити інтернет-браузер, оснащений фішинг-фільтром [5].

6. Регулярно перевіряйте стан своїх банківських рахунків та переглядайте банківські виписки, щоб переконатися у відсутності «зайвих» операцій.

7. Слідкуйте за тим, щоб у вас завжди були останні оновлення безпеки.

Таким чином, ми приходимо до висновку, що кібер-шахраї, на сьогоднішній день, мають реальну можливість не тільки заволодіти нашою конфіденційною інформацією, а й викрасти за її допомогою наші заощадження, тому завдання кожного користувача уважно стежити за електронними повідомленнями, а також проходити тільки за перевіреними та безпечними посиланнями та сайтами [6].

Механізм роботи фішингу можна описати наступним чином:

1. Фішер створює підроблену веб-сторінку, яка нагадує оригінальну сторінку, до якої він хоче отримати доступ.

2. Фішер відправляє листи електронної пошти або повідомлення в соціальних мережах з посиланням на підроблену сторінку. Ці повідомлення можуть містити підстави для віри, наприклад, вимогу негайно оновити свій профіль, змінити пароль або перевірити свій банківський рахунок.

3. Користувач, отримавши повідомлення, переходить за посиланням на підроблену сторінку, де йому пропонують ввести свої особисті дані, такі як логін і пароль, номер кредитної картки або інші конфіденційні дані.

4. Коли користувач вводить свої дані, фішер отримує доступ до цієї інформації та може використовувати її для шахрайства.

У певних випадках, фішинг може використовувати соціальну інженерію, тобто техніку впливу на психологію людини з метою отримати доступ до її конфіденційної інформації. Наприклад, фішер може відправити електронний лист, в якому намагається збудити в користувача почуття страху або обурення,

щоб той, здавши себе в оборону, відправив свої особисті дані на підроблену сторінку.

1.2. Види фішингу та життєвий цикл фішингових атак

Існує кілька видів фішингу, основні з яких описані нижче:

1. Електронна пошта (Email) фішинг: зловмисники надсилають електронні листи зі спеціально створеними посиланнями або вкладеннями, які виглядають як легітимні. При кліканні на таке посилання або відкриванні вкладення, користувач може бути перенаправлений на сайт, який виглядає як оригінальний, але фактично належить зловмиснику. На цьому сайті користувач може бути запитано про конфіденційну інформацію, наприклад, ім'я користувача та пароль [11].

Фішинг через електронну пошту є одним з найбільш поширених видів фішингу. У цьому виді атаки зловмисник використовує електронну пошту, щоб виглядати як відправник повідомлення від справжньої компанії або організації, з метою залучити отримувачів до небезпечних дій.

Зазвичай атаки фішингу через електронну пошту вимагають від отримувача відповіді на листа або переходу за посиланням, що міститься у повідомленні. Ці посилання зазвичай призводять до фальшивих веб-сайтів, які імітують справжні веб-сайти, з метою збору конфіденційної інформації.

Іноді відправники фішингових повідомлень можуть використовувати соціальну інженерію, щоб надихнути отримувачів на дії. Наприклад, вони можуть намагатися засмутити або перелякати отримувача, надаючи інформацію про незвичайну або небезпечну активність на їх обліковому записі або на рахунку відповідної компанії, що потребує негайної дії [12].

Щоб уникнути стати жертвою фішингу через електронну пошту, користувачі повинні бути уважні і перевіряти кожне повідомлення, яке вони отримують, перш ніж надавати будь-яку відповідь або інформацію. Також корисно перевіряти адресу електронної пошти відправника і не відкривати посилання, які виглядають підозріло.

2. Сайт-підробка (Phishing websites): зловмисники створюють веб-сайти, які виглядають як оригінальні, з метою отримання конфіденційної інформації. Наприклад, зловмисники можуть створити сайт, який виглядає як банківський сайт, але насправді належить їм, і запропонувати користувачу ввести свої банківські дані.

Сайт-підробка (або "фішинг-сайт") - це один із найбільш поширених видів фішингу, який полягає у створенні підробленої веб-сторінки, яка імітує оригінальний сайт. Цей фішинг зазвичай використовується зловмисниками з метою викрадення особистої інформації користувачів, такої як логіни, паролі, номери кредитних карток і т.д [10].

Фішингери, що стоять за цим видом атаки, намагаються переконати потенційну жертву відвідати їхній сайт-підробку, який зазвичай дуже схожий на оригінальний сайт (наприклад, сайт банку чи платіжної системи). Часто це досягається за допомогою листів електронної пошти, які містять посилання на такий сайт-підробку. Ці листи можуть мати вигляд офіційного повідомлення від організації, що вимагає від користувача оновити свої дані або повторно ввести свій логін та пароль.

Після переходу на сайт-підробку, користувач буде перенаправлений на сторінку, на якій йому буде запропоновано ввести свої логін та пароль, або іншу особисту інформацію. Після того, як користувач введе свої дані, вони будуть відправлені на сервер фішингерів, що дозволить їм зловити ці дані та використати для крадіжки грошей, особистих даних або злочинних цілей.

3. Соціальний фішинг (Social engineering phishing): зловмисники можуть звернутися до користувача з запитом про надання конфіденційної інформації, використовуючи психологічні маніпуляції. Наприклад, зловмисники можуть вигадати історію про те, як вони втратили доступ до свого банківського рахунку і просять користувача надати свої банківські дані для відновлення доступу.

Соціальний фішинг - це вид фішингу, в якому зловмисники використовують соціальну інженерію, щоб отримати доступ до

конфіденційної інформації, такої як паролі, імена користувачів, номери кредитних карток тощо.

Зловмисники можуть використовувати соціальні мережі, електронну пошту, чати або будь-який інший інтернет-канал, щоб вступити в довіру з потенційними жертвами та отримати від них конфіденційну інформацію. Наприклад, зловмисники можуть надіслати листи від імені банків або інших сервісів з проханням оновити свої особисті дані або паролі. У деяких випадках, зловмисники можуть використовувати соціальну інженерію, щоб отримати доступ до фізичних місць, таких як офіси або центри обробки даних [13].

Ознаки соціального фішингу можуть включати в себе неперевірені листи електронної пошти або повідомлення в соціальних мережах з проханням надати особисту інформацію, підозрілі посилання, які ведуть на незнайомі сайти або запити про передачу грошей чи інших цінностей.

Для запобігання соціальному фішингу важливо завжди перевіряти відправника листа електронної пошти або повідомлення в соціальних мережах, перевіряти адресу веб-сайту перед введенням особистої інформації та ніколи не передавати конфіденційну інформацію, якщо ви не переконалися в правомірності запиту.

4. Риболовля в мережі (Spear phishing): це різновид електронної пошти фішингу, в якому зловмисники звертаються до конкретної особи або організації з запитом про надання конфіденційної інформації

Spear phishing є більш вибагливою формою фішингу, де зловмисник використовує персоналізовані інформаційні повідомлення, щоб вигадати дійсний контекст і переконати цільову особу у виконанні шахрайської дії, наприклад, введенні свого паролю або наданні конфіденційної інформації [22].

У відмінність від звичайного фішингу, який спрямований на широку аудиторію, spear phishing є більш вибірковим і зазвичай націлений на конкретну організацію або особу. Зловмисники можуть здійснювати spear phishing через електронну пошту, соціальні мережі, месенджери та інші канали зв'язку.

Одним з прикладів spear phishing може бути імітація електронної пошти від керівництва організації, що містить персоналізований контекст і вимагає від співробітника виконання конкретної дії, наприклад, зміни паролю або надання доступу до конфіденційної інформації. Це може виглядати дуже переконливо, оскільки зловмисники можуть вивчити інформацію про організацію та її співробітників, що дозволяє їм створювати вірогідні імітації легітимних повідомлень [15].

Spear phishing може мати серйозні наслідки для організацій та осіб, які стають його жертвами. Це може призвести до витоку конфіденційної інформації, фінансової шкоди, втрати довіри та інших проблем.

5. Clone-phishing - створення фішингового листа, який містить повідомлення, що виглядає як оригінальне повідомлення, яке вже було відправлено до користувача.

Clone-phishing - це вид соціального фішингу, який використовується зловмисниками для крадіжки особистих даних та розповсюдження шкідливого програмного забезпечення. У цьому випадку зловмисники створюють точну копію легітимного електронного повідомлення, відправленого від імені довіреної компанії чи організації, з якою потенційна жертва співпрацює або взаємодіє [17].

Замість того, щоб відправити легітимне повідомлення, зловмисники модифікують його, додаючи шкідливі вкладення або посилання, які ведуть на фішинговий сайт. Ці вкладення або посилання можуть виглядати так само, як і в оригінальному повідомленні, що змушує жертву довіряти йому та відкривати.

Коли жертва відкриває лінк або завантажує вкладення, вона потрапляє на фішинговий сайт, який може бути точною копією оригінального сайту компанії чи організації. На цьому сайті жертві пропонують ввести свої особисті дані, такі як логін, пароль, реквізити банківської карти тощо, або завантажити і встановити шкідливе програмне забезпечення.

Зловмисники використовують Clone-phishing, щоб отримати доступ до важливих даних та конфіденційної інформації про жертву, таких як логіни, паролі, номери кредитних карток, паспортні дані тощо. Це дозволяє їм здійснювати крадіжки грошей, шахрайства з використанням банківських рахунків та ідентичності [18].

6. Whaling - це форма фішингу, спрямована на високопосадових посадовців, де атаки зазвичай мають на меті отримання конфіденційної інформації або викрадення грошей.

Whaling є одним з видів фішингу, який націлений на високопосадових осіб в компанії, таких як керівники, топ-менеджери, фінансові директори та інші впливові особи. В основі whaling лежить та ж сама ідея, що й у всіх інших видів фішингу – злочинці намагаються вивести цінну інформацію від своєї жертви, щоб здійснити дії, що призведуть до фінансових збитків.

Однією з особливостей whaling є те, що злочинці активно використовують соціальний інженерінг, тобто маніпулювання психологічним станом людей, щоб отримати потрібну інформацію. Найпоширенішим методом проведення whaling є відправка електронної пошти з підробленим адресою від керівника компанії або іншої високопосадової особи. У цьому електронному листі зазвичай міститься запит на надання певної інформації або вказівки на переказ коштів на підроблений банківський рахунок [16].

Для того, щоб whaling був успішним, злочинці активно використовують інформацію, яку вони отримали про своїх жертв, наприклад, про їх ділові зв'язки, структуру компанії та інші дані, які допомагають їм створити переконливу історію. Також вони можуть використовувати інші методи соціального інженерінгу, такі як вимагання швидкої відповіді або створення ситуації, коли жертва повинна вирішити проблему, яка виникла, та надати інформацію, щоб її вирішити.

7. SMS-фішинг - атаки, які відбуваються через текстові повідомлення на мобільний телефон користувача, що містять шкідливі посилання або пропозиції.

SMS-фішинг (також відомий як смішинг) - це метод атаки, який використовує текстові повідомлення для надсилання шахрайських повідомлень з метою шахрайства або шахрайства на телефони користувачів. Цей вид фішингу може містити посилання на веб-сайти, які мімікують легітимні веб-сайти, а також просять введення особистої інформації, такої як номери кредитних карток, паролі і логіни, часто під виглядом "підтвердження даних" або "невдалий вхід на сайт".

Щоб захиститися від SMS-фішингу, користувачі повинні бути обережні при надходженні незапрошених повідомлень та не відкривати посилання, які містяться в них, особливо якщо вони надходять від незнайомих джерел. Також рекомендується встановлювати антивірусні програми на свої мобільні телефони, які можуть допомогти виявити та блокувати підозрілі повідомлення [14].

SMS-фішинг (або Smishing) є одним з видів фішингу, який здійснюється через SMS-повідомлення. Цей вид атаки може використовуватися для отримання конфіденційної інформації, такої як банківські реквізити, паролі, особисті дані та інші види даних.

Схема SMS-фішингу може бути наступною: злочинець надсилає потенційній жертві текстове повідомлення, яке намагається змусити жертву виконати певну дію, таку як відвідування підробленого веб-сайту або відправку відповіді з особистою інформацією. Повідомлення може містити посилання на підроблений веб-сайт або номер телефону, до якого жертва може відправити відповідь зі своїми даними [19].

Іноді SMS-фішинг може використовуватися для зламування аккаунтів. Злочинець може надіслати текстове повідомлення з пропозицією оновити свій пароль або виконати іншу дію, яка може привести до розкриття паролю або іншої конфіденційної інформації. Після того, як злочинець отримає ці дані, він може використовувати їх для отримання доступу до різних сервісів та акаунтів, що належать жертві.

Щоб захиститися від SMS-фішингу, важливо завжди перевіряти автора повідомлення та контент, який воно містить. Не слід відкривати посилання або завантажувати файли з незнайомих джерел, а також передавати конфіденційну інформацію через текстові повідомлення.

8. Vishing - це фішинг, який відбувається через телефонні дзвінки.

Vishing (або голосовий фішинг) - це вид шахрайства, який полягає в тому, що зловмисники використовують телефонні дзвінки для того, щоб здобути особисту інформацію або гроші від потенційних жертв.

Злочинці, які здійснюють vishing, зазвичай використовують спеціальний софт, який дозволяє змінювати номер телефону на екрані телефону жертви. За допомогою підроблених номерів вони можуть пропонувати фальшиві пропозиції або імітувати дзвінок від легітимних організацій, таких як банки, поліція, податкові служби і т.д.

Частіше за все, vishing використовують для отримання фінансової інформації, такої як номери банківських рахунків, пін-коди та інші конфіденційні дані, які можуть бути використані для здійснення шахрайських операцій. Зловмисники також можуть вимагати від жертв переказів грошей або подати підроблені вимоги з оплати [24].

Основною метою vishing є створення надмірної емоційної реакції у жертви, щоб та не змогла розпізнати шахрайство та діяти із потрібною обережністю. Зазвичай, зловмисники намагаються створити невідкладність в операції та використовують такі техніки як загрози або вимагання, щоб викликати жертві страх чи паніку.

Vishing (від англ. voice phishing) - це вид шахрайства, при якому атакуючий намагається отримати конфіденційну інформацію (таку як банківські реквізити, паролі, номери соціального страхування та ін.) від жертви за допомогою голосового зв’язку, зазвичай за допомогою телефонного дзвінка.

Під час атаки використовується соціальна інженерія, щоб переконати жертву, що вона розмовляє з представником довіреної організації (банку,

компанії зі зв'язку, податкової служби тощо). Атакуючий зазвичай виступає під виглядом співробітника організації, який має доступ до конфіденційної інформації або може допомогти вирішити проблему з аккаунтом або операціями [23].

За допомогою маніпулювання жертвою, атакуючий може надіслати фішингові повідомлення, в яких надихається довіра, використовуючи ім’я компанії та інформацію про аккаунт жертви.

Наприклад, атакуючий може повідомити жертві, що її банківський аккаунт або кредитна картка були скомпрометовані, і запросити відновити доступ до аккаунту, надавши особисту інформацію або змінивши пароль через вказані на дзвінок номери.

1.3. Мотивація та мета фішингових атак

Метою фішингових атак є зазвичай зловживання довіри та наївності людей з метою здобуття конфіденційної інформації або фінансової вигоди.

Наприклад, фішер може використовувати отриману за допомогою фішингу інформацію, щоб доступитися до банківського рахунку або іншої конфіденційної інформації. Також фішер може використовувати зловмисні посилання, щоб отримати доступ до комп'ютера або мобільного пристрою, і використовувати його як засіб для злочинних дій [25].

Мотивації фішингових атак можуть бути різними, включаючи фінансовий зиск, крадіжку конфіденційної інформації, викрадення особистої інформації, шпигунство, розвідку або вірусні атаки на комп'ютерні системи. Одним з головних мотивів є фінансовий зиск, оскільки фішери можуть продавати отриману інформацію на чорному ринку або використовувати її для крадіжки грошей.

У більшості випадків фішери мають за мету використати незахищені або необізнані компанії або індивідуальних користувачів, щоб зловити їхні дані. Тому важливо бути обережним та використовувати заходи безпеки для захисту своєї особистої інформації та фінансових ресурсів.

Головною мотивацією фішингових атак є фінансовий зиск. Атаки проводяться з метою зламування доступу до банківських рахунків, крадіжки особистої інформації, паролів, номерів кредитних карток та інших фінансових даних. Ці дані можуть бути продані на чорному ринку або використані для здійснення шахрайства.

Іншими мотиваціями можуть бути здійснення шпигунства, крадіжка корпоративної інформації, викрадення особистих даних для здійснення шахрайства або шантажування. Також може бути мотивацією політична або кібершпигунська діяльність.

У деяких випадках, фішингові атаки можуть бути спрямовані на споживачів з метою поширення вірусів, програм-шпигунів або інших шкідливих програм [26].

Нарешті, можливі й інші мотивації, такі як військові або терористичні дії, або навіть просто бажання порушити стабільність та зруйнувати довіру в інтернет-комунікації.

Фішингові атаки - це спроби шахраїв і кіберзлочинців отримати конфіденційну інформацію від користувачів, використовуючи різні методи і техніки. Ці атаки можуть бути спрямовані на індивідуальних користувачів, компанії або державні установи.

Одним з найпоширеніших видів фішингу є електронна пошта. Наприклад, зловмисники можуть відправити електронного листа, який маскується під лист від банку, сервісу або компанії з проханням підтвердити свої особисті дані, пароль або іншу конфіденційну інформацію. Лист може містити посилання на підроблений сайт, який нагадує оригінальний веб-ресурс. Коли користувач переходить за посиланням і вводить свої дані, зловмисники отримують доступ до цієї інформації [27].

Іншим типом фішингу є соціальний фішинг. У цьому випадку зловмисники використовують соціальні інженерні методи, щоб отримати інформацію про своїх жертв і використовувати її для атаки [31]. Наприклад, зловмисники можуть використовувати соціальні мережі, форуми, чати та інші

онлайн-канали для збору інформації про своїх жертв, таку як ім'я, дата народження, місце роботи і т.д. Ця інформація може використовуватися для переконливого фішингу, такого як відправлення електронного листа від колеги або руководства компанії з проханням надати конфіденційну інформацію або переказати гроші.

Головною метою фішингових атак є здобуття конфіденційної інформації, такої як паролі, номери кредитних карток, особисті дані, доступ до банківських рахунків та іншої чутливої інформації. Злочинці можуть використовувати отриману інформацію для власних користей, таких як використання банківських рахунків для здійснення несанкціонованих транзакцій, крадіжка особистості, розсилка спаму та інші злочинні дії [29].

Крім того, фішингові атаки можуть бути спрямовані на отримання доступу до системи або мережі організації. Це може стати можливим через злам пароля або здобуття даних для входу в мережу. Злочинці можуть використовувати цей доступ для крадіжки корпоративної інформації, вимагати викуп у разі зараження комп'ютерної системи вірусом-вимагачем, використовувати систему для злочинних дій або знищення даних.

Також, фішинг може бути використаний як засіб для поширення шкідливого програмного забезпечення (наприклад, вірусів, троянів, червів тощо) на комп'ютер або мобільний пристрій користувача. Шкідливе ПЗ може бути використане для здійснення шпигунської діяльності, крадіжки інформації, перехоплення веб-камери та мікрофону пристрою і т.д.

Отже, мета фішингових атак полягає в здобутті користувацької інформації, доступу до комп'ютерних систем та мереж, а також у поширенні шкідливого ПЗ для подальшої крадіжки даних та інших злочинних дій.

Суть фішингових атак полягає в тому, що зловмисники намагаються отримати неправомірний доступ до конфіденційної інформації, такої як паролі, номери кредитних карток, особисті дані, інші цінні дані або гроші. Вони роблять це шляхом створення виду, що вони є надійними джерелами, такими як відомі компанії, урядові органи або інші інституції, а потім

вимагають від жертв надати їм цю конфіденційну інформацію. Зазвичай це відбувається через електронну пошту, соціальні мережі, текстові повідомлення, телефонні дзвінки або інші засоби зв'язку [32].

Основна мета фішингових атак полягає в тому, щоб обдурити жертву і отримати доступ до її конфіденційної інформації або виконати певні дії, які можуть призвести до втрати грошей або поширення вірусів та іншого шкідливого програмного забезпечення. Зловмисники можуть використовувати зібрану інформацію для крадіжки грошей, використання кредитних карток, здійснення шахрайських дій або шпигування.

Усі фішингові атаки спрямовані на здобуття конфіденційної інформації жертви, тому дуже важливо бути обережним і не надавати ніякої особистої інформації, якщо ви не впевнені в достовірності джерела запиту.

Зміст фішингових атак може варіюватися в залежності від їхньої форми і мети. Однак деякі загальні характеристики атак можуть включати:

1. Перехоплення особистої інформації: Фішингові атаки можуть бути спрямовані на отримання особистої інформації, такої як ім'я, адреса, номер соціального страхування, банківські реквізити тощо. Цю інформацію злочинці можуть використовувати для крадіжки особистих коштів, зловживанням ідентичністю та інших шахрайств [28].

2. Крадіжка грошей: Деякі фішингові атаки можуть бути спрямовані на крадіжку грошей. Наприклад, атакувачі можуть надіслати електронного листа або текстового повідомлення, який просить потенційну жертву негайно переказати гроші на певний банківський рахунок.

3. Встановлення шкідливого ПЗ: Фішингові атаки також можуть використовуватися для встановлення шкідливого програмного забезпечення на комп'ютері або мобільному пристрої. Це може дозволити злочинцям отримати доступ до конфіденційної інформації, такої як паролі, номери кредитних карток, банківські реквізити тощо [33].

4. Підробка ідентичності: Фішингові атаки можуть бути спрямовані на підробку ідентичності. Наприклад, атакувачі можуть надіслати електронного

листа від імені банку або іншої організації і просити потенційну жертву надати особисту інформацію.

З огляду на різноманітність методів та форм фішингових атак, можна стверджувати, що мета та мотивація злочинців можуть варіюватися. Однак, загалом, основною метою є отримання конфіденційної інформації, такої як паролі, номери банківських карток, особисті дані тощо, для подальшого використання їх у злочинних цілях, таких як крадіжка грошей або крадіжка ідентичності [30].

Крім того, фішингові атаки можуть бути спрямовані на розповсюдження шкідливих програмного забезпечення, яке може використовуватися для злому комп'ютера або для збору конфіденційної інформації без відома користувача. Такі атаки можуть бути використані для збирання конфіденційної інформації з великої кількості користувачів, що дозволяє злочинцям використовувати отриману інформацію для здійснення масштабних злочинних дій.

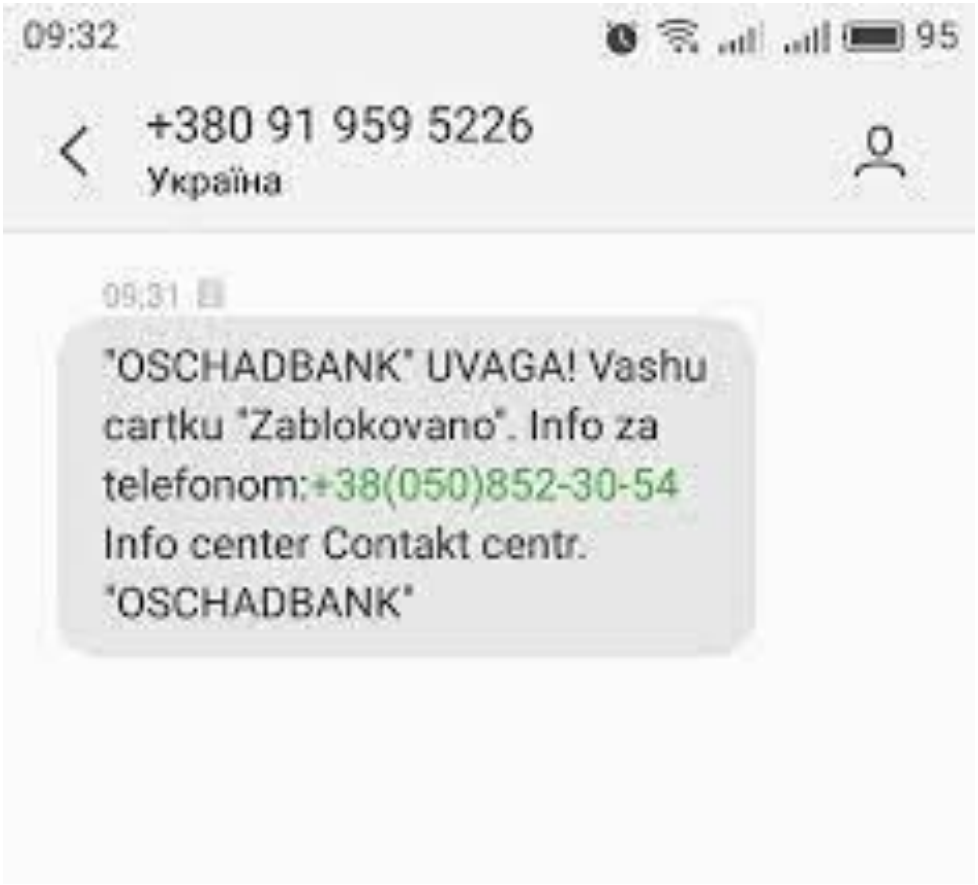
Таким чином, з метою захисту від фішингових атак, користувачам необхідно бути обережними та уважними, перевіряти автентичність відправника електронної пошти або повідомлення, уникаючи надання конфіденційної інформації, та використовувати заходи безпеки, такі як антивірусне програмне забезпечення та двофакторна автентифікація, щоб знизити ризик становлення жертвою фішингових атак.

РОЗДІЛ 2. МЕТОДИКА ДОСЛІДЖЕННЯ ФІШИНГОВИХ ПОВІДОМЛЕНЬ

2.1. Аналіз фішингових повідомлень та їх основних характеристик

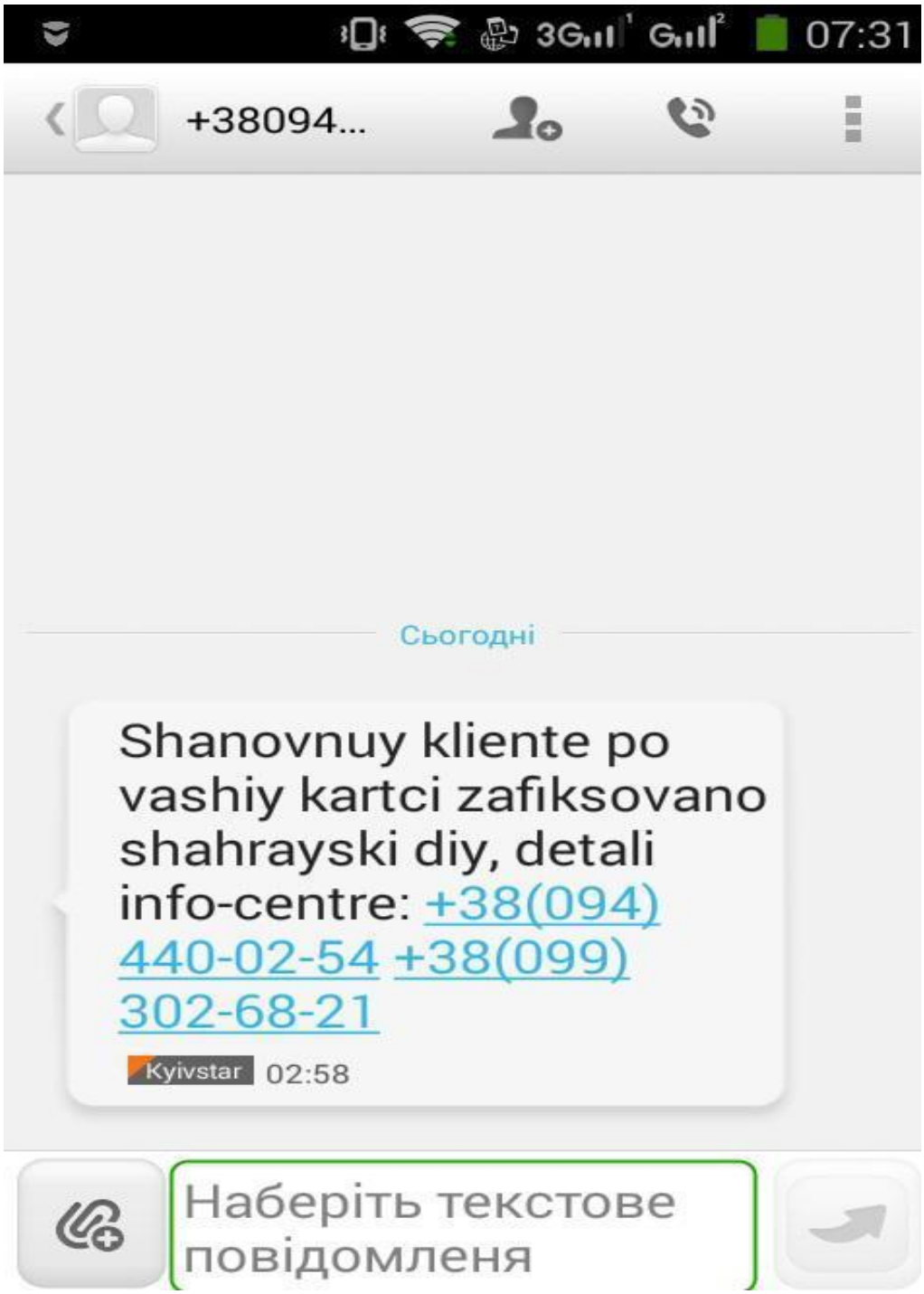
Фішингові повідомлення можуть містити різноманітні ознаки, які можуть допомогти виявити їх як підроблені.

1. Відправник: Фішингові повідомлення можуть мати вигляд, що вони надійшли від відомої організації або особи, але насправді вони можуть бути надіслані з іншої електронної адреси або з країни, що не має відношення до відомої організації. Тому, користувачі мають перевіряти електронну адресу відправника та порівнювати її з офіційними електронними адресами відомих організацій [34].



Мал. 2.1.1. –Приклад фішингового повідомлення

В даному випадку,фішингове повідомлення має вигляд, ніби воно надійшло від «ОщадБанк», але воно відправлене з незнайомого номеру, якими банки не користуються



Мал. 2.1.2. –Приклад фішингового повідомлення

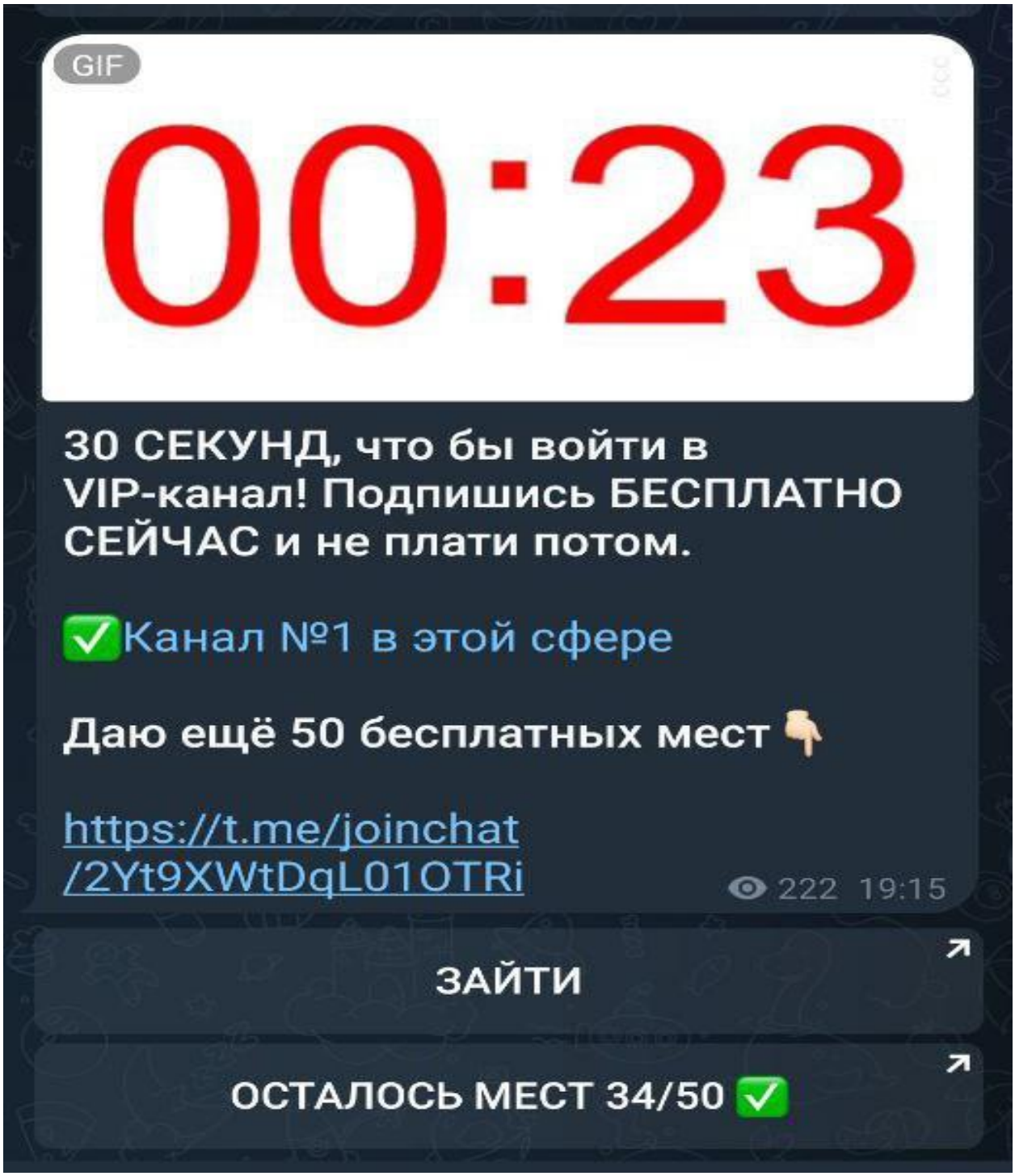
В даному випадку,фішингове повідомлення має вигляд, ніби воно надійшло від якогось офіційного банку, оскільки вміст повідомлення про те, що на карті зафіксовані шахрайські дії, але воно відправлене з незнайомого номеру і тому не може навіть розглядатися, що таке відправив банк [35].

2. Наголошення на терміновості: Фішингові повідомлення можуть містити наголошення на терміновості або негайному виконанні дій.

Зловмисники намагаються використати страх або негайну необхідність, щоб змусити користувачів діяти швидко та необдумано.

Мал. 2.1.3. –Приклад фішингового повідомлення

В даному випадку, фішингове повідомлення містить принцип терміновості, це можна побачити по величезному шрифту червоного кольору, також наявна кількість знаків оклику і такі фрази як «ОФІЦІЙНО», «ВАЖЛИВО».



Мал. 2.1.4. –Приклад фішингового повідомлення

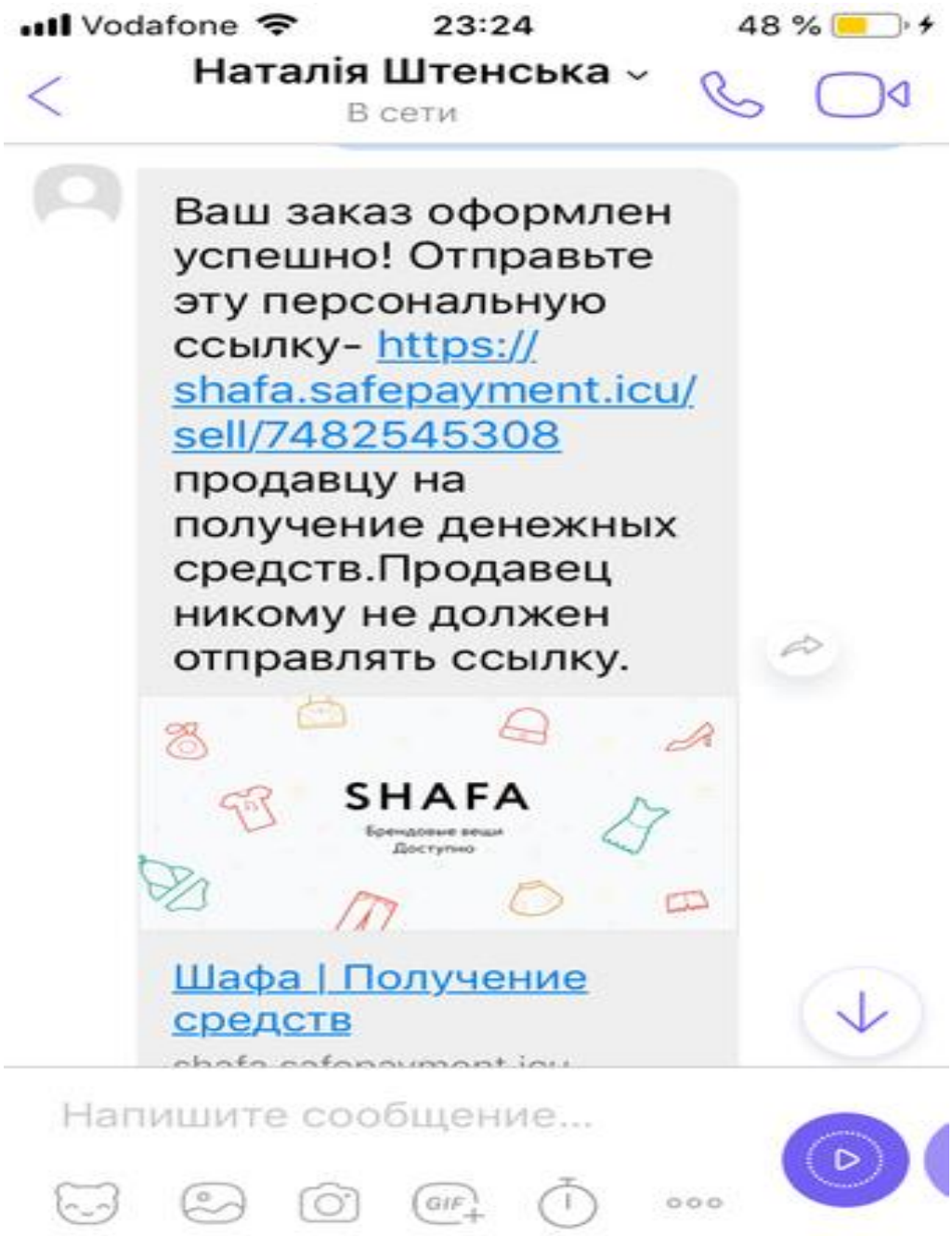
Дане фішингове повідомлення починається з фрази «30 СЕКУНД». Це зроблено для підвищення уваги до цього повідомлення і підштовхує до необдуманих і імпульсивних дій за допомогою ефекту терміновості.

Мал. 2.1.5. –Приклад фішингового повідомлення

В цьому фішинговому повідомленні принцип терміновості і важливості полягає в тому, що основна інформація виділяється знаками оклику і великим шрифтом.

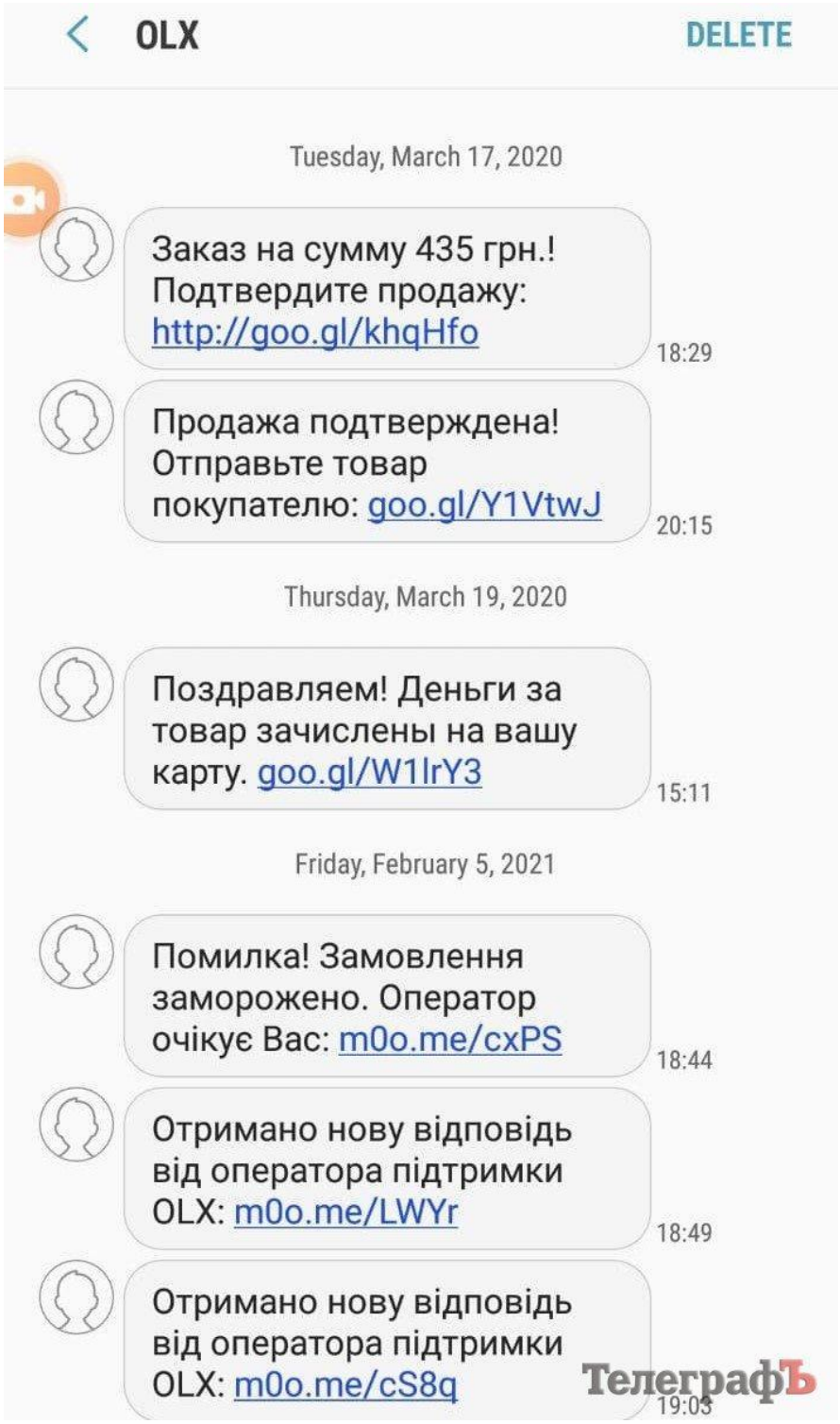
3. Незвичайний контент: Фішингові повідомлення можуть містити незвичайний контент, такий як помилки в тексті, дивні символи або відсутність звичайних елементів, які зазвичай містяться в легітимних повідомленнях [36].

4. Посилання та вкладення: Фішингові повідомлення можуть містити посилання на підроблені сторінки або вкладення, які містять шкідливі програми. Користувачі мають перевіряти посилання та вкладення, щоб переконатися, що вони ведуть до легітимних сторінок або файлів.



Мал. 2.1.6. –Приклад фішингового повідомлення

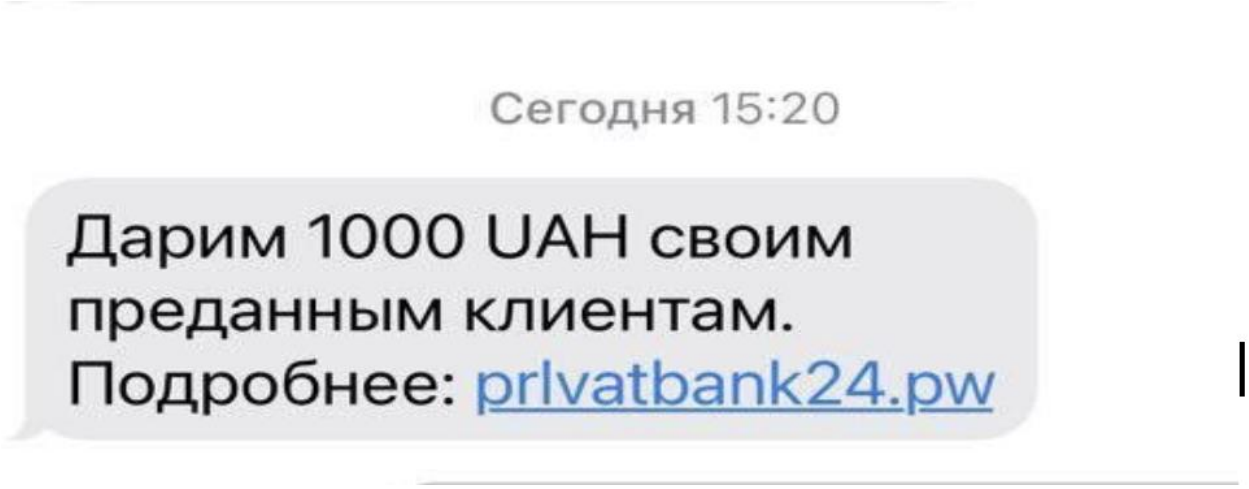
OLX як і Shafa є однією з найбільших онлайн-платформ для купівлі та продажу товарів в Україні. Жаль, але існують шахраї, які використовують цю платформу, щоб шахрайським шляхом заробляти гроші. Один з найпоширеніших шахрайських методів - це розміщення шахрайських посилань на OLX [37].



Мал. 2.1.7. –Приклад фішингового повідомлення

Шахраї можуть розміщувати оголошення про продаж товарів або послуг і надавати посилання на зовнішні сайти для оплати. Посилання можуть вести на сайти, що пропонують фальшиві послуги або товари, або ж на сайти з фішинговими формами для збору конфіденційної інформації.

5. Вигляд повідомлення. Фішингові повідомлення зазвичай мають офіційний вигляд та логотип відомих організацій, таких як банки, соціальні мережі, електронні платіжні системи тощо. Це дозволяє зловмисникам переконати користувачів в тому, що повідомлення є легітимним.



Мал. 2.1.8. –Приклад фішингового повідомлення

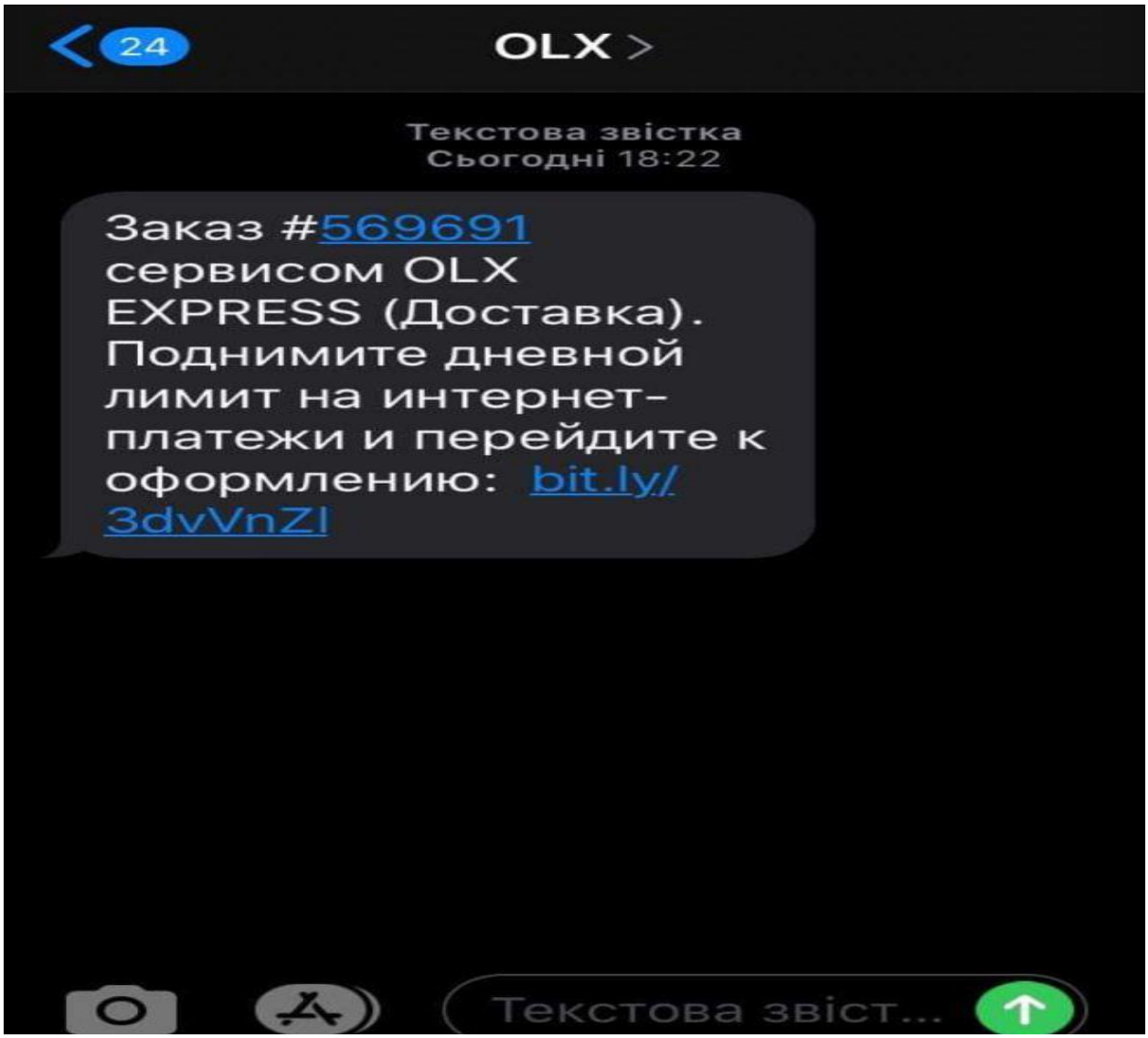
Фішери, які стоять за такими повідомленнями, намагаються виглядати якомога більш правдоподібно, використовуючи деталі, що відповідають оригінальному дизайну та формату повідомлень. Вони можуть включати логотипи, кольорову схему та шрифти, які відповідають оригінальному стилю бренду [38].

Фішингові повідомлення часто мають офіційний вигляд та логотип відомих організацій, щоб зманіпулювати отримувачами та спонукати їх до виконання певних дій, таких як надання конфіденційної інформації або виконання платежу.

Одним з найпоширеніших видів фішингових повідомлень є повідомлення про підтвердження входу до облікового запису, що надходять від фальшивих соціальних мереж, банків та інших сервісів. Вони можуть звертатися до отримувачів з проханням ввести свої дані для підтвердження або перевірки облікового запису [40]. Фішери використовують цю інформацію для отримання доступу до облікового запису та інших конфіденційних даних.

6. Вміст повідомлення. Фішингові повідомлення часто містять тискливі або залякуючі висловлювання, які намагаються спонукати користувачів до

виконання певних дій. Наприклад, повідомлення можуть містити прохання оновити свої дані на підробленій сторінці або прохання негайно змінити свій пароль, інакше будуть серйозні наслідки.



Мал. 2.1.9. –Приклад фішингового повідомлення

Фішери намагаються викликати у користувачів почуття небезпеки, тривоги та терміновості, щоб прискорити процес прийняття рішення та викликати бажання діяти швидко. Це може включати загрози втрати доступу до облікового запису, блокування або скасування послуг, фінансових штрафів та інших наслідків, які можуть виглядати дуже реальними та серйозними [39].

Однак, важливо пам'ятати, що відомі організації, такі як банки або інші сервіси, не будуть надсилати тискливі або залякуючі повідомлення, щоб

змусити користувачів надавати конфіденційну інформацію або виконувати платежі.

7. Посилання. Фішингові повідомлення містять посилання на підроблені веб-сайти, які нагадують офіційні веб-сайти відомих організацій. Зловмисники намагаються переконати користувачів перейти за цими посиланнями та ввести свої конфіденційні дані.

8. Спосіб доставки повідомлення. Фішингові повідомлення можуть бути доставлені за допомогою електронної пошти.

9. Підроблені логотипи та графічні елементи: фішингові повідомлення можуть містити підроблені логотипи та графічні елементи відомих компаній або брендів, щоб здатися більш вірогідними [43].

10. Надмірний тиск: фішингові повідомлення можуть містити твердження, що негайно потрібно виконати якусь дію, наприклад, змінити пароль або оновити інформацію в своєму аккаунті. Зловмисники можуть навіть погрожувати користувачеві, що його аккаунт буде заблоковано, якщо він не виконає певні дії.

Отже, аналіз фішингових повідомлень є важливою складовою заходів з кібербезпеки, оскільки дозволяє ідентифікувати та виявляти шахраїв, які намагаються отримати доступ до конфіденційної інформації користувачів.

2.2. Опис нейролінгвістичних технік та їх вплив на людський мозок

Нейролінгвістичні техніки (НЛП) - це набір психотерапевтичних методів, що використовують мову та поведінку для досягнення змін у психіці та поведінці людини. Ці техніки ґрунтуються на взаємозв'язку між мовою, поведінкою та психологічними процесами в мозку [44].

Нейролінгвістичне програмування (НЛП) виникло ще в другій половині минулого століття в США як "нове вчення про можливості в комунікаціях", але проблематика його статусу, наукова специфіка та сфера застосування і досі є актуальними проблемами для вивчення НЛП цілою спільнотою психологів, спеціалістами різних сфер діяльності та аматорами (наприклад, пікаперами).

Полеміка навколо правильності методів НЛП, і навіть його естетичності - це з головних " гарячих точок " як сучасної психології, а й релігії, естетиці - культури загалом. Інтерес до цих проблем не згасає вже близько півстоліття.

Важливо підкреслити, що сучасна психологія (у тому числі - психологія відносин, що розглядається лише в рамках пікапа, але в класифікаторі академічних дисциплін має назву "сімейна психологія") разом із НЛП, їх спільні досягнення, накопичені працею як вчених-професіоналів (Р.А. Бендлер, Дж. Гріндер), так і любителів лягли в основу сучасних методик ведення ділових переговорів, комунікацій у бізнесі, маркетингу та просто міжособистісних відносин [42].

Мета даної роботи - правильно визначити теоретичні положення концепції нейролінгвістичного програмування в історичному контексті та на сучасному етапі розвитку, ідентифікувати найбільш актуальні проблеми теми та подати наявні альтернативні шляхи вирішення цих проблем і, нарешті, якщо це можливо, визначити місце цієї концепції у структурі сучасної психології.

Завдання реферату зводяться до того що, щоб досліджувати теоретичні (і деяких випадках - практичні) положення концепції нейролінгвістичного програмування, визначити специфічність його принципів і положень, виявити хронологічну структуру НЛП, виражену через переосмислення окремих положень, до першого десятиліття XXI століття, і навіть визначити становище НЛП у психології.

Нейролінгвістичне програмування – це спосіб (або навіть мова) опису суб'єктивного досвіду людини, її розумових, поведінкових та комунікативних патернів. НЛП допомагає зрозуміти, як сприймають світ навколо, як вони спілкуються друг з одним, описує стратегії поведінки.

Вже напрацьовані стратегії НЛП у різних галузях можуть бути корисними стосовно контексту областей терапії та бізнесу. Можливість відокремлення структури навички дозволяє переносити стратегії між областями у вигляді моделювання. Навчання НЛП як дисципліни, що має моделювання як функцію, дозволяє принагідно отримати розвиток

комунікативних навичок, багатопозиційного сприйняття світу, поведінкової гнучкості та зробити значне особистісне зростання [45].

Незважаючи на популярність, НЛП продовжує бути суперечливим, зокрема, у терапії та бізнесі. Навіть після трьох десятиліть існування НЛП не має наукового обґрунтування, що теж є спірним, оскільки теоретична база спирається на досвідчені дослідження поведінкових та комунікативних стратегій конкретних людей (М. Еріксона, У. Діснея).

Грунтуючись на мовних патернах та сигналах тіла, зібраних експертними методами під час спостережень кількох психотерапевтів, практикуючі нейролінгвістичне програмування вважають, що наша суб'єктивна реальність визначає переконання, сприйняття та поведінку, і, отже, можливо проводити зміни поведінки, трансформувати переконання та лікувати травми. Техніки, вироблені з урахуванням даних спостережень, своїми творцями описувалися як " терапевтична магія " , тоді як саме НЛП описувалося як " дослідження структури суб'єктивного досвіду " . Ці твердження ґрунтуються на принципі, що будь-яка поведінка (чи то досконала чи дисфункціональна) не проявляється випадково, але має структуру, яку можливо зрозуміти [41].

НЛП застосовується в цілій низці сфер діяльності: продажу, психотерапія, комунікація, освіта, коучинг, спорт, управління бізнесом, міжособистісні відносини, а також у духовних рухах та спокусі. НЛП звинувачують у суперечливості, а також іноді критикують за недоведеність та псевдонауковість ті, хто стежить за випадками шахрайства, що містять перебільшення заяв та неетичних практик. Як серед практиків, так і серед скептично налаштованих людей існує значна різноманітність думок щодо того, що слід вважати НЛП, а що не слід.

Ось кілька типів НЛП-технік та їх вплив на людський мозок:

1. Моделювання: НЛП використовує техніку моделювання, щоб вивчити та імітувати поведінку та стратегії успіху інших людей. Це може включати вивчення мовного стилю, тіла, поз, жестів та інших аспектів поведінки.

2. Переформулювання: НЛП використовує техніку переформулювання для зміни сприйняття та розуміння ситуації. Це може допомогти людині змінити свій погляд на проблему та знайти нові способи розв'язання.

3. Калібрування: Техніка калібрування в НЛП включає в себе спостереження та аналіз змін в психологічному стані людини, таких як дихання, тон мови, рухи та інші фізичні ознаки. Це може допомогти розпізнати емоції та переконання людини та допомогти виявити можливості для змін [47].

4. Анкерування: Техніка анкерування НЛП полягає в тому, що певний стимул (наприклад, слово, звук, дотик) стає тригером для певної емоції. Це може допомогти людині управляти своїми емоціями та знайти способи досягнення бажаних результатів.

Сучасне уявлення про НЛП не обмежується лише цими пресупозиціями. Часто використовуються інші принципи, серед яких:

▪ ***Люди мають у своєму розпорядженні всі ресурси, необхідні для успіху.*** Стверджується, що суб'єкту корисно вірити в те, що він має все необхідне для проведення зміни, оскільки, якщо це дійсно так, це допоможе йому досягти результатів.

▪ ***Структура важливіша, ніж зміст***. Якщо дві проблеми схожа психологічна структура, до них, мабуть, можна використовувати аналогічний підхід. Часто саме структура проблеми (як відбувається її фіксація, які види переконань її підкріплюють, як клієнт думає про неї) важлива найбільше, а чи не деталі ситуації, у неї вплетеної. Цей поділ форми та змісту також використовується і в сучасній західній психіатрії (у числі піонерів даного підходу Карл Ясперс та Курт Шнайдер) [49].

▪ ***Якщо завжди робити те, що ти завжди робив, ти завжди отримуватимеш те, що завжди отримував, або в іншому формулюванні***: "Якщо ти робиш щось, що не працює, спробуй зробити щось інше" (Бендлер). НЛП розглядає завдання як багаті теми на дослідження, і принцип постійного пошуку нових підходів притаманний всієї його методології.

▪ ***Принцип утилізації або "використовуй все, що працює***". Принцип, запозичений у Мілтона Еріксона, відомого за вміння позитивно використати сформований клієнтом суб'єктивний образ своїх дефектів чи обмежень. НЛП працює за принципом, якщо щось допомагає, це можна використовувати.

▪ ***Не існує опірних клієнтів, є лише недостатньо кваліфіковані терапевти.*** Опір також має комунікативний сенс. Воно надає інформацію про внутрішній світ клієнта, і часто слід брати до уваги і досліджувати як цінну інформацію про психіці клієнта. В даному підході НЛП-психотерапія відрізняється від деяких інших психотерапевтичних напрямків, в яких опір розглядається як фактор, з яким слід боротися, з основою думки, що "пацієнт просто не готовий до змін". У НЛП ж опір вважається несвідомим повідомленням, що говорить про те, що обрано неправильний напрямок роботи і в якому слід рухатися [46].

▪ ***Важливість результату (ефективності), а не механічної процедури (ефективності)***: якщо щось можна зробити за десять хвилин, не слід витрачати на це годину. НЛП виступає на користь короткострокової терапії, тобто в ньому вважається, що у багатьох випадках все, що необхідно, щоб допомогти клієнту, це змінити те, як він інтерпретує ситуацію. Під завданням психотерапії розуміється ефективне дослідження того, як людина суб'єктивно розуміє, представляє і переживає свою проблему і як можливо допомогти їм досягти своєї мети, змінивши її розуміння про все це.

▪ ***Тіло і розум – елементи єдиної системи***. У НЛП враховується те, що організм (тілесність) впливає психіку, а психіка впливає тіло. Те, як людина ходить, рухається, дихає, його м'язові затискачі - це, як впливає на нього його психоемоційний стан.

▪ ***НЛП ґрунтується на сенсорному спостереженні***. Спочатку як дані визначення патернів і структур, які у собі та інших людей, НЛП враховує лише те, що можна особисто сприйняти у вигляді сенсорики (зовнішньої чи внутрішньої). Сприйняття вважається єдиною основою отримання актуальної інформації про світі. Такі ж явища, як "читання думок", або абстрактне

припущення, засноване на минулому, а не поточному досвіді (наприклад, індивідуальні чи культурні стереотипи про те, що має бути), і рівняння на "апріорне знання" (тобто уявлення про те , яким світ має бути) у НЛП уникаються. Тим не менш, логічні міркування та постановка гіпотез можуть використовуватися як інструмент для визначення можливих патернів та напрямів дослідження, проте вони завжди потребують перевірки через сенсорне спостереження [48].

▪ ***Усвідомлення сенсу не завжди необхідне***. На відміну від традиційних психотерапевтичних шкіл, ефективна зміна чи навчання на несвідомому рівні важливіші, ніж свідоме розуміння. Відповідно до НЛП, зміна який завжди потребує інтерпретації чи аналізу, важливо лише зміна карти переконань у світі і себе, у якому раніше недоступне стає можливим.

▪ ***Жоден патерн не слід розглядати як універсальний***. У НЛП мається на увазі, що структура, чи організація, особистого досвіду глибоко індивідуальна. Тобто ця структура унікальним чином розвивається протягом індивідуального життя людини під впливом різних внутрішніх та зовнішніх факторів. Тому жоден із методів НЛП не слід поширювати на всіх людей.

2.3. Розгляд найпоширеніших нейролінгвістичних технік, що використовуються в заголовках фішингових повідомлень

Підхід до "проблеми" та її "вирішення" в нейролінгвістичному програмуванні відрізняється від використовуваного в класичній клінічній психіатрії. Модель НЛП-психотерапії ґрунтується на допомозі клієнтам у подоланні швидше суб'єктивно сприйманих проблем, а не об'єктивно сприйманих, тобто тих проблем, які клієнт сам сприймає або може сприйняти, а не тих, які, на думку оточуючих, можуть бути. НЛП-психотерапії не властивий нозологічний підхід, і вона уникає опису певних психічних станів у вигляді "захворювань"; психотерапія НЛП зазвичай не будується на основі критеріїв захворювання, описаних у "Діагностичному та статистичному довіднику психічних розладів" (DSM), швидше вона будується навколо того,

що сам суб'єкт бажає виправити у своєму житті. Нозологічна думка в НЛП може розглядатися лише як одна з можливих, але сама терапія орієнтована на індивідуальний підхід [50].

Метамодель - це модель мови, яка визначає ті лінгвістичні патерни, які роблять неясним сенс комунікації, завдяки процесам спотворення, недогляду та узагальнення, і визначає конкретні питання, які мають на меті прояснити і поставити під сумнів неточності мови, щоб відновити їх зв'язок із сенсорним досвідом глибинною структурою. Метамодель вперше була описана в книзі "Структура Магії" Річарда Бендлера та Джона Гріндера та розроблена на основі трансформаційної лінгвістики Ноама Хомського. "Мілтон-модель" протилежна метамоделі та описує свідоме застосування метамодельних порушень та мовленнєвих пресуппозицій для формування трансу [51].

Метамодель описує перетворення глибинної структури людського досвіду на поверхневу структуру, що виражається в мові. Досвід зазнає таких порушень як видалення (опущення), спотворення і узагальнення (генералізація). Паттерни метамоделі - це шаблони, якими описуються порушення метамоделі, визначається наявність тієї чи іншої порушення у мові, і якими формується метамодельное питання прояснення кожного порушення.

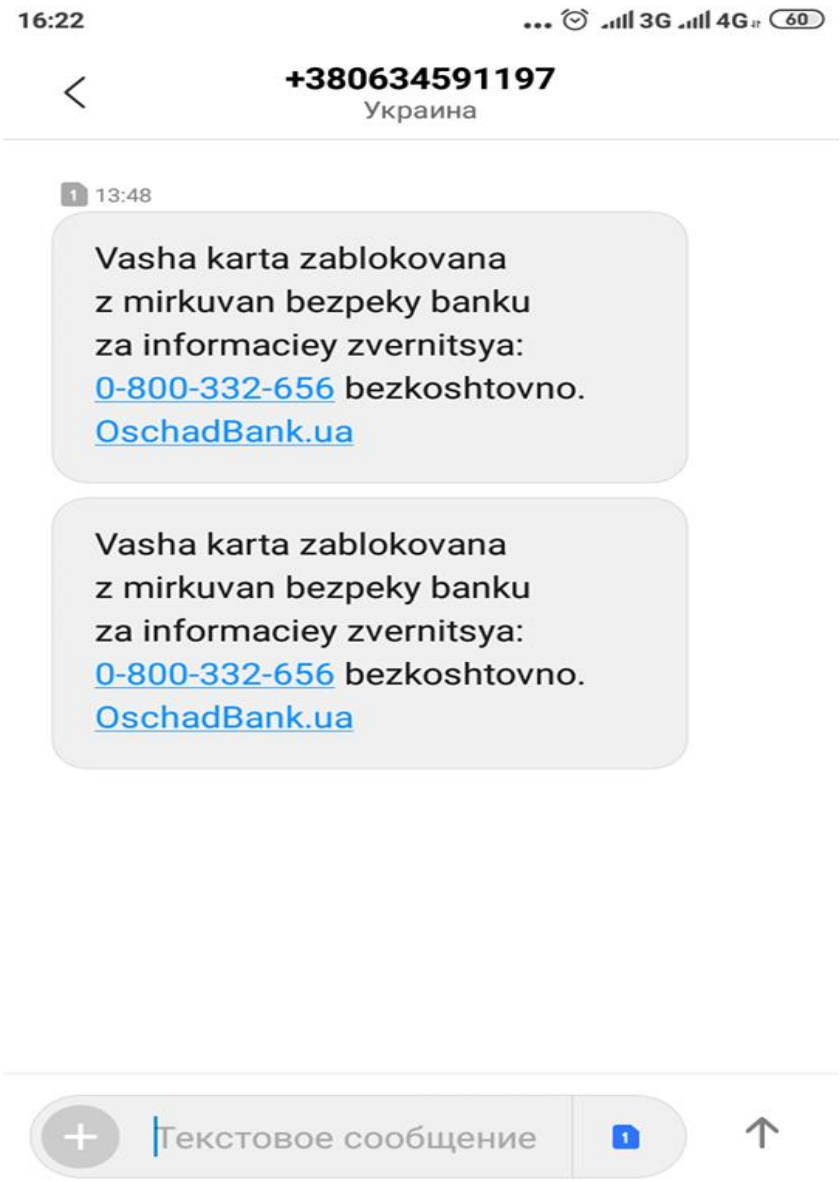
Таблиця 2.3.1. Метамодельні порушення

Видалення	
Відсутність вказівного індексу	Також називається втрата іменного покажчика, втрата референтного індексу. Зразок: кажуть, зима буде холодною.
Виключення	
Порівняння	Застосовується порівняльне прикметник, але упускається, із чим саме проводиться порівняння. Зразок: Жити стало краще, жити

	стало веселіше. Запитання наприклад: Краще / веселіше порівняно з чим?
Судження	Упускається хтось автор судження, і за яким критерієм воно зроблено. Приклад: Я - егоїст! Запитання наприклад: Хто це сказав? Хто автор судження?
Узагальнення	
Неконкретне дієслово	Неспецифічне дієслово
Неконкретний іменник	Неспецифічний іменник
Спотворення	
Номіналізація	Дієслово, що описує процес, що протікає, перетворений на іменник. Кожна номіналізація містить у собі пару втрачених іменників та неконкретне дієслово.
Реверсивний референт	Зразок: Ти мене засмучуєш. Запитання: Як ти робиш себе засмученим?

Нейролінгвістичні техніки можуть використовуватись шахраями в заголовках фішингових повідомлень, щоб привернути увагу користувачів та змусити їх виконати певні дії. Деякі з найпоширеніших таких технік включають:

1. Звернення до емоцій: Шахраї можуть використовувати заголовки з підвищеною емоційною зарядкою, щоб привернути увагу користувачів. Наприклад, "Ваш акаунт буде заблоковано!" або "Ваші кошти у небезпеці!".



Мал. 2.3.1. –Приклад фішингового повідомлення

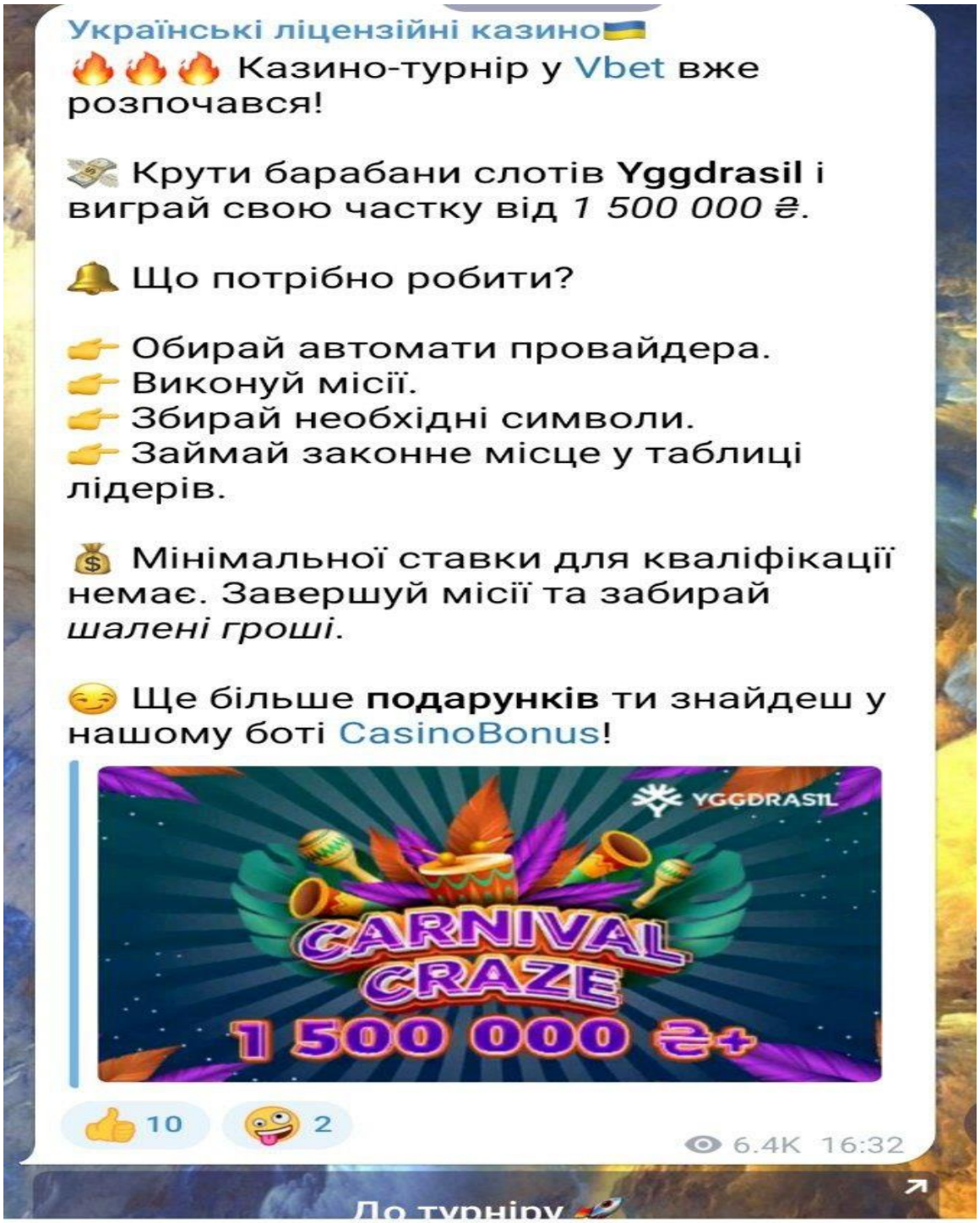
"ЗАБЛОКОВАНО" - Цей заголовок викликає паніку в користувачів, які можуть бути занадто зануреними у свої онлайн-акаунти, і спонукає їх до негайної дії.

"ТЕРМІНОВО!" - Заголовок з наголошенням на терміновості спонукає користувача вжити швидких дій, оскільки є відчуття, що на горизонті наближається якийсь небезпечний термін [52].

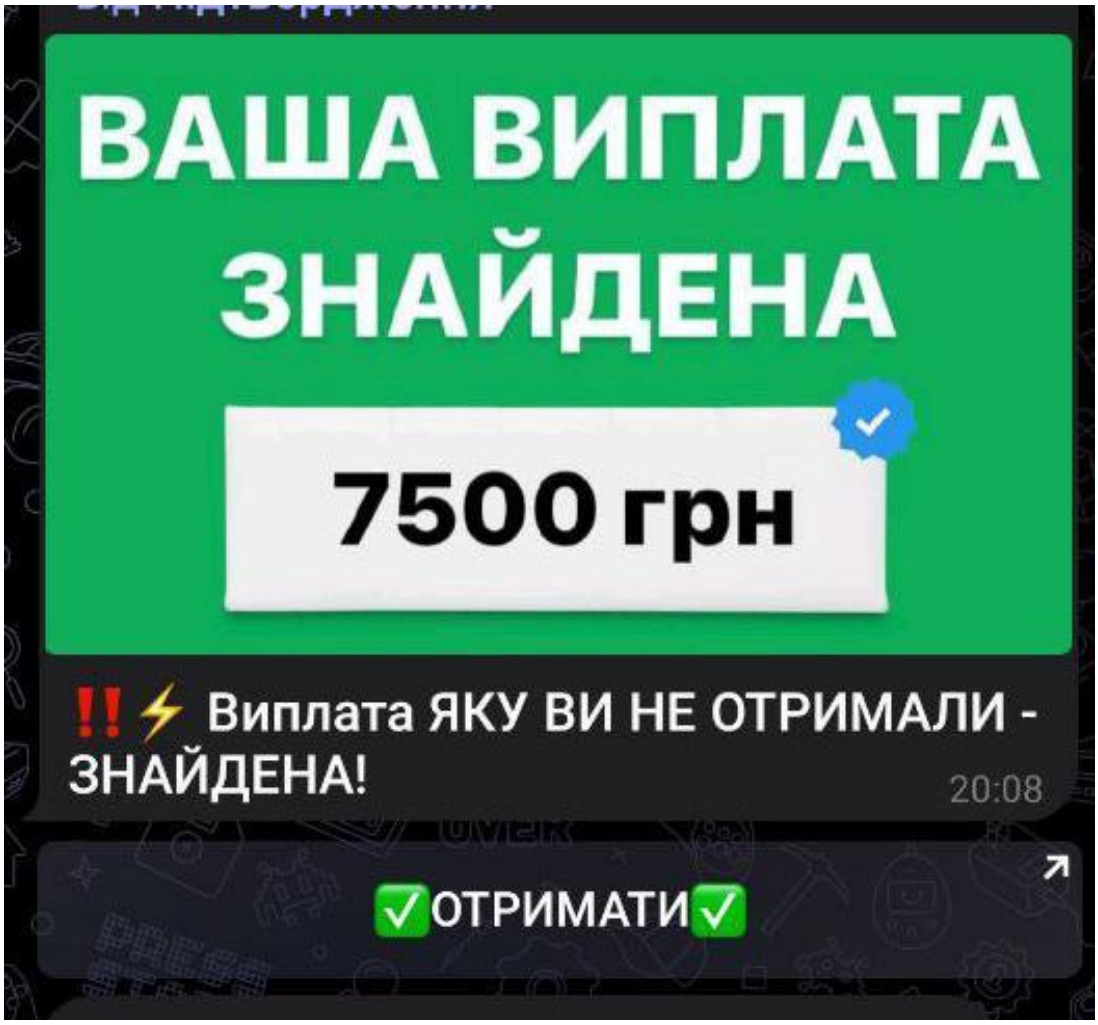
"УВАГА!" - Цей заголовок намагається привернути увагу користувача, зробити його уважнішим та більш зацікавленим у повідомленні.

2. Пропозиції про виграш: Шахраї можуть використовувати заголовки, які пропонують користувачам можливість виграти щось або отримати

безкоштовний доступ до чогось. Наприклад, "Виграйте $1000 зараз!" або "Отримайте доступ до преміум-вмісту безкоштовно!".



Мал. 2.3.2. –Приклад фішингового повідомлення



Мал. 2.3.3. –Приклад фішингового повідомлення

Так, це ще одна популярна нейролінгвістична техніка, яку використовують шахраї в заголовках фішингових повідомлень. Заголовки, які пропонують можливість отримати щось безкоштовно або виграти щось, зазвичай привертають увагу користувачів і спонукають їх до відкриття повідомлення або відповіді на нього [53].

Шахраї можуть використовувати цю техніку, щоб запропонувати користувачам можливість отримати безкоштовну підписку на платформу, виграти подарунки або отримати доступ до ексклюзивного вмісту. Однак, після того, як користувачі відкривають таке повідомлення або відповідають на нього, шахраї можуть звернутися до них з проханням надати особисту інформацію або виконати інші дії, що можуть призвести до крадіжки їхніх даних або грошей.

3. Посилання на відомі бренди: Шахраї можуть використовувати імена відомих брендів або компаній в заголовках, щоб здати свої повідомлення більш довірчими. Наприклад, "PayPal підтвердження аккаунту" або "Google оновлення безпеки".

Мал. 2.3.4. –Приклад фішингового повідомлення

Так, шахраї часто використовують імена відомих брендів або компаній в заголовках своїх фішингових повідомлень, щоб створити враження, що це офіційне повідомлення від цих компаній. Вони можуть використовувати логотипи, назви та кольорову гаму, щоб створити вигляд офіційного повідомлення. Це може допомогти шахраям переконати користувачів у тому, що повідомлення є легітимним, та спонукати їх до виконання певних дій. Однак варто пам'ятати, що офіційні компанії ніколи не запитуватимуть особисту інформацію або паролі через електронну пошту [54].

Важливо розуміти, що шахраї можуть використовувати різні комбінації цих технік в заголовках фішингових повідомлень.

РОЗДІЛ 3. НЕЙРОЛІНГВІСТИЧНИЙ АНАЛІЗ ФІШИНГОВИХ ПОВІДОМЛЕНЬ

3.1. Аналіз найбільш ефективних нейролінгвістичних технік в заголовках фішингових повідомлень

Нейролінгвістичний аналіз (NLP) може бути корисним для виявлення фішингових повідомлень та їх класифікації на основі різних параметрів. Наприклад, можна проаналізувати такі параметри, як синтаксична структура повідомлення, використання спеціальних слів та термінів, наявність посилань та ін.

Одним зі способів застосування NLP є аналіз семантичного контексту повідомлення. Фішингові повідомлення часто містять певні ключові слова або фрази, які намагаються змусити отримувача реагувати швидко та емоційно. Такі ключові слова можуть включати "негайно", "важливо", "увага" та інші. Також фішингові повідомлення можуть включати вимоги надати конфіденційну інформацію або просити виконати певні дії, наприклад, натиснути на посилання або завантажити документи.

Ще одним параметром, який можна проаналізувати за допомогою NLP, є використання спеціальних слів та термінів. Фішингові повідомлення можуть містити слова, які зазвичай пов'язуються з фішингом, наприклад, "phishing", "scam", "spoofing" та інші. Також вони можуть містити інші терміни, які використовуються в контексті кібербезпеки, наприклад, "вірус", "шпигунський софт" тощо [59].

Фішинг – це один з найпоширеніших видів кібератак, який полягає в тому, що злочинці намагаються отримати конфіденційну інформацію, таку як паролі, номери банківських карток, електронні адреси, за допомогою підроблених електронних листів. Одним з ключових аспектів фішингових повідомлень є заголовки, які мають за мету привернути увагу отримувачів та спонукати їх до відкриття листа та виконання дій, які можуть призвести до крадіжки особистої інформації.

Дослідники у сфері кібербезпеки встановили, що ефективність фішингу значно залежить від якості та змісту заголовків. Найбільш ефективні нейролінгвістичні техніки, які використовуються в заголовках фішингових повідомлень, полягають у використанні емоційно заряджених слів, фішингових технік маніпулювання, використанні відомих торгових марок та імітації повідомлень від відомих організацій [55].

Перша найбільш ефективна техніка - використання емоційно заряджених слів. Заголовки фішингових повідомлень можуть містити такі емоційно заряджені слова, як "терміново", "негайно", "ексклюзивно", "надзвичайно", "безкоштовно". Вони допомагають злочинцям привернути увагу отримувачів та спонукати їх до відкриття листа.

Друга ефективна техніка - використання фішингових технік маніпулювання.

Фішинг - це атака, яка передбачає використання підроблених повідомлень з метою виманити конфіденційну інформацію, таку як паролі, номери кредитних карток та інші особисті дані. Один з найбільш ефективних способів, яким користуються кіберзлочинці, є використання нейролінгвістичних технік у заголовках фішингових повідомлень.

Нейролінгвістичні техніки (NLP) - це засоби, які допомагають відтворювати людську мову за допомогою комп'ютера. Вони дозволяють створювати повідомлення, які максимально схожі на ті, що використовуються в реальному житті. Нейролінгвістичні техніки дозволяють створювати заголовки, які змушують людей реагувати і відкривати фішингові повідомлення.

Одним з ефективних способів використання NLP є створення заголовків, які містять емоційну складову. Наприклад, "Ваш обліковий запис заблоковано" або "Важлива інформація щодо вашого банківського рахунку". Ці заголовки створюють емоційний резонанс у людей, що змушує їх відкривати повідомлення і відповідати на запити, навіть якщо вони сумніваються щодо їх достовірності.

Ще одним способом є використання заголовків, які містять конкретну інформацію про користувача, наприклад, "Для Марини: спеціальна пропозиція на відпочинок". Ці заголовки намагаються надати враження, що повідомлення є персоналізованим і надіслане саме для даного користувача [57].

Перший спосіб, який використовували фішери, був крадіжка паролів користувачів та використання алгоритмів для створення випадкових номерів кредитних карток. Незважаючи на те, що вдалі атаки були рідкісні, їх було достатньо, щоб завдати значної шкоди. Випадкові номери кредитних карток використовувалися для відкриття рахунків AOL. Ці облікові записи використовувалися для спаму (масової розсилки повідомлень).

У 1995 році компанія AOL вжила заходів безпеки для того, щоб запобігти використанню випадково згенерованих номерів кредитних карток. Після цього фішери створили схему шахрайства, яка стала дуже поширеною. Через системи миттєвого обміну повідомленнями та електронною поштою AOL вони надсилали повідомлення користувачам, видаючи себе за співробітників AOL.

Ці повідомлення запитували користувачів підтвердження їх облікових записів або підтвердження їх платіжної інформації. Наприкінці 2003 року фішери зареєстрували десятки доменів, які виглядали справжніми сайтами, такими як PayPal. Вони використовували поштові програми, щоб надіслати фальшиві електронні листи клієнтам PayPal [61].

Цих клієнтів приводили на підроблені сайти та просили оновити дані їхніх кредитних карток та іншу ідентифікуючу інформацію. На початку 2004 р фішингові атаки стали більш витонченими та результативними. За останнє десятиліття розроблено нові, складніші методи та вдосконалено існуючі.

В даний час існує безліч методів фішингу. Слід додати, що фішинг-атака може використовувати соціальну інженерію та складатися з комбінації методів, наведених нижче.

Email/Spam – найпоширеніший вид фішингу. Застосовує підхід «spray and pray», тобто один і той же електронний лист відправляється мільйонам користувачів, сподіваючись, що фішинг-атака закінчиться успіхом [

Malware - фішингові шахрайства, пов'язані зі шкідливими програмами, які вимагають, щоб вони були запущені на комп'ютері користувача. Наприклад, ransomware — шкідлива програма, яка відмовляє у доступі до пристрою або файлів доти, доки не буде виплачена певна грошова сума.

Така програма, як keylogger, використовується для ідентифікації введення з клавіатури. Інформація надсилається хакерам, які можуть розшифровувати паролі та інші види інформації. Шкідлива програма trojan проникає до комп'ютера під виглядом легітимного програмного засобу, але насправді здійснює несанкціонований доступ до облікового запису користувача. Потім отримана інформація передається кіберзлочинцям. Шкідливе програмне забезпечення зазвичай прикріплюється до електронного листа, надісланого користувачеві фішерами, або може бути також прикріплено до файлів, що завантажуються [58].

Malvertising – це шкідлива реклама, що містить сценарії, призначені для завантаження шкідливих програм або примусового розміщення небажаного контенту на пристрої користувача.

Vishing (Voice Phishing) - метод фішингу, в якому шахрай робить телефонні дзвінки користувачеві. Ціль полягає в тому, щоб отримати конфіденційну інформацію через телефон.

Smishing (SMS Phishing) — це метод, який здійснюється через телефонну службу коротких повідомлень (SMS). Наприклад, текст такого повідомлення намагається схилити жертву до розкриття особистої інформації за допомогою посилання, яке веде на фішинговий сайт [60].

Phishing є більш цілеспрямованою атакою, при якій шахраї знають, яку конкретну людину чи організацію вони переслідують. Зловмисники досліджують мету, щоб зробити атаку більш персоналізованою та збільшити ймовірність потрапляння жертви у їхню пастку.

Whaling — метод не дуже відрізняється від Spear Phishing, але цільова група стає більш специфічною та обмеженою. Цей метод орієнтований на керівні посади, які вважаються важливими фігурами в інформаційному ланцюжку будь-якої організації, зазвичай відомі як «Whale» («Кіт») у термінах фішингу.

Phishing through Search Engines — це метод, що включає пошукові системи, де користувач направляється на сайти, які можуть пропонувати недорогі продукти або послуги. Коли користувач намагається купити продукт, він вводить дані платіжної картки або електронного гаманця, які збираються фішинговим сайтом [56].

Web Based Delivery - є одним із найскладніших методів фішингу. Також відомий як "man-in-the-middle", коли хакер знаходиться між оригінальним сайтом та фішинговою системою. Фішер відстежує деталі під час транзакції між справжнім веб-сайтом та користувачем, причому користувач про це не знає.

Pop-Ups - спливаючі повідомлення є одним із найпростіших методів для результативного проведення фішинг-атак. Вони дозволяють зловмисникам отримувати реєстраційні дані, відправляючи користувачам спливаючі повідомлення та зрештою наводячи їх на підроблені веб-сайти. Один з варіантів фішингових атак, також відомий як in-session phishing, працює шляхом відображення спливаючого вікна під час сеансу онлайнбанкінгу і виглядає як повідомлення від банку.

Session Hijacking — це метод захоплення сеансу, при якому фішер використовує механізм управління веб-сеансом для крадіжки інформації у користувача.

Content Injection — це спосіб, коли фішер змінює частину вмісту на сторінці надійного веб-сайту. Це робиться для того, щоб ввести в оману користувача і відправити його на сторінку за межами справжнього веб-сайту, де користувачеві пропонується ввести особисту інформацію.

Clone phishing - це тип фішингової атаки, при якій законний і раніше доставлений електронний лист, що містить вкладення або посилання, використовується для створення майже ідентичного або клонованого електронного листа

Вкладення або посилання в електронному листі замінюються шкідливою версією, а потім відправляються з адреси електронної пошти, підробленої, щоб здаватися вихідним від початкового відправника. Як правило, для цього потрібно, щоб відправник, або одержувач були попередньо зламані третьою стороною.

Filter evasion — метод, у якому фішери використовують зображення замість тексту, щоб утруднити антифішинговим фільтрам виявлення тексту, зазвичай використовується у фішингових листах. У відповідь складніші антифішингові фільтри здатні відновлювати прихований текст у зображеннях за допомогою OCR (оптичного розпізнавання символів).

Link Manipulation - за допомогою даного методу, шахрай відправляє посилання на шкідливий веб-сайт

Коли користувач натискає на неї, він відкриває сайт фішера замість того, що вказано у засланні. Фішери можуть використовувати піддомени. Наприклад, дивлячись на URL-адресу www.mybank.user.com, необізнана особа вважає, що посилання приведе її до розділу «user». Насправді посилання веде до розділу «mybank», тому що ієрархія доменів завжди йде справа наліво. Існує спосіб приховати фактичну URL-адресу під звичайним текстом. Замість відображення фактичної URL-адреси фішери використовують такі пропозиції, як «натисніть тут» або «підпишіться».

Насправді URL-адреса, яка ховається за текстом, веде на фішингові сайти. Більш переконливий лист може навіть відображати фактичне посилання, але веде вона на фішинговий сайт. Інший метод маніпулювання посиланнями полягає в тому, що шахраї купують домени з різними варіантами написання популярного домену, наприклад: facebok.com, googlle.com, yahooo.com і т.д. Потім вони дурять користувачів, створюючи схожі сайти та

запитуючи особисту інформацію. У наступному методі зловмисник вводить в оману щодо посилання, використовуючи переваги схожих символів. Наприклад, латинські літери "c", "o" та "x" можуть замінюватися на аналогічні літери кирилиці.

Website Forgery - спосіб при якому шкідливий сайт видає себе за справжній. Підробка в основному здійснюється двома способами: міжсайтовим скриптингом та заміною сайту.

Міжсайтовий скриптинг (XSS) — це атака, коли хакер впроваджує шкідливий код у веб-додаток чи веб-сайт. Це дуже поширена і широко використовувана техніка, за якої жертва не є прямою мішенню. Швидше за все, зловмисник використовує вразливість у веб-застосунку або веб-сайті, який відвідує користувач. Зрештою, шкідливий сценарій доставляється в браузер жертви [62].

Інший метод полягає в наступному: створюється веб-сайт, який виглядає схожим на законний сайт, до якого користувач дійсно має намір отримати доступ. Підроблений веб-сайт має схожий інтерфейс користувача і дизайн, часто має схожу URL-адресу.

Нейролінгвістичні техніки можуть бути корисними для аналізу заголовків фішингових повідомлень та виявлення тих, які є найбільш ефективними для залучення уваги та маніпулювання отримувачем. Ось деякі з найбільш ефективних технік, які можуть бути використані в заголовках фішингових повідомлень:

1. Емоційна маніпуляція: Заголовки фішингових повідомлень можуть містити слова, які мають емоційний заряд, такі як "шокуючі", "здивовані", "жахливі", "вражаючі" тощо. Ці слова можуть залучити увагу отримувача та спонукати його до подальшого читання повідомлення.

2. Використання термінів зі світу кібербезпеки: Заголовки фішингових повідомлень можуть містити терміни, які зазвичай пов'язуються з кібербезпекою, такі як "перевірка безпеки", "перевірка на віруси", "небезпечний вміст" тощо. Ці терміни можуть створювати враження, що

повідомлення має важливий характер та пов'язане з кібербезпекою, що може викликати більшу увагу та збільшити шанси на успішне проведення фішингової атаки.

3. Імітація повідомлень відомих компаній: Заголовки фішингових повідомлень можуть намагатися імітувати повідомлення відомих компаній, таких як Google, PayPal, Amazon тощо. Це може збільшити ймовірність того, що отримувач зверне увагу на повідомлення та відповість на нього.

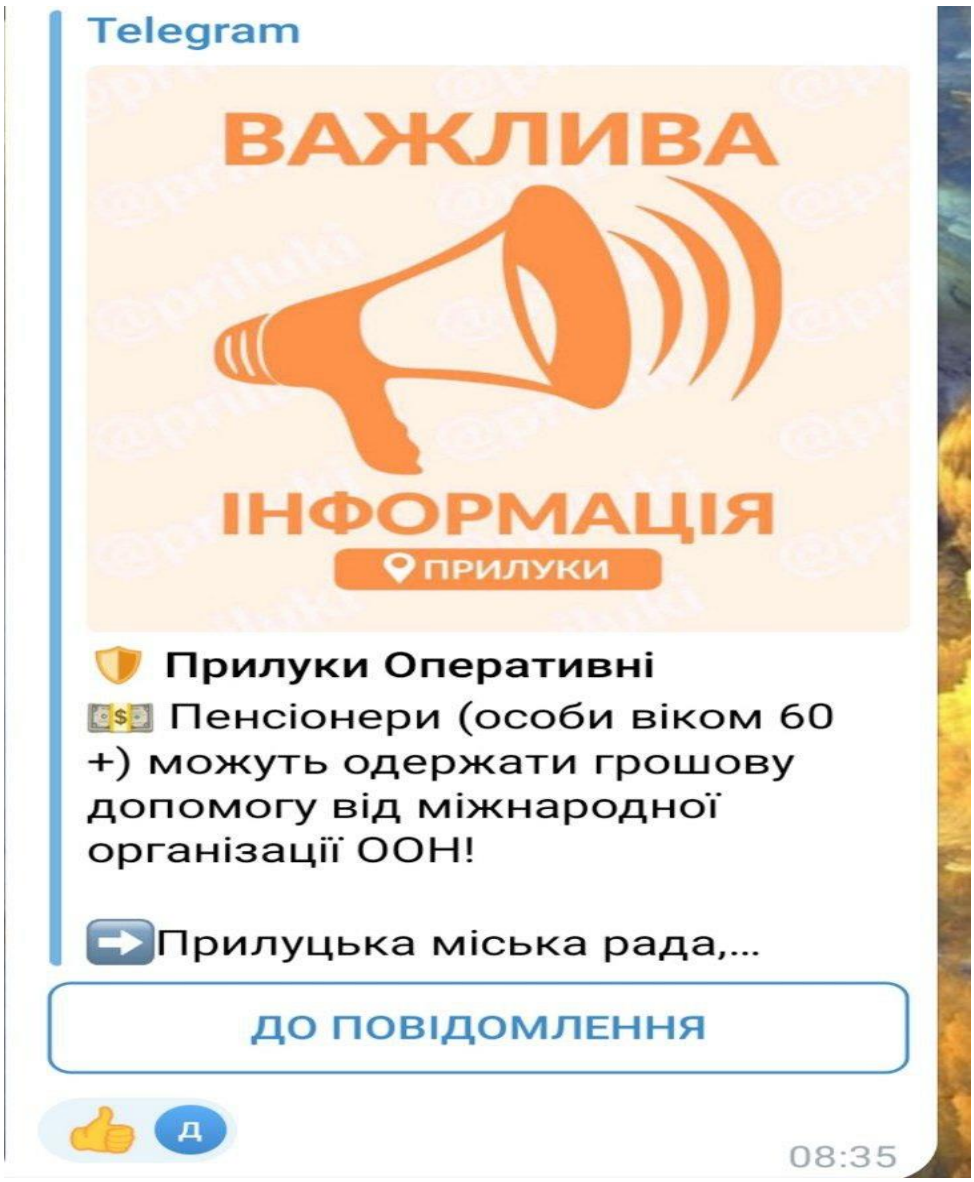
4. Емоційність: Фішингові повідомлення можуть містити заголовки, які викликають емоційну реакцію у отримувача. Наприклад, "Ваш рахунок було заблоковано!" або "Ваша безпека в небезпеці!". Такі заголовки можуть змусити отримувача швидко реагувати та виконувати дії без додаткової перевірки.

5. Авторитетність: Фішингові повідомлення можуть містити заголовки, які намагаються дати враження, що вони відправлені відомим або авторитетним джерелом. Наприклад, "PayPal повідомляє про проблеми з вашим рахунком" або "Microsoft Security повідомляє про новий вірус". Такі заголовки можуть змусити отримувача вірити, що повідомлення є справжнім та дійсним.

6. Співпадіння: Фішингові повідомлення можуть містити заголовки, які намагаються використовувати інформацію про отримувача, щоб змусити його відкрити повідомлення. Наприклад, "Ви отримали подарунок від Amazon!" або "Ваша банківська картка була заблокована". Такі заголовки можуть змусити отримувача вважати, що повідомлення є персоналізованим та має важливу інформацію для нього [63].

Фішингові повідомлення зазвичай мають заголовки, які спонукають отримувача відкрити повідомлення та взяти на себе певні дії. Для створення ефективного заголовка фішингового повідомлення зловмисники можуть використовувати різні нейролінгвістичні техніки. Далі наведені деякі з найбільш ефективних технік з прикладами.

1. Створення термінового враження: Фішингові повідомлення можуть містити слова, які створюють враження терміновості та потреби відкрити повідомлення негайно. Наприклад, "ВАЖЛИВЕ ПОВІДОМЛЕННЯ! НЕОБХІДНО ВІДПОВІСТИ НЕГАЙНО!", "УВАГА! ТЕРМІНОВО!"

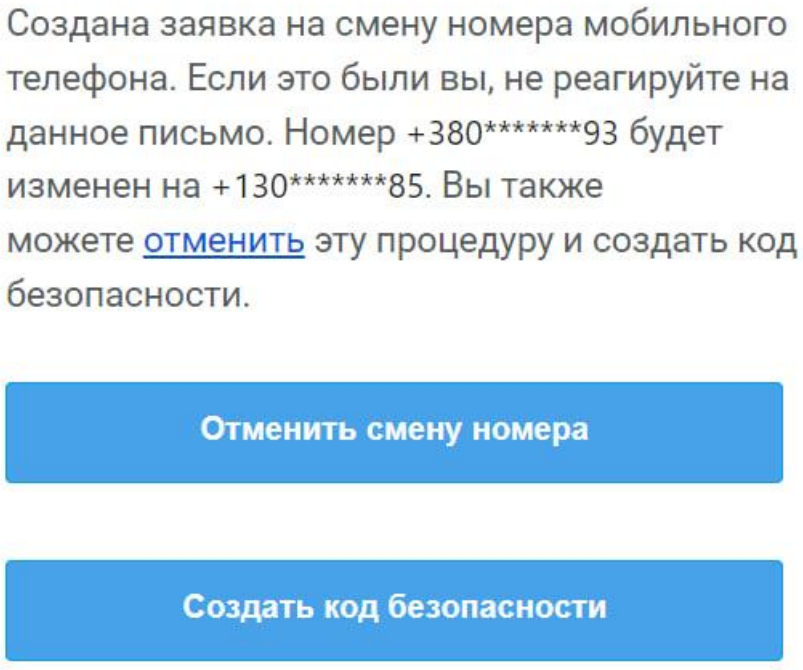


Мал. 3.1.1. – Приклад фішингового повідомлення, який створює термінове враження

2. Створення підозрілого враження: Фішингові повідомлення можуть містити заголовки, які створюють враження, що їхнє вміст підозрілий або несподіваний. Наприклад, "Незвичайна активність на вашому акаунті", "Підозрілі операції на вашому банківському рахунку"

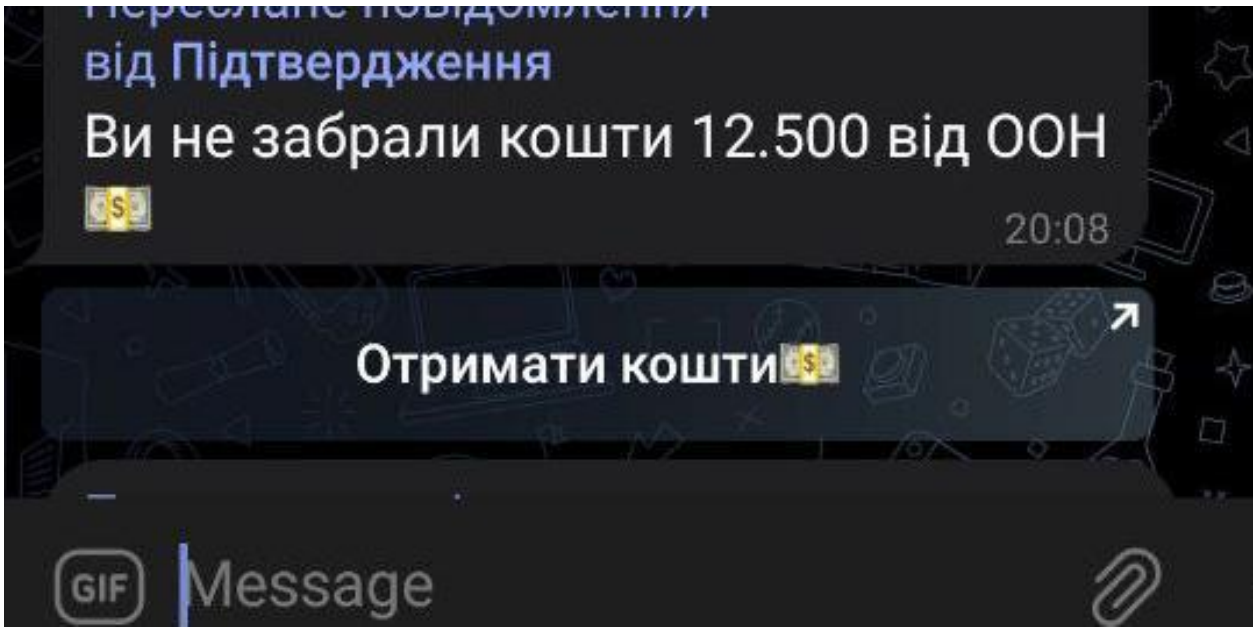
Мал. 3.1.2. – Приклад фішингового повідомлення, який створює підозріле враження

3. Створення заголовка від імені відомої компанії: Фішингові повідомлення можуть містити заголовки, які створюють враження, що вони відправлені від імені відомої компанії, наприклад, "Microsoft Security Alert", "Google Account Warning"



Мал. 3.1.2. – Приклад фішингового повідомлення, який створює заголовок від відомої компанії

4. Створення враження надзвичайної можливості: Фішингові повідомлення можуть містити заголовки, які створюють враження, що отримувач може отримати щось надзвичайне або незвичайне. Наприклад, "Виграйте безкоштовний подарунок!", "Отримайте 1000 доларів за 5 хвилин!"



Мал. 3.1.2. – Приклад фішингового повідомлення, який створює враження надзвичайної можливості

Отже, нейролінгвістичні техніки можуть бути корисними для створення ефективних фішингових повідомлень, оскільки вони дозволяють створювати заголовки та текст, які змушують людей діяти швидко та емоційно.

3.2. Порівняння ефективності використання нейролінгвістичних технік з традиційними методами фішингу

Нейролінгвістичні техніки фішингу можуть бути ефективнішими, ніж традиційні методи фішингу, оскільки вони засновані на використанні мовних та психологічних методів, які дозволяють зловмисникам створювати більш переконливі атаки.

Наприклад, з використанням нейролінгвістичних технік, зловмисники можуть аналізувати мовні зразки та психологічні властивості цільових

користувачів, що дозволяє їм створювати персоналізовані атаки, які більше відповідають потребам та інтересам конкретних осіб.

З іншого боку, традиційні методи фішингу можуть бути менш ефективними, оскільки вони зазвичай базуються на використанні загальних шаблонів та імітації повідомлень відомих компаній або організацій. Крім того, користувачі можуть бути звичайно пильнішими до незнайомих повідомлень, тому зловмисники повинні вкладати більше зусиль у підвищення переконливості своїх атак [64].

Отже, використання нейролінгвістичних технік може дозволити зловмисникам досягти більшої ефективності в проведенні фішинг-атак, однак важливо зауважити, що будь-який тип фішинг-атаки є незаконним та повинен бути уникнутий.

Нейролінгвістичні техніки використовуються в багатьох сферах, включаючи кібербезпеку, зокрема фішинг. Якщо порівнювати ефективність використання нейролінгвістичних технік з традиційними методами фішингу, то можна зробити наступні висновки:

Традиційні методи фішингу, такі як відправка електронної пошти або повідомлення з підробленим відправником, можуть бути ефективними, якщо вони виконані досконало. Проте, їх ефективність залежить від того, наскільки користувачі попереджені про можливі загрози та вміють розпізнавати підроблені повідомлення.

Нейролінгвістичні техніки можуть покращити ефективність фішингу, оскільки вони дозволяють здійснювати напади більш спеціалізовано і з використанням більш складних методів. Наприклад, використання штучного інтелекту може дозволити виявляти індивідуальні риси поведінки користувачів та використовувати цю інформацію для більш точної спрямованої атаки.

Отже, хоча традиційні методи фішингу можуть бути ефективними, нейролінгвістичні техніки можуть покращити ефективність нападів та зробити їх більш складними для виявлення. Проте, важливо зазначити, що

використання нейролінгвістичних технік для фішингу є незаконним та шкідливим для користувачів.

Нейролінгвістичні техніки в фішингу можуть бути ефективнішими за традиційні методи, оскільки вони засновані на використанні штучного інтелекту і навчення машин з досвідом виявлення шахрайства. Однак, все залежить від контексту та вмінь атакувальників.

Наприклад, традиційний метод фішингу може включати в себе відправлення електронної пошти або повідомлення, що містить підозрілі посилання або вимоги до надання конфіденційної інформації, з метою залучити потенційну жертву до небезпечної дії. Цей метод може бути досить ефективним, якщо він підібраний правильно і виконаний професійно.

З іншого боку, нейролінгвістичні техніки можуть використовувати аналіз мовлення та засоби штучного інтелекту для створення більш реалістичних та переконливих повідомлень фішингу. Наприклад, генерація тексту на основі навчальних даних може дати можливість створювати повідомлення, які більш точно імітують тон та стиль комунікації організації, від імені якої вони надходять. Це може зробити фішинг-атаку більш успішною в масштабах великих корпорацій та державних організацій [65].

Нейролінгвістичний підхід до фішингу полягає в тому, щоб використовувати мовні техніки для злочинних цілей. Наприклад, фішер може намагатися впливати на жертву, використовуючи соціальні інженерні методи, які включають в себе переконливу мову, звернення до емоцій та маніпуляцію мисленням. Ці техніки можуть бути дуже ефективними, оскільки вони спираються на знання про людську психологію та мовленнєву поведінку.

Традиційні методи фішингу, з іншого боку, мають більш технічний підхід. Наприклад, фішер може використовувати фішингові сайти, які намагаються переконати жертву введенням свого логіну та паролю. Інші методи фішингу можуть включати в себе відправлення електронної пошти з запитом на оновлення даних або використання зловмисних програм для отримання доступу до системи.

Залежно від ситуації та цілей фішера, різні підходи можуть бути ефективні. Наприклад, якщо фішер має доступ до інформації про жертву, такої як соціальні мережі або електронні записи, то використання нейролінгвістичних технік може бути дуже ефективним.

Нейролінгвістичні техніки можуть бути ефективнішими в порівнянні з традиційними методами фішингу, оскільки вони здатні підлаштуватися до конкретних потреб індивідуального користувача та викликати більше довіри.

Ось декілька прикладів:

1. Підхід, що використовує мовні моделі, може бути ефективним у фішингу, оскільки він дозволяє використовувати більш натуральну мову та відповідати на запитання користувачів у реальному часі. Це може зробити фішингові повідомлення більш переконливими та зрозумілими для потенційної жертви.

2. Аналіз соціальних мереж та інших джерел даних може допомогти створити персоналізовану фішингову атаку. Наприклад, якщо хакер знає, що користувач любить подорожувати, він може використовувати цю інформацію, щоб надіслати фішингове повідомлення, яке містить пропозицію про подорож.

3. Фішинг-атаки можуть використовувати нейронні мережі для автоматичної обробки відповідей користувачів та відповідного підлаштування стратегії атаки. Наприклад, якщо користувач виявляє підозру, фішингова атака може змінити свій підхід та надіслати інше повідомлення, щоб збільшити шанси на успіх.

Традиційні методи фішингу, такі як масові розсилки електронних листів або використання стандартних шаблонів повідомлень, можуть бути менш ефективними, оскільки вони не враховують індивідуальних потреб.

Нейролінгвістичні техніки та традиційні методи фішингу є двома різними підходами до здійснення атак на інформаційні системи.

Традиційні методи фішингу часто базуються на використанні соціальної інженерії та маніпуляції психологічним станом потенційної жертви. Такі методи можуть включати в себе відправку фішингових листів, які виглядають

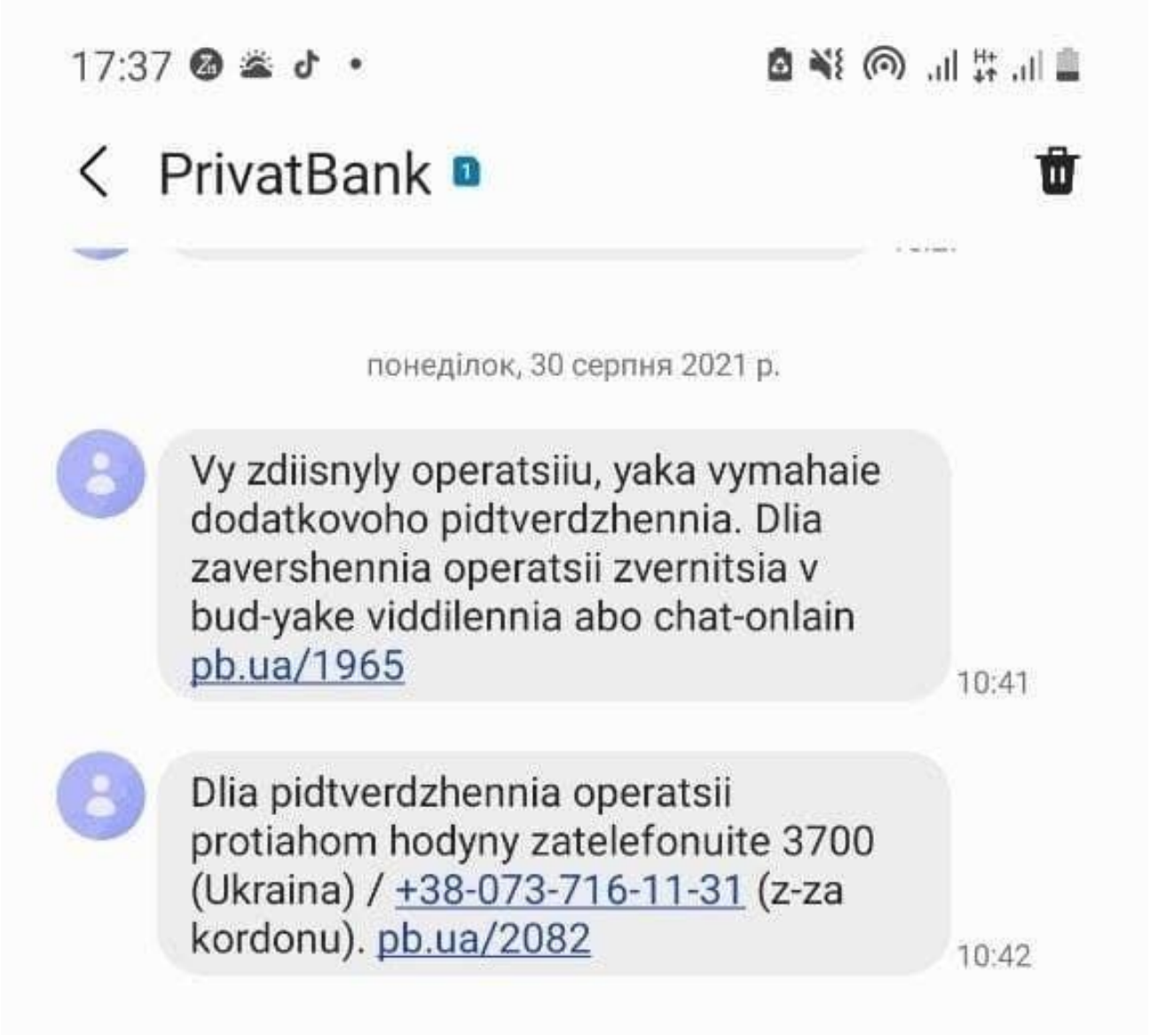
як повідомлення від надійних джерел (наприклад, банків), запитів на введення конфіденційної інформації, або надання інших привабливих пропозицій, щоб залучити увагу жертви.

У свою чергу, нейролінгвістичні техніки використовують нейромережі та аналіз текстів для створення більш переконливих та підступних повідомлень. Такі повідомлення можуть містити персоналізовані дані, що отримані з соціальних мереж або звідки-небудь іншого, та піддаватися аналізу психологічних характеристик жертви для створення ефективніших схем маніпуляції [66].

Отже, різниця між цими двома підходами полягає в тому, що нейролінгвістичні техніки базуються на більш складному технічному підході, що дозволяє створювати більш переконливі та цілеспрямовані повідомлення. Однак, в той же час, традиційні методи фішингу все ще можуть бути досить ефективними в більш простих ситуаціях, де вимагається менше складності.

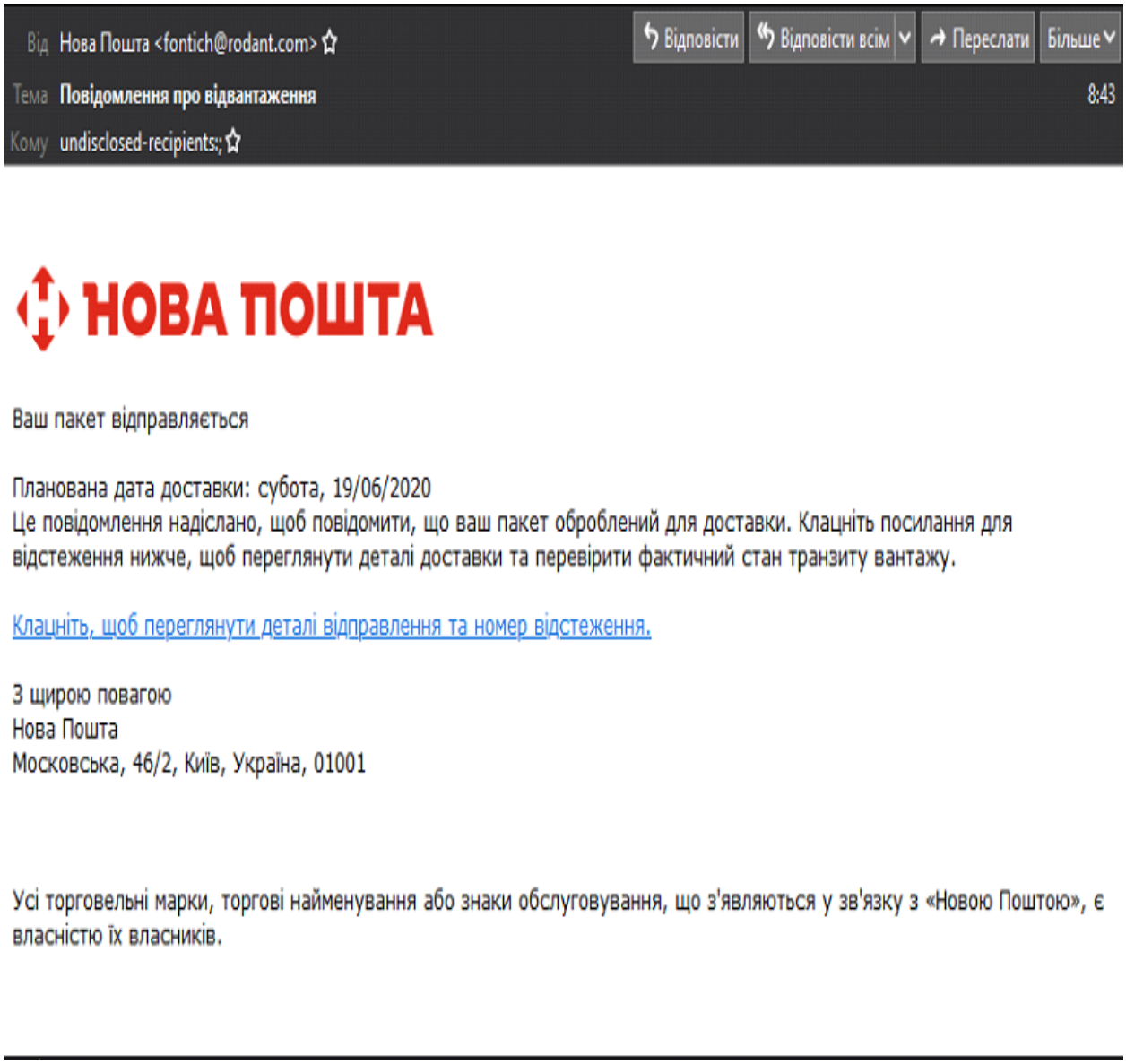
Приклади традиційних методів фішингу:

1. Підробка електронної пошти від імені банку або іншої організації: зловмисники можуть відправити електронну пошту, яка здається від імені банку, з запитом про оновлення або перевірку ваших банківських даних. У листі можуть бути посилання на фальшиві веб-сайти, на які вас направлять, де вас просять ввести свої банківські дані. Це може дозволити зловмисникам отримати доступ до вашого банківського рахунку.



Мал. 3.2.1. – Приклад фішингового повідомлення, який є підробкою від імені банку

2. Підробка веб-сайтів: зловмисники можуть створювати фальшиві веб-сайти, що дуже схожі на офіційні, з метою змусити вас ввести свої логіни та паролі для входу на різні веб-сайти. Зазвичай це робиться з метою отримання доступу до вашої електронної пошти, соціальних мереж, банківських або інших фінансових рахунків.



Мал. 3.2.2. – Приклад фішингового повідомлення, який створює підробку веб-сайту

3. Фізичний фішинг: це може бути спроба отримати доступ до вашої інформації шляхом проникнення в приміщення або залишення фальшивих документів, які містять запити про ваші конфіденційні дані, на робочому місці або в іншому місці, де ви можете знайти ці документи.

4. Спам-атаки: зловмисники можуть відправляти вам електронну пошту, яка містить непотрібну інформацію або шкідливі віруси. Це може бути спробою отримати доступ до вашої інформації або зараження вашого комп'ютера.

Мал. 3.2.3. – Приклад фішингового повідомлення, який є Спам-атакою

Фішинг - це форма кібершахрайства, яка зазвичай використовується для крадіжки особистої інформації та даних про користувачів, таких як паролі, імена користувачів, номери кредитних карток та інші конфіденційні дані.

Нейролінгвістичні методи фішингу - це недобросовісні техніки використання мовленнєвих психологічних підходів з метою обману людей та

отримання від них конфіденційної інформації, такої як логіни, паролі, номери банківських карток та інше.

Деякі з найбільш поширених методів фішингу, що використовують нейролінгвістичні методи, включають наступні:

1. Соціальна інженерія: Фішер може намагатися використовувати знання про людину, її інтереси та пристрасті для створення переконливих повідомлень, що мають намір обдурити людей. Наприклад, він може створювати повідомлення з пропозиціями, які відповідають інтересам людей або надсилати електронні листи відомих брендів, звертаючись до людських емоцій.

2. Використання виражень, які надають ситуації терміновості та небезпеки: Фішер може використовувати фрази, що надають враження, що потрібно негайно діяти для запобігання небезпеці або втраті доступу до важливої інформації.

3. Підробка даних відомих компаній: Фішер може використовувати техніки фальшування даних відомих компаній, щоб здобути довіру людей та переконати їх надати конфіденційну інформацію.

4. Використання техніки соціального давлення: Фішер може використовувати техніку соціального давлення, щоб переконати людей надати конфіденційну інформацію.

Один з методів нейролінгвістичного фішингу - це використання мовних аналізаторів для створення повідомлень, які звучать, ніби вони були написані людиною, а не комп'ютером. Це зменшує ймовірність, що людина підозрюватиме, що вона спілкується з фішером.

Інші методи нейролінгвістичного фішингу включають використання аналізу мови та стилістичних особливостей повідомлень для того, щоб створити переконливі сценарії та історії, які спонукають людей до дій, які можуть призвести до витоку конфіденційної інформації. Фішери можуть використовувати нейролінгвістичний аналіз для аналізу соціальних мереж та

інших джерел інформації, щоб створити персоналізовані повідомлення, які максимально переконливо спонукають людей до небезпечних дій.

Отже, фішинг - це вид кібератак, в якому зловмисники намагаються отримати конфіденційну інформацію від користувачів, таку як логіни, паролі, номери кредитних карток і інші особисті дані. Зазвичай фішинг-атаки здійснюються шляхом відправки електронних листів або повідомлень, що виглядають як легітимні комунікації від відомих організацій або осіб, з якими користувачі взаємодіють. Наприклад, зловмисники можуть надіслати електронний лист, який виглядає як повідомлення від вашого банку, з проханням оновити свої особисті дані на підробленій сторінці. Коли користувачі вводять свої дані на цій підробленій сторінці, зловмисники можуть використовувати ці дані для крадіжки грошей або злому інших онлайн-аккаунтів. Щоб захиститися від фішингу, користувачі повинні бути обережні і не вводити свої конфіденційні дані на неперевірених сторінках, а також використовувати програмне забезпечення для захисту від шкідливих програм та вірусів.

3.3. Оптимальні методи захисту від фішингу з використанням нейролінгвістичних технік

Оптимальні методи захисту від фішингу з використанням нейролінгвістичних технік - це методи захисту, які використовують мовні аналізи та машинне навчання для виявлення та запобігання фішинговим атакам. Ці методи дозволяють комп'ютерам розпізнавати фішингові повідомлення та відрізняти їх від легітимних повідомлень [67].

Нейролінгвістичні техніки використовуються для аналізу тексту фішингових повідомлень та виявлення ознак, які можуть свідчити про шахрайську природу повідомлення. Наприклад, такі ознаки можуть включати використання мови підступу, вимогливості, викликів до дії або вимагань надати конфіденційну інформацію.

Оптимальні методи захисту від фішингу з використанням нейролінгвістичних технік можуть включати в себе програмне забезпечення, яке використовує аналіз мовлення та машинне навчання для виявлення фішингових повідомлень. Також до них можуть входити методи тренування співробітників на розпізнавання фішингових атак та підвищення рівня свідомості про загрози безпеки.

Отже, оптимальні методи захисту від фішингу з використанням нейролінгвістичних технік є важливим інструментом для захисту від шахрайських атак та забезпечення безпеки даних індивідуальних користувачів та компаній.

Оптимальні методи захисту від фішингу з використанням нейролінгвістичних технік включають:

1. Навчання співробітників - важливо регулярно навчати своїх співробітників про ризики, пов'язані з фішингом, і навчати їх розпізнавати небезпечні повідомлення. Це можна зробити через тренінги з безпеки, симуляції фішингу та інші методи.

2. Використання технологій захисту - можна використовувати програмне забезпечення для виявлення та блокування фішингових повідомлень. Ці інструменти використовують різні технології, такі як машинне навчання та аналіз поведінки користувача.

3. Перевірка посилань - важливо перевіряти будь-які посилання в повідомленнях, перш ніж клікати на них. Наприклад, можна навести курсор на посилання, щоб перевірити його адресу. Якщо адреса виглядає підозріло, краще утриматися від кліку.

4. Двофакторна аутентифікація - використання двофакторної аутентифікації дозволяє забезпечити додатковий рівень захисту облікового запису. Це означає, що, навіть якщо зловмисник вкраде ваш пароль, він не зможе отримати доступ до вашого облікового запису без додаткового підтвердження.

5. Підтримка безпечної культури - важливо створити культуру безпеки, в якій співробітники можуть вільно обговорювати питання безпеки та повідомляти про підозрілі повідомлення. Це дозволить оперативно реагувати на фішингові атаки та зменшити їх вплив [68].

Існує кілька ефективних методів захисту від фішингу:

1. Будьте обережні з надісланими повідомленнями: Ніколи не натискайте на посилання або не завантажуйте файли з надісланих повідомлень, які виглядають підозріло. Якщо повідомлення виглядає небезпечним або містить незвичайну пропозицію, краще уникати кліку на посилання та негайно видалити повідомлення.

2. Перевіряйте адресу веб-сайту: Перед введенням особистих даних на веб-сайті перевірте його адресу, щоб переконатися, що він є легітимним. Зловмисники часто створюють подібні веб-сайти, щоб перехопити ваші особисті дані.

3. Використовуйте паролі, які важко вгадати: Використовуйте складні паролі, які складаються з букв, цифр та спецсимволів. Ніколи не використовуйте ті ж самі паролі на різних веб-сайтах.

4. Використовуйте двофакторну аутентифікацію: Двофакторна аутентифікація - це додатковий рівень захисту, що забезпечується через надсилання коду підтвердження на ваш мобільний телефон або інший пристрій. Це забезпечує більший рівень безпеки в разі витоку пароля.

5. Встановлюйте антивірусне програмне забезпечення: Антивірусне програмне забезпечення допомагає виявляти шкідливе програмне забезпечення та зловмисні посилання на веб-сайтах.

6. Регулярно оновлюйте програмне забезпечення: Регулярне оновлення програмного забезпечення може допомогти запобігти використанню вразливостей в програмах зловмисниками.

Методи захисту від фішингу - це різноманітні техніки та заходи, які використовуються для запобігання атакам фішингу та зменшення їхнього впливу. Фішинг - це вид кібератак, при якому зловмисники використовують

підроблені повідомлення або веб-сторінки для шахрайства, отримання доступу до конфіденційної інформації або злому систем безпеки.

Методи захисту від фішингу можуть включати як технічні, так і не технічні заходи. До технічних методів можуть відноситися використання програмного забезпечення для виявлення фішингових повідомлень та блокування їх, перевірка пошти на наявність підозрілих повідомлень, застосування двофакторної аутентифікації для забезпечення додаткового рівня безпеки облікових записів та інші.

Не технічні методи можуть включати навчання співробітників про ризики фішингу та методи його розпізнавання, створення культури безпеки, де співробітники можуть вільно обговорювати питання безпеки та повідомляти про підозрілі повідомлення, а також регулярну перевірку та поновлення політик безпеки компанії.

Загалом, методи захисту від фішингу мають на меті запобігти витоку конфіденційної інформації, захистити компанії та їхніх співробітників від кібератак та збільшити загальний рівень безпеки.

Захист від фішингу може бути складним завданням, оскільки зловмисники можуть використовувати різні техніки та тонкощі, щоб переконати жертву відкрити небезпечний файл або ввести свої конфіденційні дані на фішинговій сторінці [69].

Зокрема, нейролінгвістичні методи можуть зробити фішингове повідомлення ще більш переконливим та складним до виявлення. Наприклад, зловмисники можуть використовувати мовні прийоми, які збільшують шанси, що жертва буде відкривати посилання або завантажувати файл.

Однак, знання та застосування кількох простих правил можуть значно зменшити ризик стати жертвою фішингу.

Фішингові атаки - це вид кібератак, що полягає в тому, що зловмисники намагаються отримати вашу особисту інформацію, таку як паролі, номери кредитних карток, соціальні мережі, електронну пошту та іншу конфіденційну

інформацію, шляхом використання підроблених веб-сторінок, електронних листів, повідомлень та інших засобів.

1. Захист від фішингу є дуже важливим, оскільки фішери можуть використовувати отриману інформацію для крадіжки вашої ідентичності, викрадення грошей з вашого банківського рахунку або для інших шахрайських дій. Нижче перераховані кілька причин, чому варто захиститися від фішингових атак:

2. Захист особистої інформації: Фішери можуть використовувати отриману інформацію для крадіжки вашої ідентичності або для доступу до ваших особистих інформаційних ресурсів. Якщо ваша особиста інформація потрапляє в руки зловмисників, це може призвести до серйозних наслідків.

3. Захист від шахрайства: Шахраї можуть використовувати отриману інформацію для крадіжки грошей з вашого банківського рахунку або для інших шахрайських дій. Якщо ви станете жертвою фішингової атаки, то зловмисники можуть використовувати ваші особисті дані для створення фальшивих документів або отримання кредитів.

4. Захист від вірусів та інших шкідливих програм: Фішингові атаки можуть бути використані для поширення вірусів.

Фішинг - це метод шахрайства, коли злочинці намагаються отримати конфіденційну інформацію, таку як паролі, номери кредитних карток, електронні адреси та інші особисті дані. Це робиться через надсилання листів електронної пошти, повідомлень в соціальних мережах та інших комунікаційних каналах, в яких шахраї виглядають як довірені відправники.

Існує багато методів захисту від кібератак, які можуть бути застосовані для захисту від різних типів загроз. Основні принципи методів захисту від кібератак такі:

1. Захист від зловмисних програм (антивіруси, антишпигунські програми, файрволи тощо): ці програми дозволяють виявляти та блокувати шкідливі програми, що можуть пошкодити комп'ютер, або викрасти конфіденційну інформацію.

2. Підвищення безпеки паролів та доступів: слабкі паролі та відсутність механізмів перевірки автентичності можуть стати вхідними воротами для кіберзлочинців. Підвищення складності паролів та двофакторна аутентифікація можуть значно зменшити ризик несанкціонованого доступу.

3. Резервне копіювання даних: регулярне створення резервних копій даних дозволяє відновити інформацію в разі її втрати або пошкодження.

4. Шифрування даних: шифрування даних може допомогти захистити конфіденційну інформацію від несанкціонованого доступу.

5. Оновлення програмного забезпечення: оновлення програмного забезпечення (операційної системи, браузера, додатків) є важливим для запобігання кібератак. Багато програмних оновлень містять виправлення вразливостей, які можуть бути використані кіберзлочинцями.

6. Контроль за мережевою активністю: моніторинг мережевої активності може допомогти виявити аномальні дії на мережі та вчасно вжити заходів для їх блокування [70].

Отже, щоб захистити себе від нейролінгвістичного фішингу, варто бути пильними та уважними, коли отримуєте повідомлення з проханням надати конфіденційну інформацію. Також варто перевіряти посилання, які включені в повідомлення, та убезпечувати свої облікові записи за допомогою сильних паролів та двофакторної аутентифікації.

РОЗДІЛ 4. РОЗРОБЛЕННЯ ЕЛЕКТРОННОГО ДОВІДНИКА

4.1 Особливості сайту, загальна інформація

Сайт "Нейролінгвістичні техніки в заголовках фішингових повідомлень" є інформаційно-просвітницьким ресурсом, присвяченим проблемі фішингу - виду інтернет-шахрайства, спрямованого на виманювання конфіденційних даних користувачів.

Особливістю сайту є його вузька спеціалізація на аналізі заголовків фішингових повідомлень з точки зору використання в них нейролінгвістичних технік для маніпулювання увагою і емоціями потенційних жертв. Такий підхід дозволяє детально розкрити одну з ключових складових фішингу і допомогти користувачам краще розпізнавати шахрайські листи.

Сайт має освітню і попереджувальну мету - він прагне підвищити обізнаність людей про загрозу фішингу, навчити основним ознакам фішингових повідомлень і дати практичні поради з безпеки.

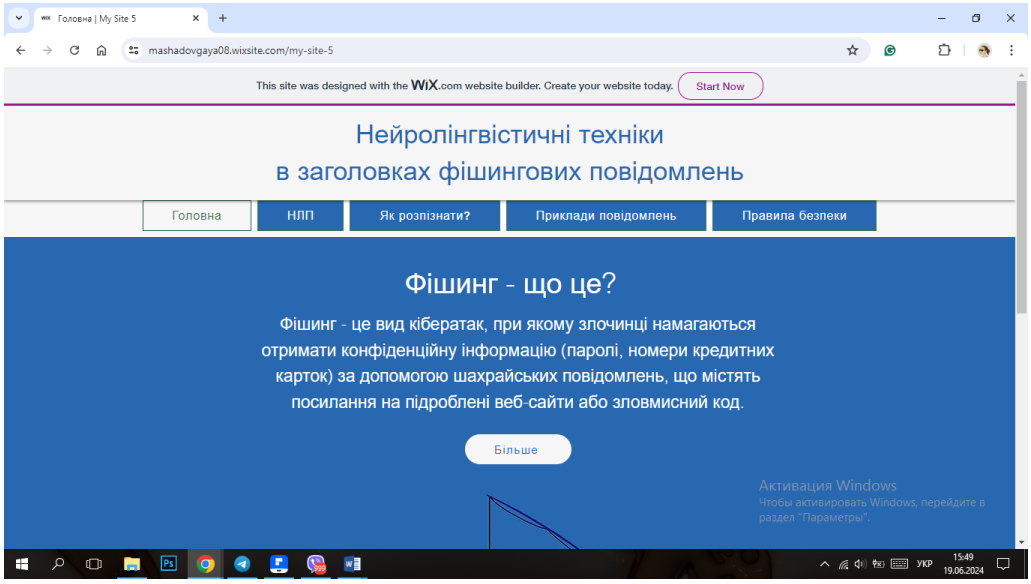
Матеріали сайту будуть корисні як пересічним інтернет-користувачам, так і фахівцям з інформаційних технологій і кібербезпеки. Використання реальних прикладів фішингових листів робить інформацію більш наочною і практично застосовною.

Сайт має міждисциплінарний характер, який поєднує знання з інформаційної безпеки, лінгвістики і психології для всебічного висвітлення проблеми фішингу.

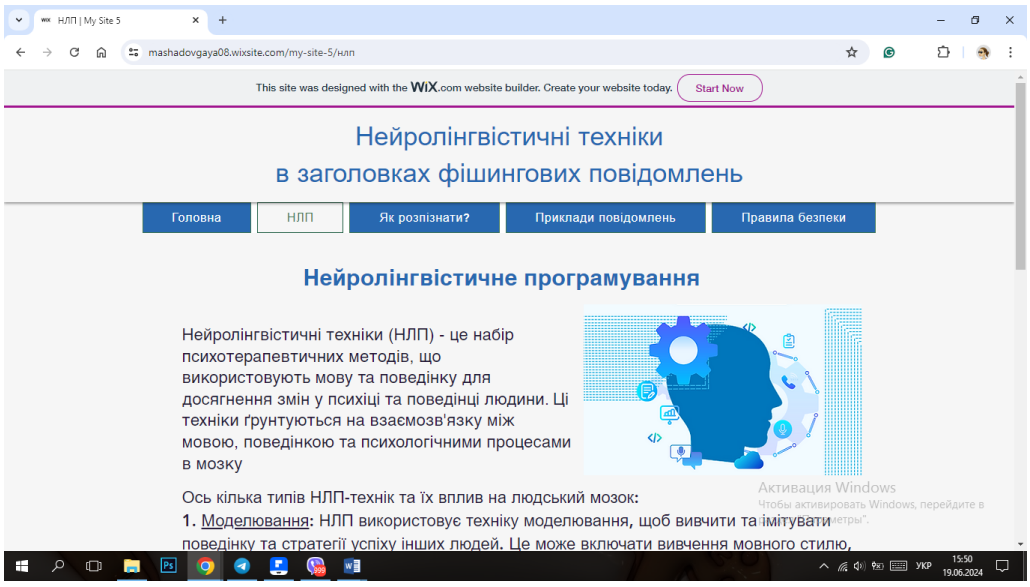
4.1 Модель сайту, його характеристики

Сайт має лаконічний і функціональний дизайн, орієнтований на зручність сприйняття інформації. Головне меню дозволяє швидко отримати доступ до основних розділів: загальних відомостей про фішинг, опису нейролінгвістичних технік в фішингових повідомленнях, порад з розпізнавання фішингу, прикладів реальних фішингових листів і правил кібербезпеки.

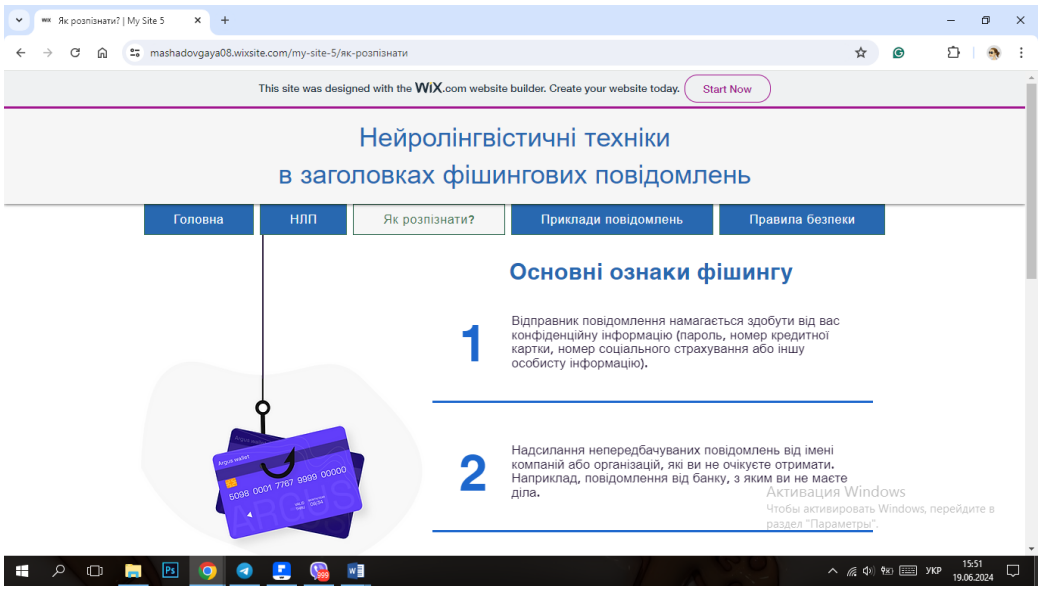
На головній сторінці відвідувач відразу бачить стислий опис проблеми фішингу і три ключові ознаки фішингових повідомлень з іконками, що формує загальне розуміння теми сайту.



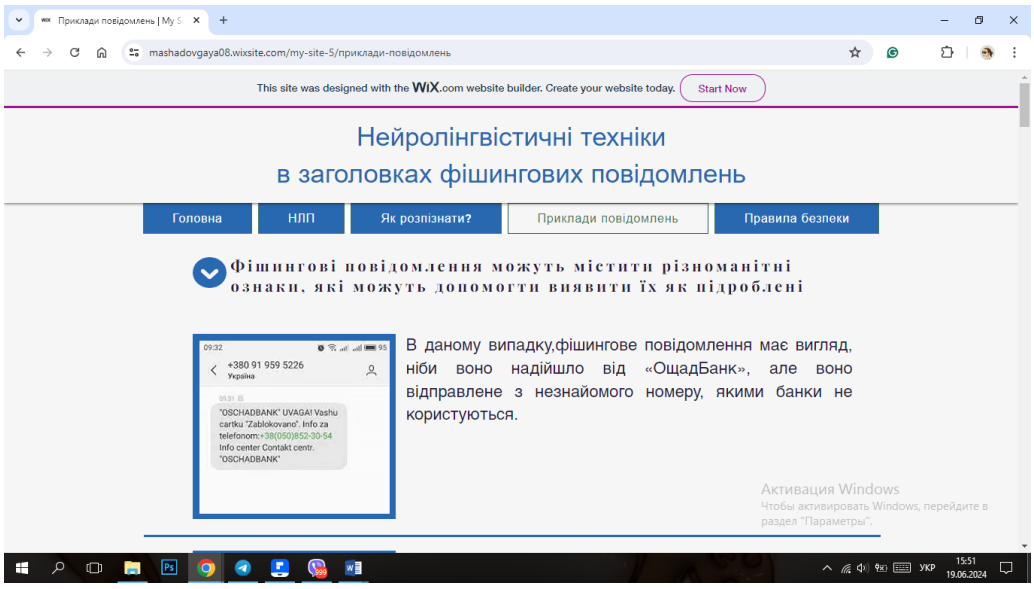
Розділ "НЛП" детально пояснює, які нейролінгвістичні техніки найчастіше використовуються шахраями для психологічного впливу на отримувачів листів.



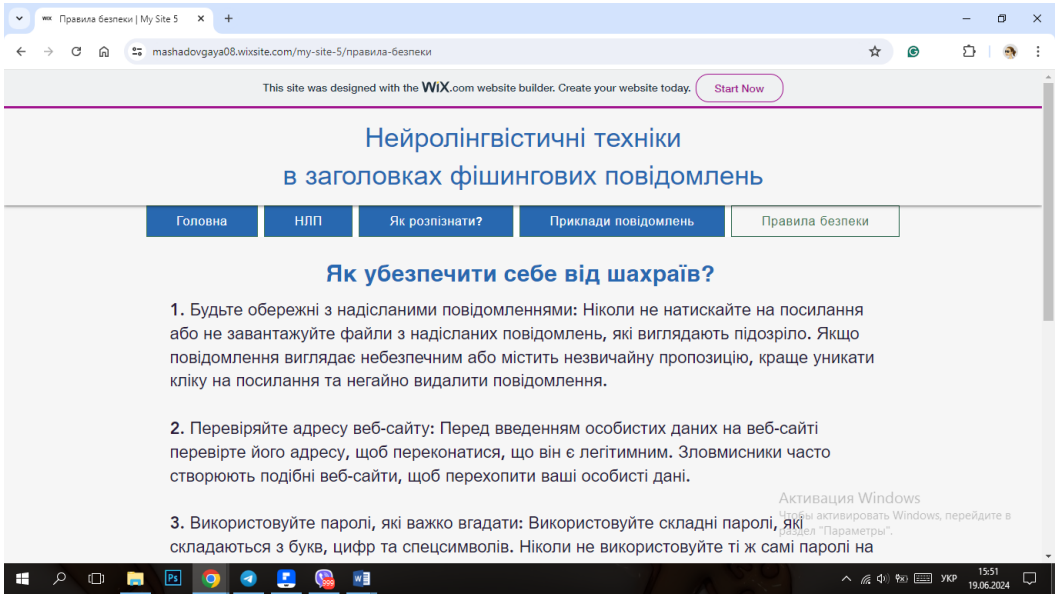
В розділі "Як розпізнати?" користувач знайде докладну інструкцію з виявлення підозрілих ознак фішингових повідомлень, як технічних, так і змістовних.



"Приклади повідомлень" наочно ілюструють застосування маніпулятивних технік на практиці, демонструючи скріншоти реальних фішингових листів з поясненнями.



Розділ "Правила безпеки" містить загальні рекомендації як з розпізнавання фішингу, так і з безпечної роботи в інтернеті в цілому.



Сайт не перевантажений зайвою інформацією, зберігає чіткість структури і фокус на головній темі. Він може слугувати як довідковим матеріалом для самоосвіти, так і наочним посібником для використання на курсах і тренінгах з інформаційної безпеки.

В цілому, сайт є вузькоспеціалізованим, практично орієнтованим освітнім інтернет-ресурсом, який ефективно поєднує якісний контент, продуману структуру і ергономічний дизайн для досягнення своєї мети - навчання користувачів протистояти фішинговим атакам.

ВИСНОВКИ

Нейролінгвістичні техніки можуть бути використані для створення заголовків фішингових повідомлень, що мають на меті обману людей і викрадення їх особистої інформації або грошей.

За допомогою нейролінгвістичних технік, зловмисники можуть підібрати слова та вирази, які максимально ефективно сприятимуть психологічному впливу на людей. Наприклад, вони можуть використовувати заголовки зі словами "увага", "невідкладно" або "важливо", щоб викликати паніку і термінову реакцію.

Однак, зловмисники не залежать виключно від нейролінгвістичних технік. Вони також використовують і інші методи маніпулювання, такі як використання логотипів відомих компаній, емоційних звернень та інші.

Отже, важливо бути обережним і не довіряти будь-якій електронній пошті або повідомленню, яке виглядає підозріло або надто натискає на швидку реакцію. Варто перевіряти автора повідомлення, не клікати на посилання в ньому та не вводити особисту інформацію.

Аналіз фішингових повідомлень є важливим елементом боротьби з кіберзлочинністю. Фішинг-атаки є одними з найпоширеніших видів кібератак, що спрямовані на отримання конфіденційної інформації, такої як паролі, номери кредитних карток та інші особисті дані.

Під час аналізу фішингових повідомлень необхідно звернути увагу на кілька ключових моментів. Серед них:

- Адреса електронної пошти відправника повідомлення;
- Назва та текст повідомлення;
- Посилання, які містяться в повідомленні;
- Запити, що містяться в повідомленні.

Аналізуючи ці фактори, можна виявити ознаки фішингового повідомлення та визначити його достовірність.

Крім того, важливо розуміти, що фішингові атаки постійно змінюються та вдосконалюються. Тому потрібно не тільки знати, як розпізнати фішинг, але і вести постійний моніторинг нових методів атак та вдосконалювати заходи безпеки.

В цілому, аналіз фішингових повідомлень є важливим елементом кібербезпеки, який допомагає зменшити ризики втрати конфіденційної інформації та запобігти фінансовим втратам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бахрушин В.Є. Методи аналізу даних : навчальний посібник для студентів /. В.Є. Бахрушин. – Запоріжжя : КПУ, 2011. – 268 с.
2. Войтович О. П., Ювковецький О. С. Класифікація вразливостей Webресурсів [Електронний ресурс] / О. П. Войтович, О. С. Ювковецький. – Режим доступу: http://itce.pu.if.ua/files/topics/VoytovychYuvkovetskyi.pdf
3. Литвинов В.В. Петрі-об’єктна модель системи управління розподіленими обчислювальними ресурсами / В.В. Литвинов, І.В. Стеценко // Тези доповідей Міжнародної науково-практичної конференції „Інформаційні технології в освіті, науці і техніці”(ІТОНТ2012): Черкаси, 25-27 квітня 2012р. – У 2 т. – Черкаси: ЧДТУ, 2012. – Т.1. – С.33-34.
4. Моделювання та аналіз безпеки розподілених інформаційних систем : М74 навч. посіб. [для студ. спец. 121 «Інженерія програмного забезпечення»] / В. В. Литвинов, В. В. Казимир, І. В. Стеценко та ін. – Чернігів : Чернігів. нац. технол. ун-т, 2016. – 254 с.
5. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»
6. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»
7. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»
8. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»
9. Петрі - об’єктна модель поширення кібератак в РІС. Стеценко І.В. – С 4. [Електроний ресурс], режим доступу - http://simulation.su/uploads/files/default/2018-litvinov-stecenko.pdf.

10. Постанова Кабінету міністрів України №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006
11. Про електронні документи та електронний документообіг [Електронний ресурс] : закон України від 22.05.2003 № 851-IV. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/8515.
12. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : закон України від 05.07.1994 № 80/94-ВР. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-вр.
13. Про захист персональних даних . [Електронний ресурс] : закон України від 01.06.2010 № 2297-VI. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-51.
14. Про інформацію [Електронний ресурс] : закон України від 02.10.1992 № 2657-XII. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12.
15. Сервер - Вікіпедія [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80.
16. Стеценко И.В. Алгоритм імітації Петрі-об'єктної моделі / І.В. Стеценко // Математичні машини і системи. – Київ, 2012. - №2 . №1 . – С.154-165.
17. Яіцький А. О. Ефективні методи та засоби захисту фішингових атак / А. О. Яіцький, М. Г. Сахаров. – Варшава: Problems of science and practice, tasks and ways to solve them. – 2022. – С. 417-419.
18. Яіцький А. О. Застосування хмарних технологій в космосі / А. О. Яіцький, М. Г. Сахаров. – Київ: Priority directions of science and technology development. – 2021. – С. 337-339.
19. 2022 SonicWall cyber threat report. [Електронний ресурс] / Bill Conner // SonicWall. – 2022. – Режим доступу до ресурсу: https://www.infopointsecurity.de/media/2022-sonicwall-cyber-threat-report.pdf.
20. Abonormal Security Quarterly BEC Report. [Електронний ресурс] / Evan Reiser // Abnormal Security. – 2020. – Режим доступу до ресурсу:

https://info.abnormalsecurity.com/rs/231IDP139/images/AS_Qtrly_BEC_Report_Q3_2 020.pdf.

21. Aggarwaly, A., Rajadesingan, A. and Kumaraguru, P., 2012. PhishAri:Automatic Realtime Phishing Detection on Twitter, Seventh IEEE APWG eCrime Researchers Summit (eCRS), Las Croabas, Puerto Rico, pp. 22-25, Available at: , (Accessed 25 November 2016)
22. An Article of a Follow-up Study of Detecting Phishing Emails. [Електронний ресурс] / Ernst Bekkering, Dan Hutchison, Laurie Werner // Researchgate. – 2015. – Режим доступу до ресурсу: https://www.researchgate.net/profile/ErnstBekkering/publication/267705517_A_Follow up_Study_of_Detecting_Phishing_Emails/links/557ed71608aeb61eae260c2f/A-Followup-Study-of-Detecting-Phishing-Emails.pdf.
23. An Article of Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection. [Електронний ресурс] / Abdullah Alnajim, Malcolm Munro // Researchgate. – 2009. – Режим доступу до ресурсу: https://www.researchgate.net/publication/220841443_An_AntiPhishing_Approach_that _Uses_Training_Intervention_for_Phishing_Websites_Detection.
24. Anil K. Jain with RadhaChitta and Rong Jin, Clustering Big Data: Department of Computer Science Michigan State University, 2012
25. Arachchilage, N. A. G. (2015). User-Centred Security Education: A Game Design to Thwart Phishing Attacks. arXiv preprint arXiv:1511.03459.
26. Cerrito PB: Introduction to Data Mining Using SAS Enterprise Miner, SAS Institute Inc., 2008.
27. Cost of a Data Breach Report 2021 [Електронний ресурс] // IBM Security. – 2020. – Режим доступу до ресурсу: https://www.ibm.com/downloads/cas/OJDVQGRY.
28. CSS - Вікіпедія [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/CSS.

29. DBIR 2021 Data Breach Investigation Report [Електронний ресурс] // Verizon. – 2021. – Режим доступу до ресурсу: https://www.verizon.com/business/resources/reports/2021-data-breach-investigationsreport.pdf.
30. Deanna D. Caputo, Shari Lawrence Pfleeger, Jesse D. Freeman, M. Eric Johnson. Going Spear Phishing: Exploring Embedded Training and Awareness / D. Deanna Caputo, Pfleeger Lawrence Shari, Freeman D. Jesse, Johnson M. Eric // США: IEEE, 2013. – 38 с.
31. Denial of Service Attacks [Електронний ресурс] – Режим доступу: https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf
32. Detection of Phishing Attacks: A Machine Learning Approach. [Електронний ресурс] / Ram Basnet, Srinivas Mukkamala, Andrew H. Sung // Researchgate,2008. Режим доступу до ресурсу:https://www.researchgate.net/publication/226420039_Detection_of_Phishing_Attacks_A_Machine_Learning_Approach.
33. ECMAScript - Вікіпедія [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/ECMAScript.
34. FireEye, ―Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign‖, Available at: https://www.fireeye.com/blog/threatresearch/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
35. G. Bottazzi et al., "MP-Shield: A Framework for Phishing Detection in Mobile Devices", in Proceedings of the 3rd IEEE International Workshop on Cybercrimes and Emerging Web Environments, Liverpool, UK, October 2015.
36. G. Tally, R. Thomas, T. V. Vleck, ―Anti-Phishing : Best Practices for Institutions and Consumers‖ Mcafee research technical report, September 2004.
37. GARTNER. ―Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks‖, December 17,2007, available: ―http://www.gartner.com/it/page.jsp?id=565125‖

38. Google Safe Browsing Service of Google that helps protect devices. [Електронний ресурс] // Google. – 2022. – Режим доступу до ресурсу: https://transparencyreport.google.com/safe-browsing/overview.
39. How to Conduct Email Phishing Experiments. [Електронний ресурс] / Kaspar Jüristo // Computer Science. – 2018. – Режим доступу до ресурсу: https://1library.net/document/q7x98rky-how-to-conduct-email-phishingexperiments.html.
40. HTML - Вікіпедія [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/HTML.
41. HTTP - Вікіпедія [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/HTTP.
42. International Intellectual Property Alliance Special Report 2016 [Електронний ресурс]. – Режим доступу: http://www.iipawebsite.com/
43. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ―Internet of Things (IoT): A vision, architectural elements, and future directions,‖ Future Generation Computer Systems, vol.29, no.7, pp. 1645–1660, 2013.
44. Jiawei Han, Micheline Kamber, Jian Pei. Data Mining: Concepts and Techniques, 2012
45. K. A. Abdul Nazeer, M. P. Sebastian. Improving the Accuracy and Efficiency of the k-means Clustering Algorithm, London, U.K, 2009
46. K. Munivara Prasad, A. Rama Mohan Reddy, K. Venugopal Rao. DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms – A Survey [Електронний ресурс] – Режим доступу: https://globaljournals.org/GJCST_Volume14/3-DoS-and-DDoS-Attacks-DefenseDetection.pdf
47. Kirlappos, I. and Sasse, M.A., 2012. Security education against phishing: A modest proposal for a major rethink. IEEE Security and Privacy Magazine, 10(2), pp.24- 32.
48. Krieg, G.and Kopan, T. 2016. CNN News, Is this the email that hacked John Podesta's account?, Available at: , (Accessed 19 November 2016)

49. Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F. and Hong, J., 2007. Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer, APWG eCrime Researchers Summit, 4-5October 2007, Pittsburgh, PA, USA.
50. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. and Hong, J., 2008. Lessons from a real world evaluation of anti-phishing training, eCrime Researchers Summit, 15-16 October, pp.1–12
51. Madan Lal Bhasin. Data Mining:A Competitive Tool in the Banking and Retail Industries, The Chartered Accountant October, 2006.
52. Madhav P. Namdev. Phishing Attacks and Detection / P. Namdev Madhav - Англія:, LAP Lambert Academic Publishing, 2015. – 68 с.
53. Marforio, C., Masti, R.J., Soriente, C., Kostiainen, K. and Capkun, S., 2016, October. Hardened Setup of Personalized Security Indicators to Counter Phishing Attacks in Mobile Banking. In Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices (pp. 83-92). ACM.
54. Matthew L Cole. The Complete Guide to Patents, Copyrights, and Trademarks: What You Need to Know Explained Simply. / Cole L Matthew // США: Atlantic Publishing Group Inc., 2008. – 288 с.
55. MongoDB - Вікіпедія [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/MongoDB.
56. Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh, and John C. Mitchell, ―Client-side defence against web-based identity theft,‖ in NDSS. The Internet Society, 2004.
57. Node.js - Вікіпедія [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Node.js.
58. Oluwatobi Ayodeji Akanbi, Iraj Sadegh Amiri, Elahe Fazeldehkordi: A Machine-Learning Approach to Phishing Detection and Defense. / Oluwatobi Ayodeji Akanbi, Iraj Sadegh Amiri, Elahe Fazeldehkordi // США: Syngress Media, 2015. – 100 с.

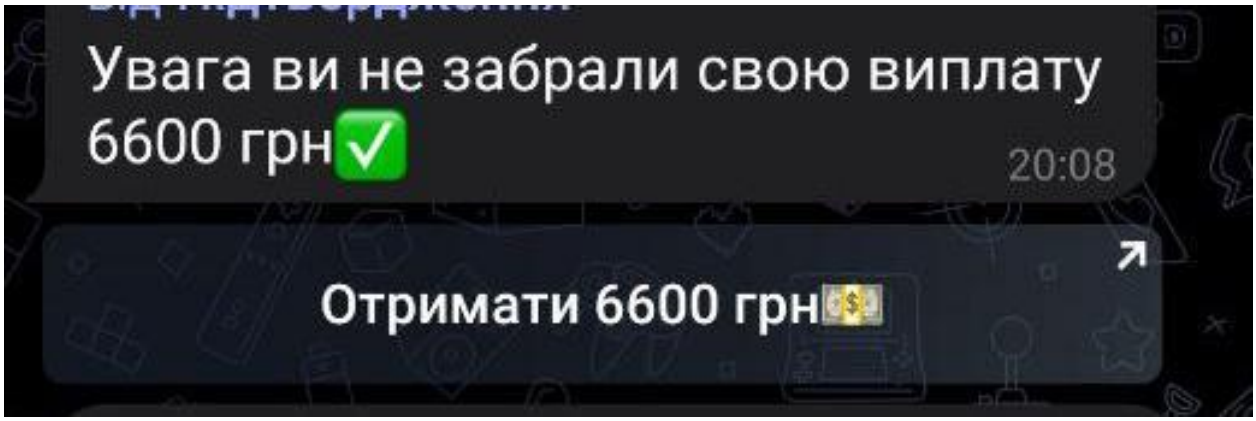
59. Rachna Dhamija, and J.D. Tygar, ―The Battle against Phishing - Dynamic Security Skins,‖ Proceeding SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security, PP 77 – 88, 2005.
60. Robust Email Security Requires Alignment Between Security Practitioners and Decision Makers [Електронний ресурс] // Osterman Research.– 2020. – Режим доступу до ресурсу: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWIy Sx.
61. SAS Enterprice Miner. Обзор решения [Електронний ресурс] – Режим доступу: https://www.sas.com/content/dam/SAS/ru_ru/doc/factsheet/sasenterprise-miner-04-04-2016.pdf 98
62. School of phish: A real-world evaluation of anti-phishing training. [Електронний ресурс] / Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, Theodore Pham // DBLP. – 2009. – Режим доступу до ресурсу:https://www.heinz.cmu.edu/~acquisti/papers/Acquisti_Rea lWorld_Evaluation_of_Anti-Phishing_Training.pdf.
63. Simon Haykin. Neural Networks and Learning Machines Third Edition – University Hamilton, Ontario, Canada, 2008. – 906 с.
64. Srivastava; B. B. Gupta; A. Tyagi; A. Shamn; A. Mishra, ―Recent Survey on DDoS Attacks and Defence Mechanisms,‖ Advances in Parallel Distributed Computing, Communications in Computer and Information Science, vol. 203, pp. 570-580.
65. The SSL Store: The 12 Most Costly Phishing Attack Examples [Електронний ресурс] // SSL Store. – 2021. – Режим доступу до ресурсу: https://www.thesslstore.com/blog/the-dirty-dozen-the-12-most-costly-phishing-attackexamples/.
66. The Top Five Security Threats to Your Banking Institution [Електронний ресурс]. – Режим доступу : http://www.level3.com/-

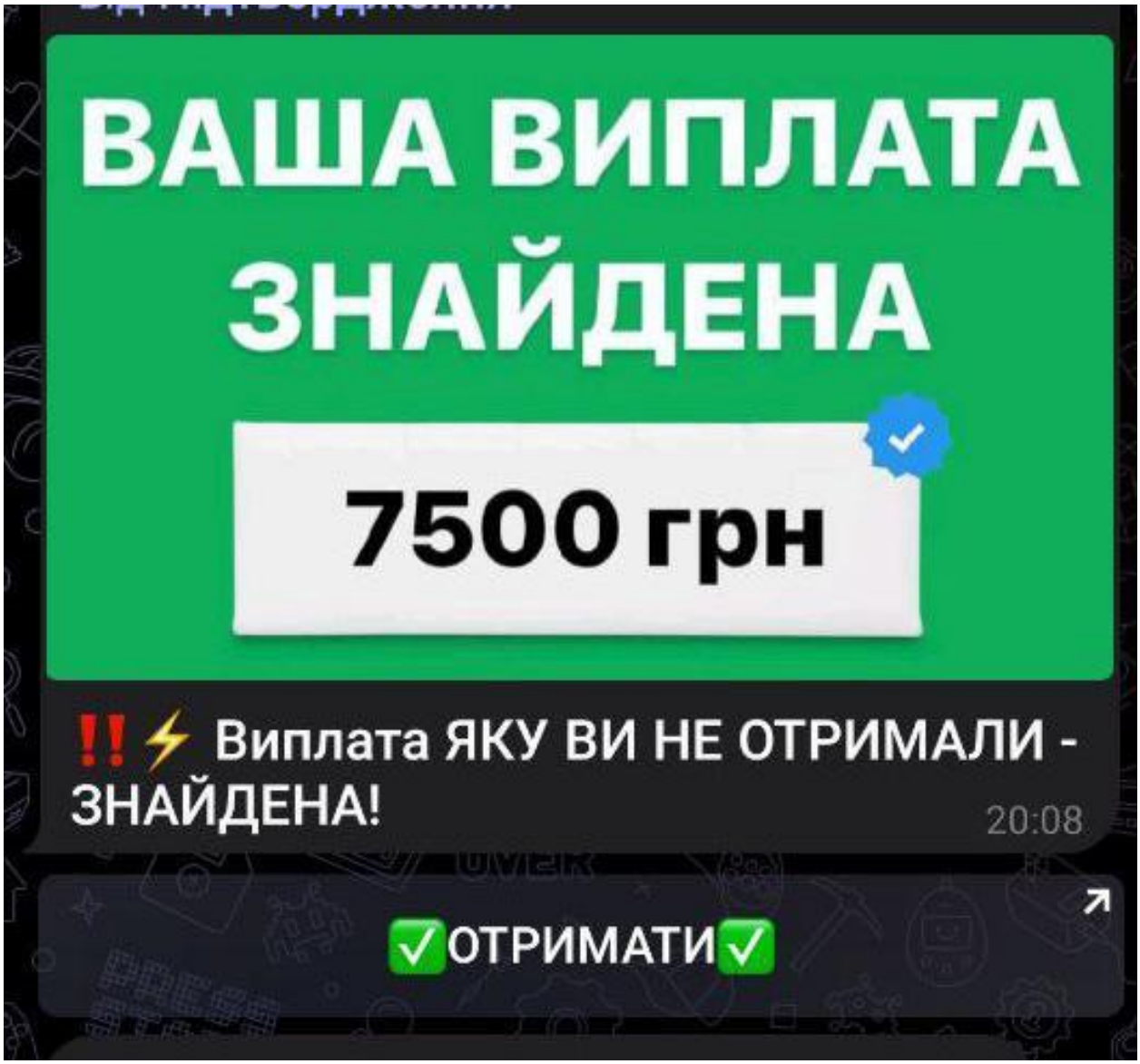
/media/files/infographics/en_infg_financialserv_topnetworksecuritythreats_regi ona lbanks.pdf

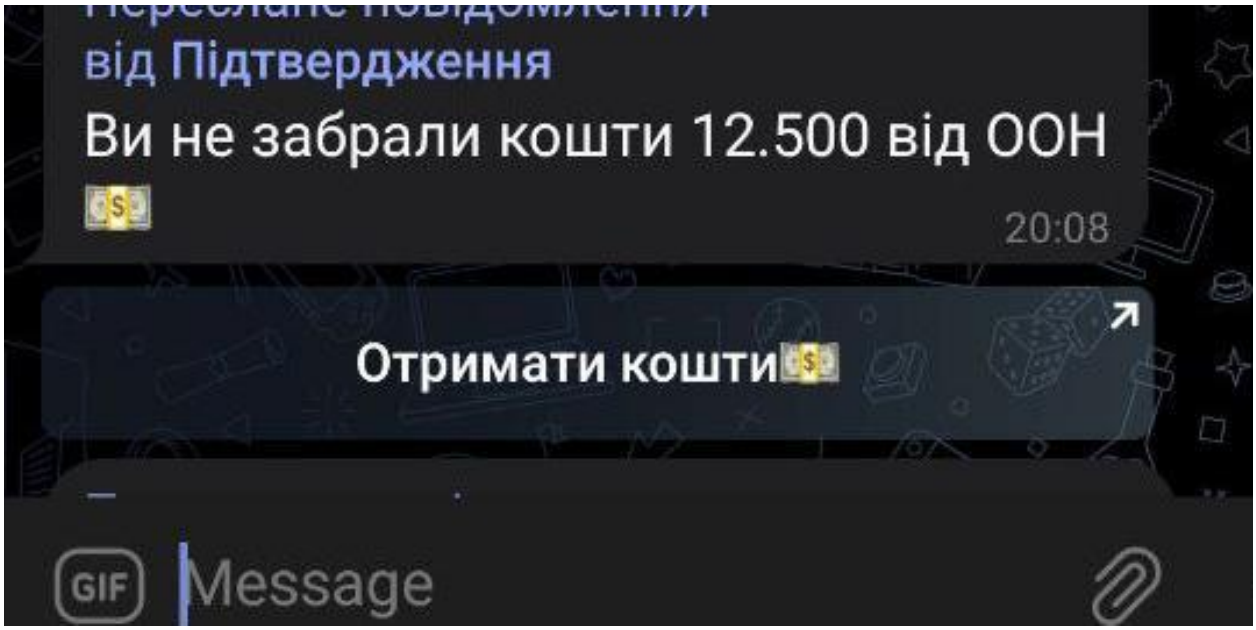
67. Trend Report «Financial Cyber Threats Q1 2017» conducted with Kaspersky Labs and Telefónica [Електронний ресурс]. – Режим доступу : http://www.level3.com//media/files/infographics/en_infg_financialserv_topnet wor ksecuritythreats_regionalbanks.pdf
68. Wu, M., Miller, R. and Garfinkel, S., 2005. Do Security Toolbars Actually Prevent Phishing Attacks?, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, Quebec, Canada, 22 - 27April 2006.
69. Wu, M., Miller, R. and Garfinkel, S., 2005. Do Security Toolbars Actually Prevent Phishing Attacks?, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, Quebec, Canada, 22 - 27April 2006.
70. Zhao, M., An, B. and Kiekintveld, C., 2016, February. Optimizing personalized email filtering thresholds to mitigate sequential spear phishing attacks. In Proceedings of the 30th AAAI Conference on Artificial Intelligence (AAAI).

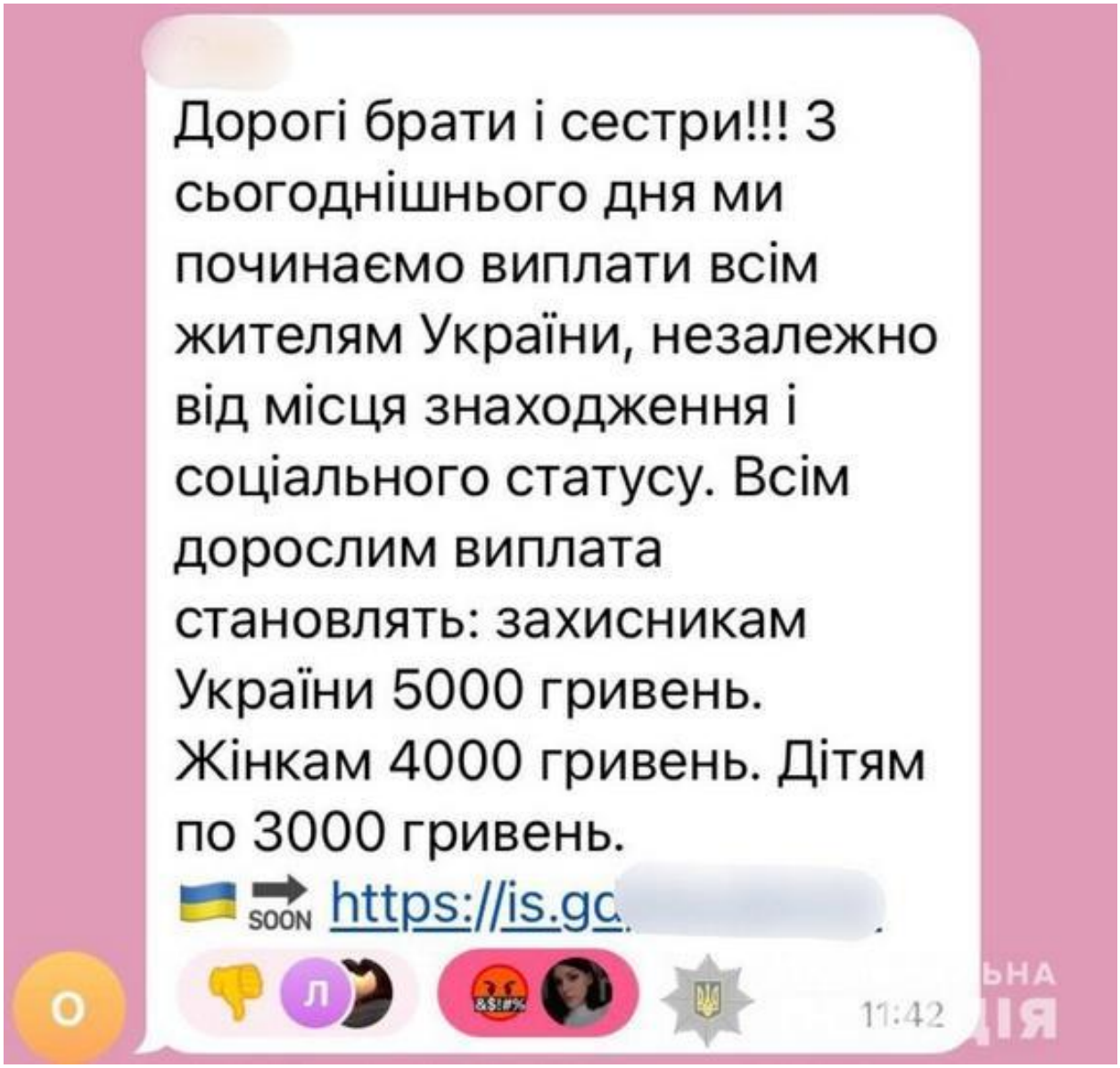
ДОДАТОК А

ПРИКЛАДИ ФІШИНГОВИХ ПОВІДОМЛЕНЬ






від Підтвердження
Ви не забрали кошти 12.500 від ООН
20:08
Отримати кошти
GIF
Message


Дорогі брати і сестри!!! З сьогоднішнього дня ми починаємо виплати всім жителям України, незалежно від місця знаходження і соціального статусу. Всім дорослим виплата становлять: захисникам України 5000 гривень. Жінкам 4000 гривень. Дітям по 3000 гривень.
SOON
https://is.gc
11:42

перемоги вже почався!

💣 Онлайн-казино Superboss експериментує з виграшами та розкидається ними в усі сторони.

💰 Бери участь у розіграші **Еліксир перемоги** та змагайся за призовий фонд 👉 *80 000 ₴*.

😎 Купуй білети, грай у слоти 🎰 та ставай одним із *50 переможців*.

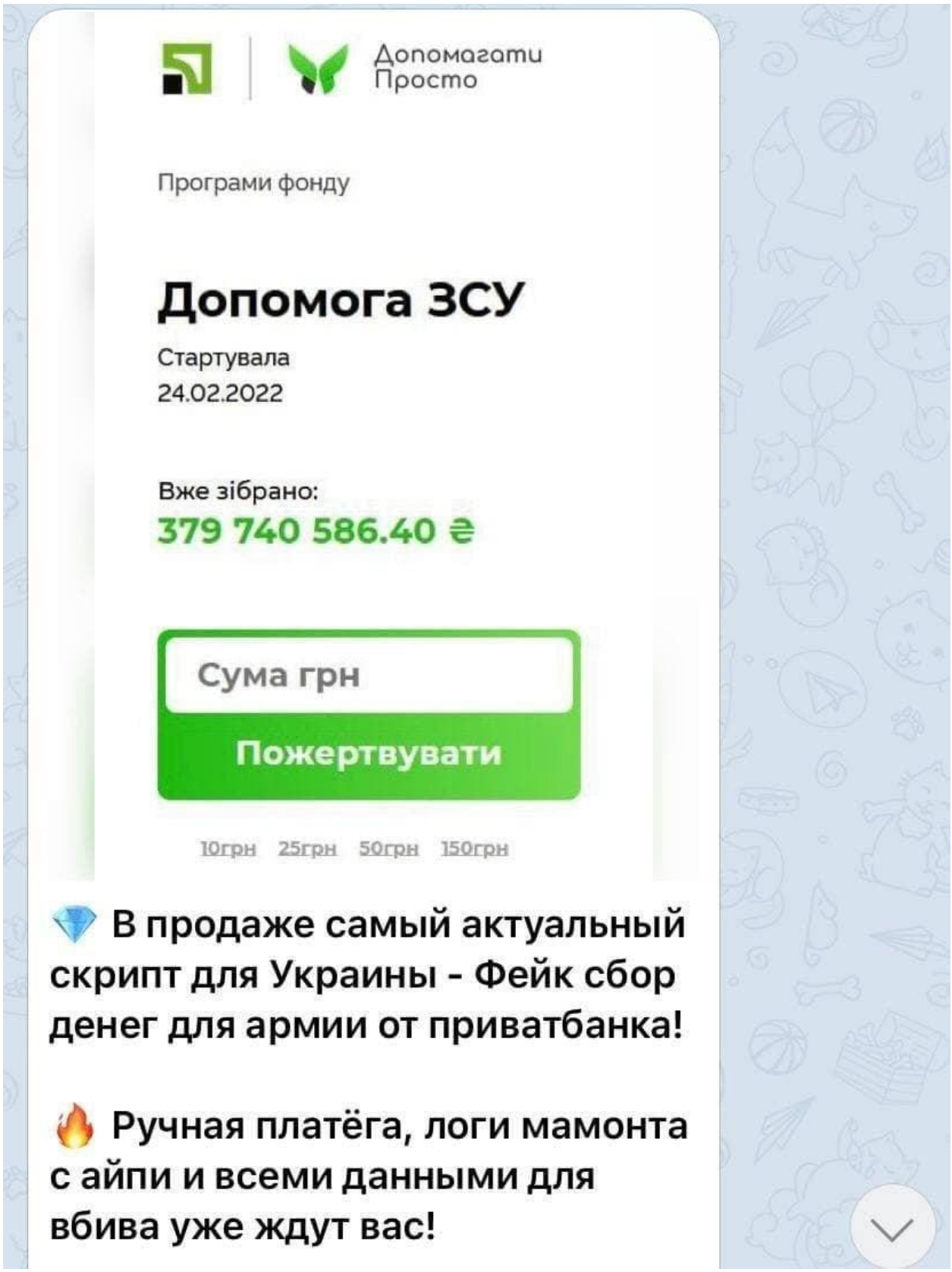
👌 І не забувай використовувати промокод **UA1BONUS**, щоб отримувати 👉 бонуси.

😎 Нові **бонуси та турніри** 🎁 від найкращих казино ти знайдеш у нашому боті CasinoBonus!

👍 15 🥰 2 ❤️ 1 😁 1 🤔 1 🤗 1

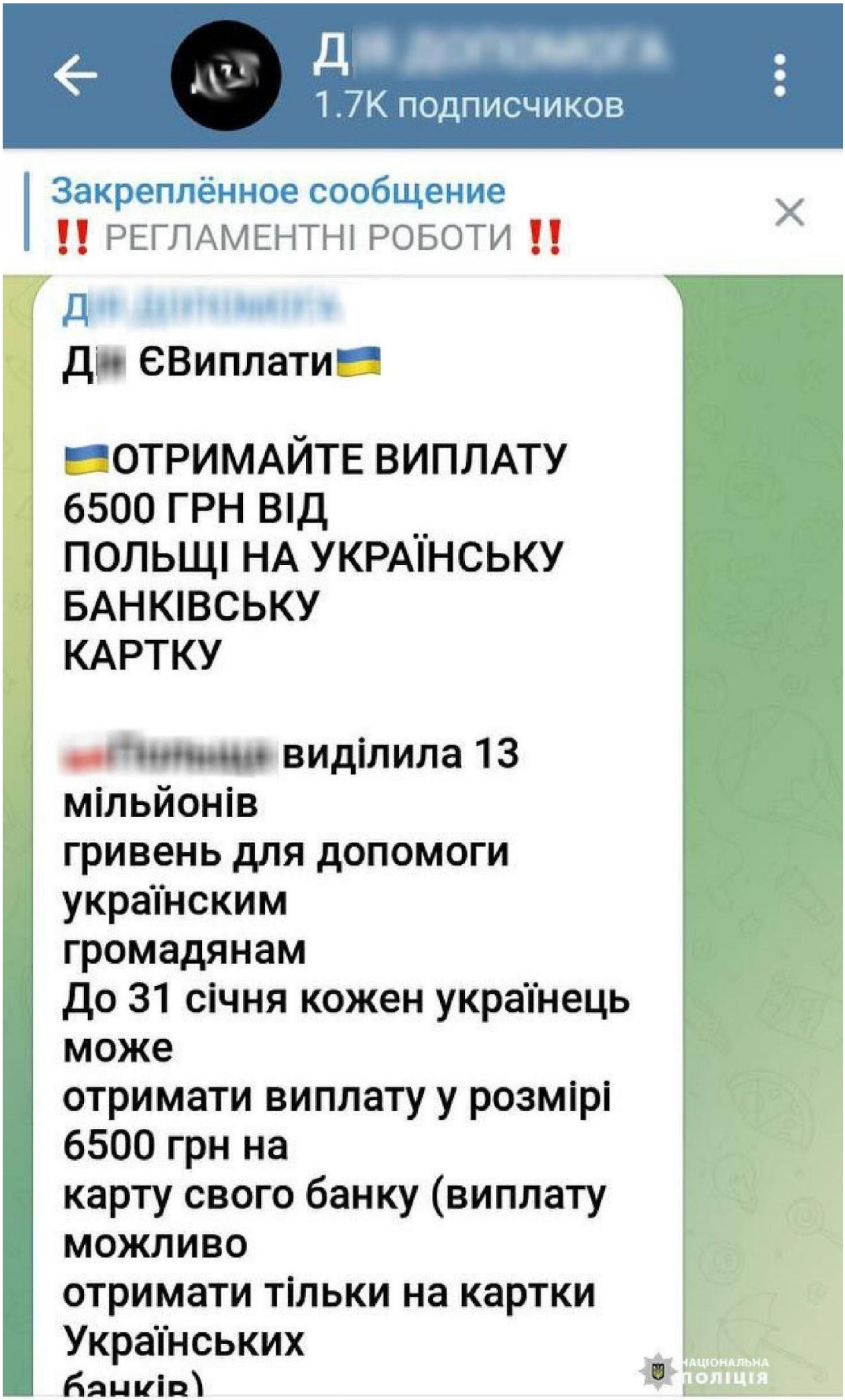
6.6K 21:03

До розіграшу 💸



💎 В продаже самый актуальный скрипт для Украины - Фейк сбор денег для армии от приватбанка!

🔥 Ручная платёга, логи мамонта с айпи и всеми данными для вбива уже ждут вас!


Д
1.7K подписчиков
Закреплённое сообщение
‼️ РЕГЛАМЕНТНІ РОБОТИ ‼️
Д ЄВиплати🇺🇦
🇺🇦ОТРИМАЙТЕ ВИПЛАТУ
6500 ГРН ВІД
ПОЛЬЩІ НА УКРАЇНСЬКУ
БАНКІВСЬКУ
КАРТКУ
виділила 13
мільйонів
гривень для допомоги
українським
громадянам
До 31 січня кожен українець
може
отримати виплату у розмірі
6500 грн на
карту свого банку (виплату
можливо
отримати тільки на картки
Українських
банків)
НАЦІОНАЛЬНА ПОЛІЦІЯ

Від Нова Пошта <fontich@rodant.com>
Тема **Повідомлення про відвантаження**
Кому undisclosed-recipients:;

Відповісти | Відповісти всім | Переслати | Більше
8:43

НОВА ПОШТА

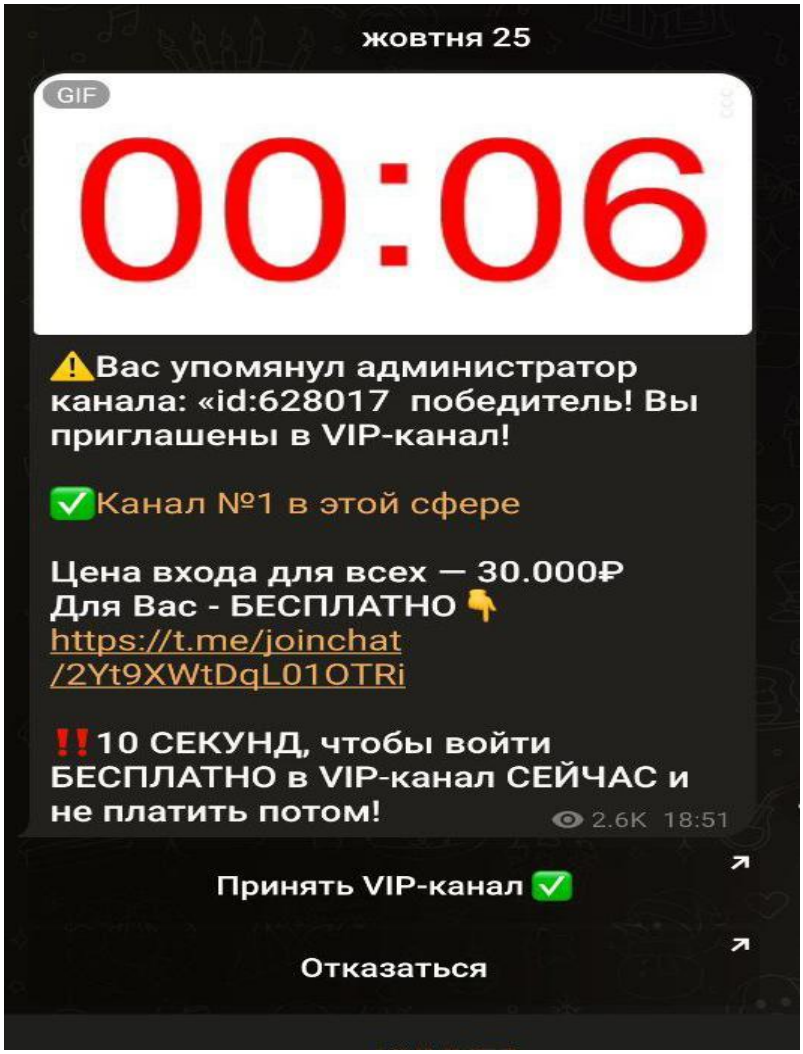
Ваш пакет відправляється

Планована дата доставки: субота, 19/06/2020
Це повідомлення надіслано, щоб повідомити, що ваш пакет оброблений для доставки. Клацніть посилання для відстеження нижче, щоб переглянути деталі доставки та перевірити фактичний стан транзиту вантажу.

Клацніть, щоб переглянути деталі відправлення та номер відстеження.

З щирою повагою
Нова Пошта
Московська, 46/2, Київ, Україна, 01001

Усі торговельні марки, торгові найменування або знаки обслуговування, що з'являються у зв'язку з «Новою Поштою», є власністю їх власників.



21.09.22

😎Привіт ПЕРЕМОЖЕЦЬ !!!
😎
🍋🤩🍋Прямо зараз ВАС ЧЕКАЄ БОНУС 10000 гривень на ПЕРШИЙ ДЕПОЗИТ🍋🤩🍋 !! - 👉 https://cutt.ly/tX58cpO?RXHM=cgv 👈 Забери 10000 гривень та 250 фріспінов на 🤑🤑 ПЕРШИЙ ДЕПОЗИТ 🤑🤑 при реєстрації за посиланням - 👉 https://cutt.ly/tX58cpO?RXHM=cgv 👈
🇺🇦 все буде Україна 🇺🇦

13:56

ПЕРЕВІРИТИ, чи містить це повідомлення спам

Українські ліцензійні казино🇺🇦

13 березня

🎰 Крути **Bonus Machine** в онлайн-казино Slots City та отримуй 🎁 подарунки.

💸 На тебе чекає **крутезна** машина з грошима 💰 та безкоштовними обертами.

💣 Отримати спіни можна **за 7-й, 14-й та 21-й депозити** 👌 *від 300 ₴*.

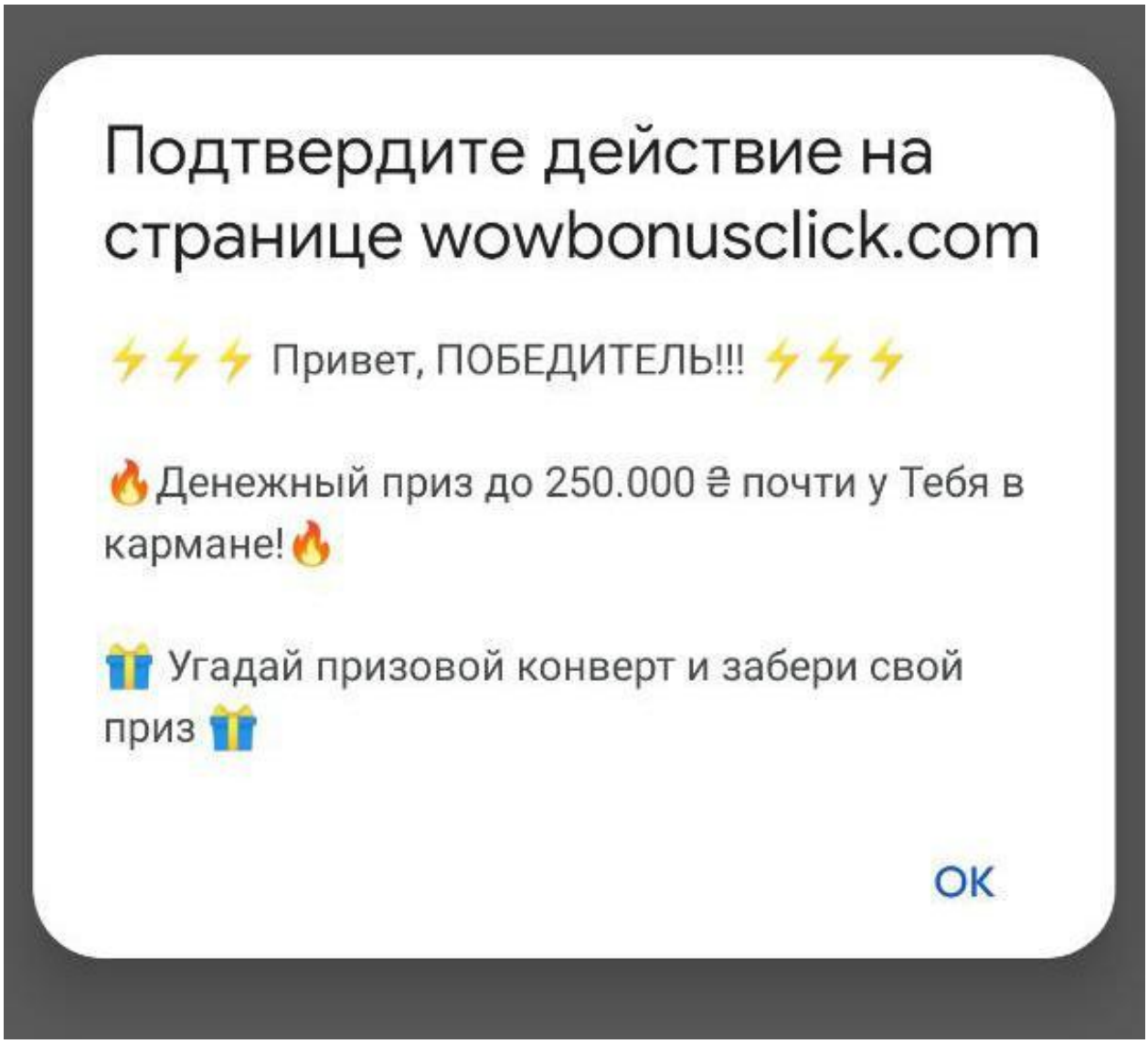
👉 **Перший** оберт дозволить виграти *від 100 ₴ до 2500 ₴*.
👉 **Другий** – *від 5 до 100* безкоштовних обертів.
👉 **Третій** – *від 100 ₴ до 10 000 ₴*.

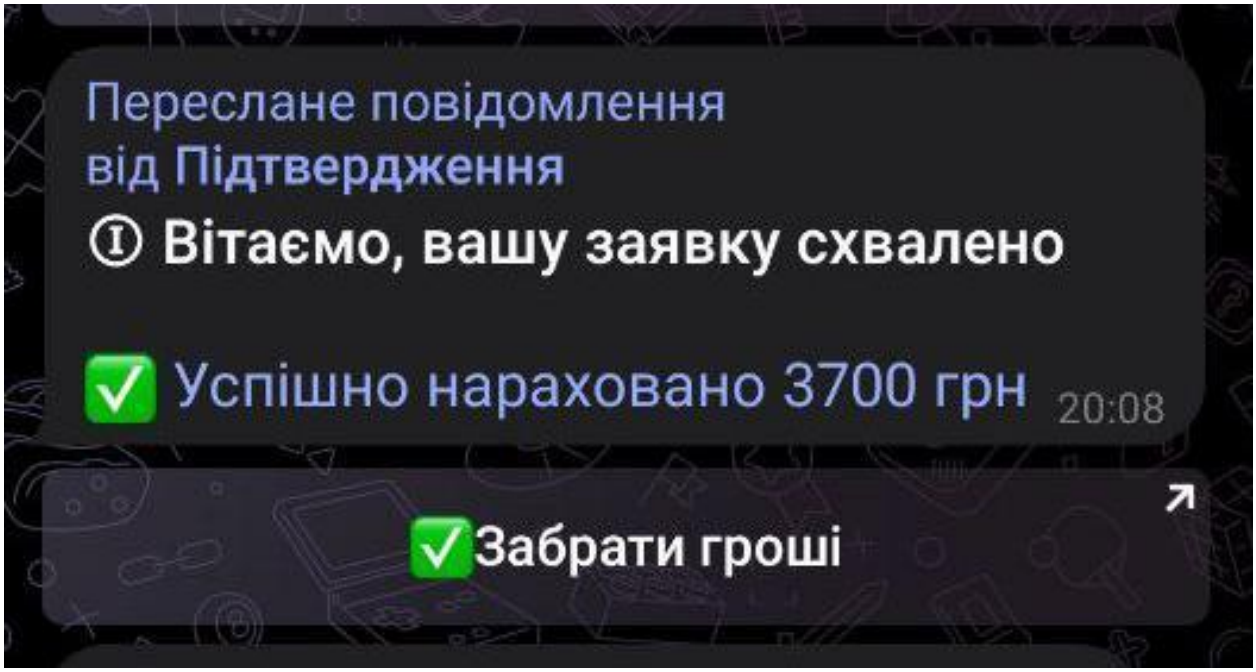
🎁 А якщо ти ще не зареєстрований у казино, використовуй промокод **CITY1**, щоб отримати бонус!

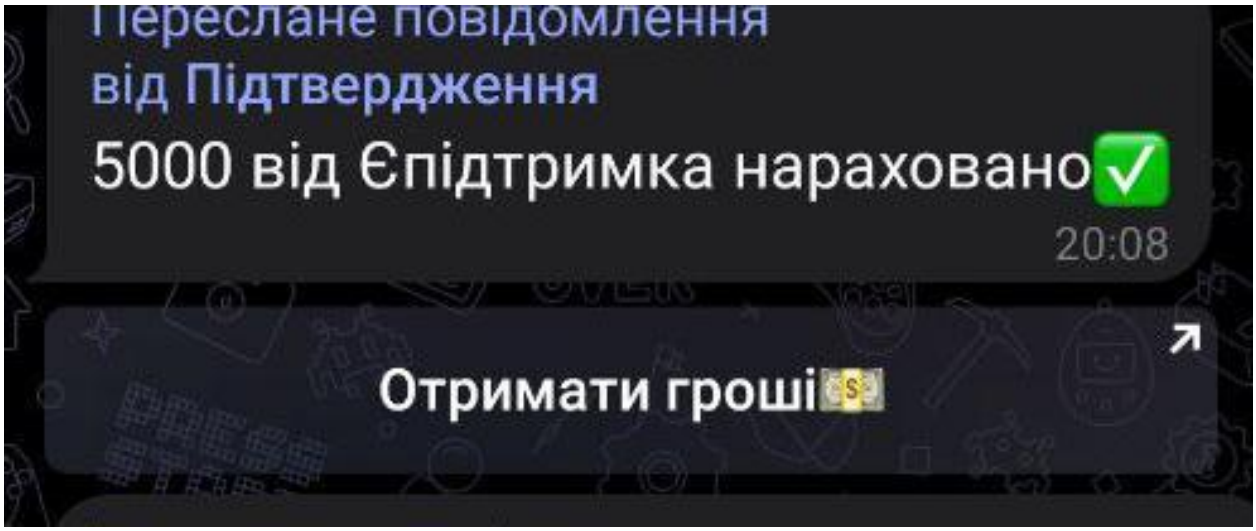
👍 14 ❤️ 3 👎 1

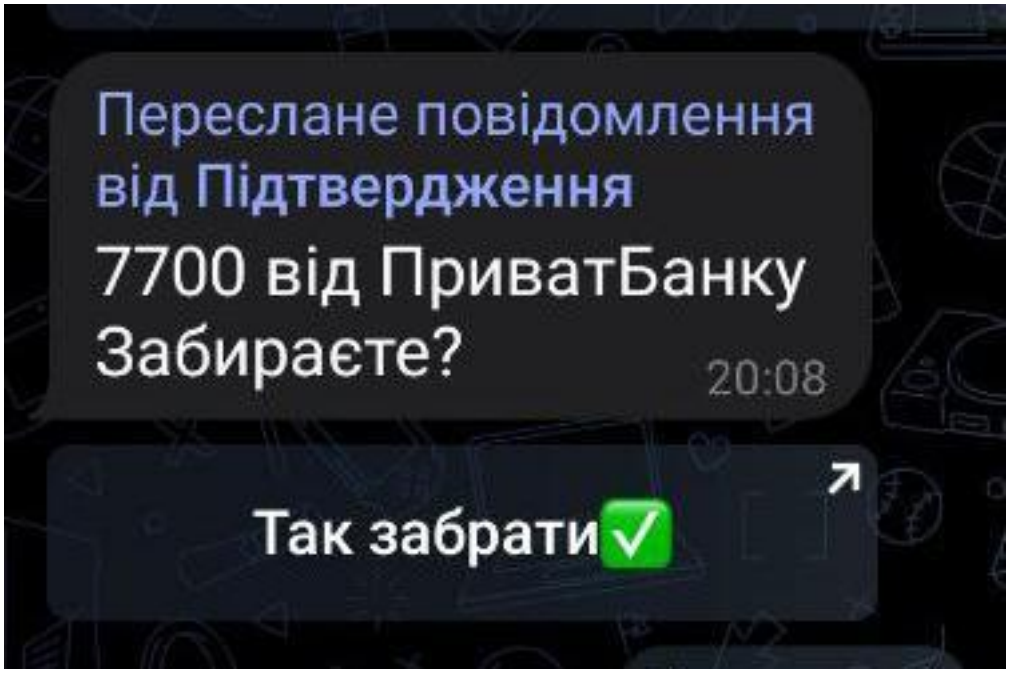
6.9K 17:00

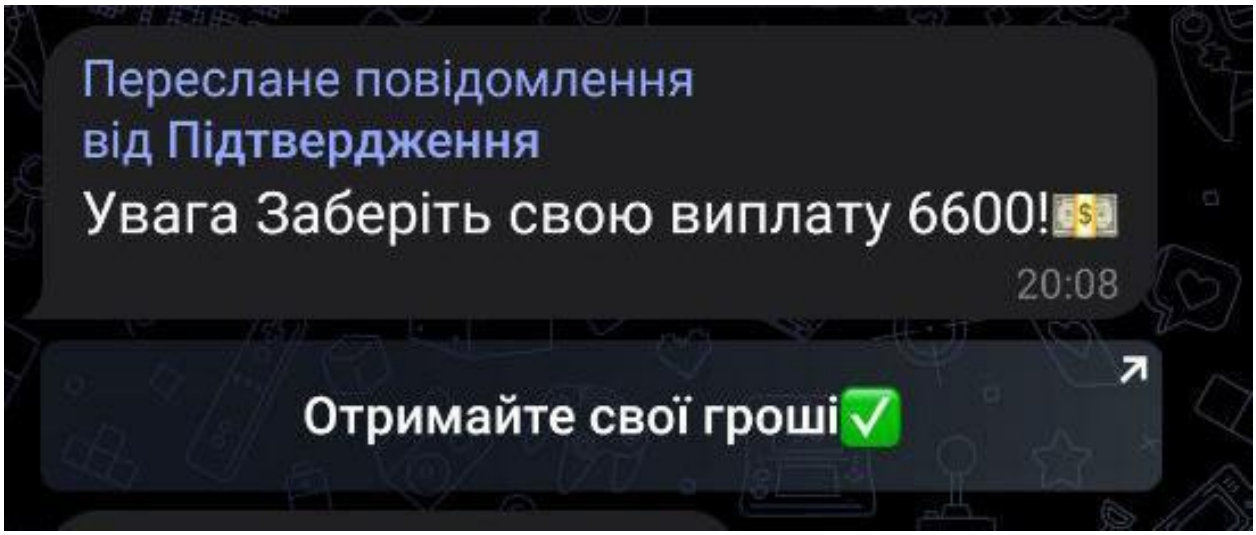
Bonus Machine 🚀

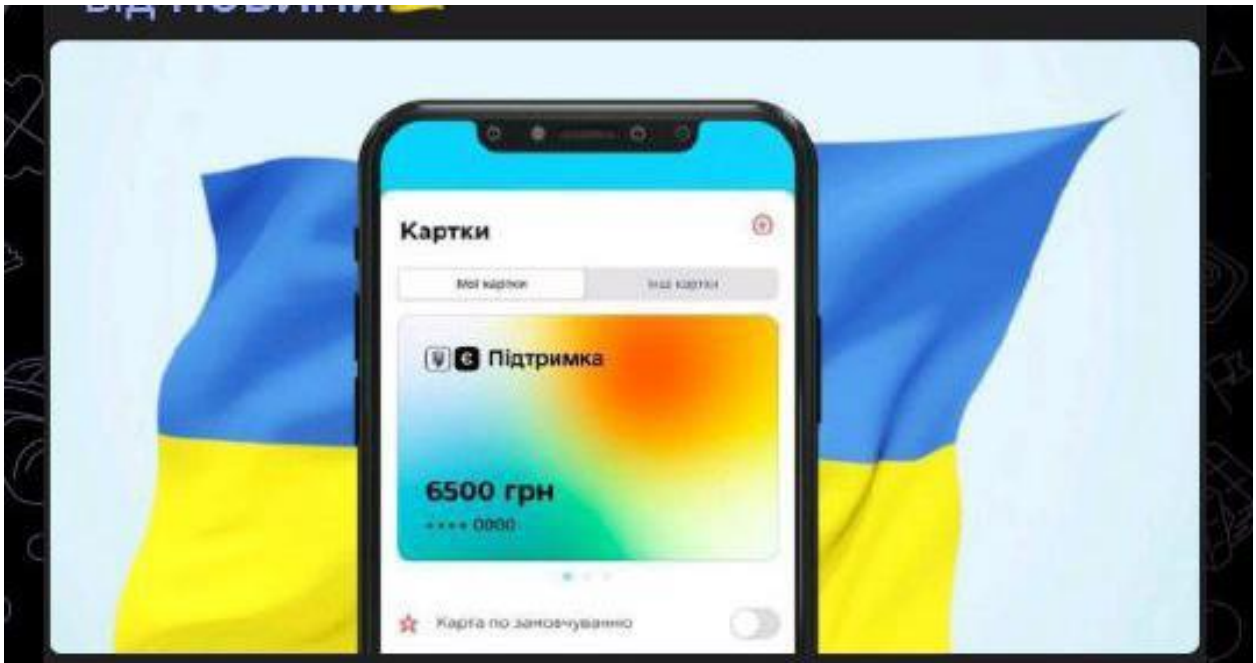

Подтвердите действие на странице wowbonusclick.com
⚡⚡⚡ Привет, ПОБЕДИТЕЛЬ!!! ⚡⚡⚡
🔥Денежный приз до 250.000 ₴ почти у Тебя в кармане!🔥
🎁 Угадай призовой конверт и забери свой приз 🎁
OK


Переслане повідомлення
від Підтвердження
ⓘ Вітаємо, вашу заявку схвалено
✅ Успішно нараховано 3700 грн 20:08
✅Забрати гроші


Переслане повідомлення
від Підтвердження
5000 від Єпідтримка нараховано✅
20:08
Отримати гроші💵


Переслане повідомлення
від Підтвердження
7700 від ПриватБанку
Забираєте?
20:08
Так забрати✅


Переслане повідомлення
від Підтвердження
Увага Заберіть свою виплату 6600!💵
20:08
Отримайте свої гроші✅



ⓘ На ваш акаунт єПідтримка можлива виплата 6 500.00 ₴

Вам доступна разова виплата в розмірі 6500 ‼️

Для отримання виплати оберіть свій банк.

⬇️⬇️⬇️

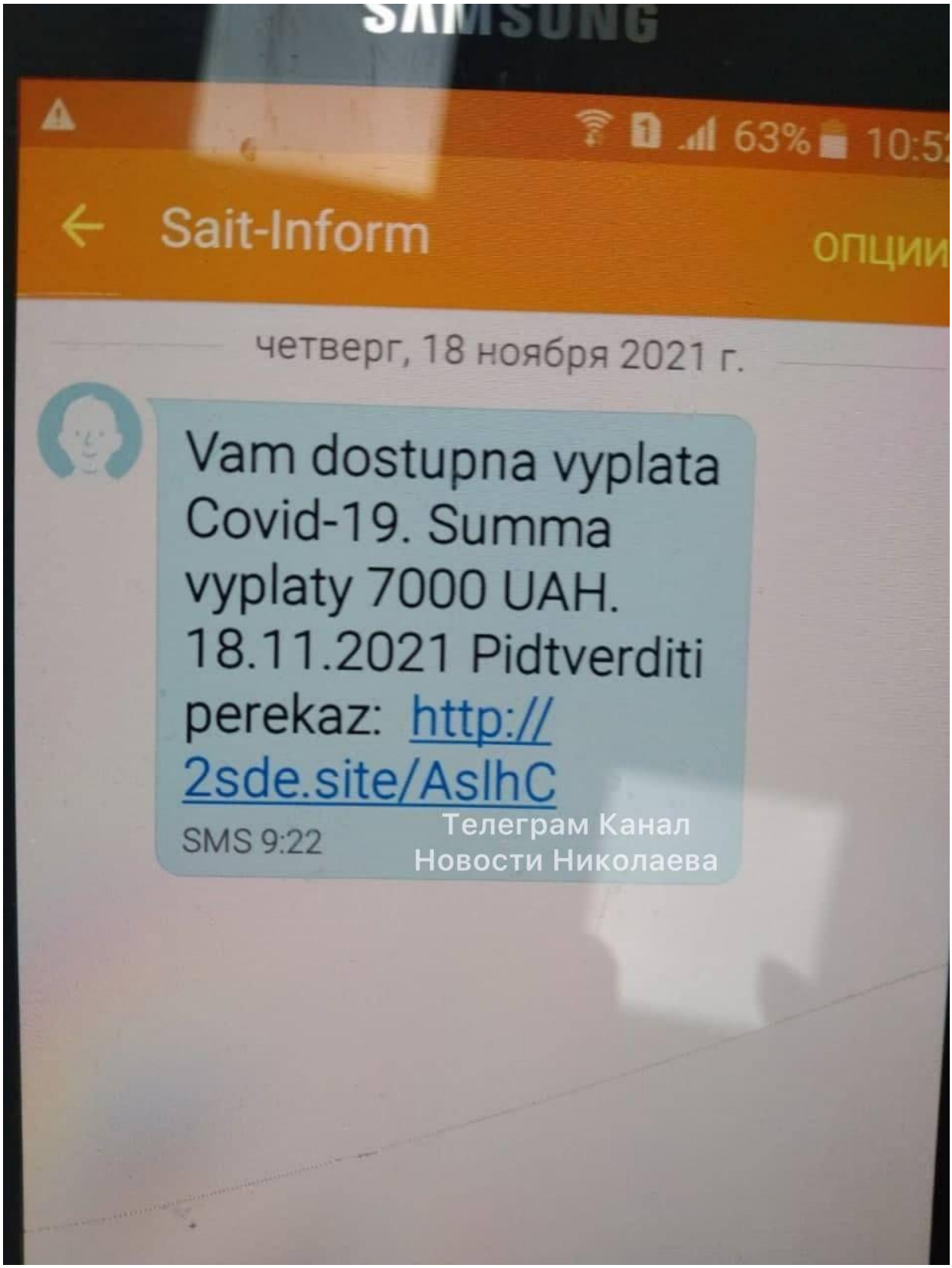
20:06

Приват Банк

Ощад Банк

Monobank

Інший Банк


SAMSUNG
63%
Sait-Inform
ОПЦИИ
четверг, 18 ноября 2021 г.
Vam dostupna vyplata Covid-19. Summa vyplaty 7000 UAH. 18.11.2021 Pidtverditi perekaz: http://2sde.site/AslhC
SMS 9:22
Телеграм Канал
Новости Николаева

Українські ліцензійні казино🇺🇦

🎁 Лови **вітальний подарунок** від онлайн-казино Cosmolot!

💰 Кожен новачок отримує *до 100 000 ₴ і 525 FS* 💣 за перші **5 депозитів**.

😎 Мінімальна сума поповнення – *від 100 ₴*.

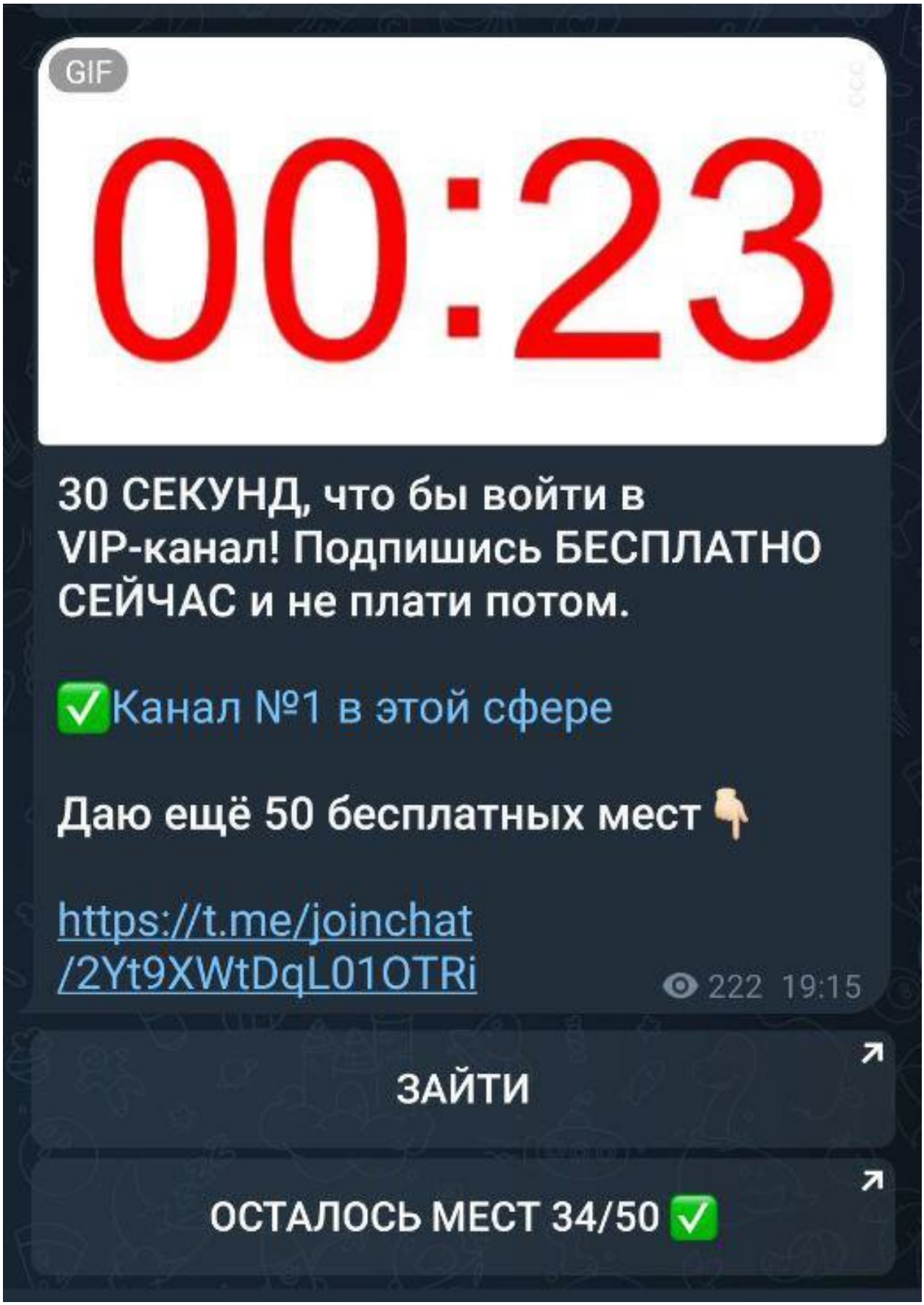
🚀 Крім того, є ще й **VIP Пакет** 💸 з подарунком *до 150 000 ₴ і 750 FS*.

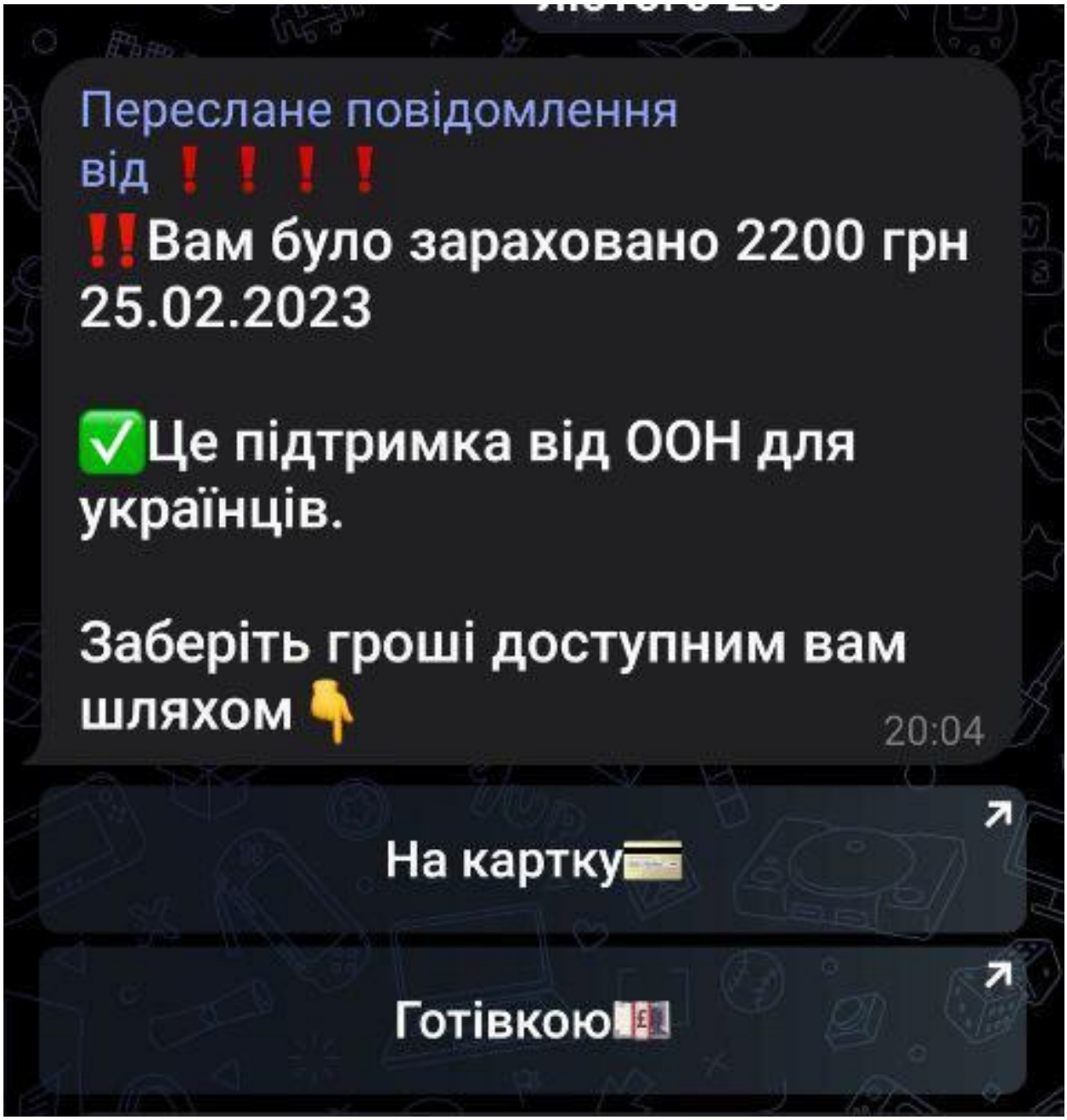
👉 Щоб отримати бонус, потрібно поповнити депозит на суму *від 2000 ₴*.

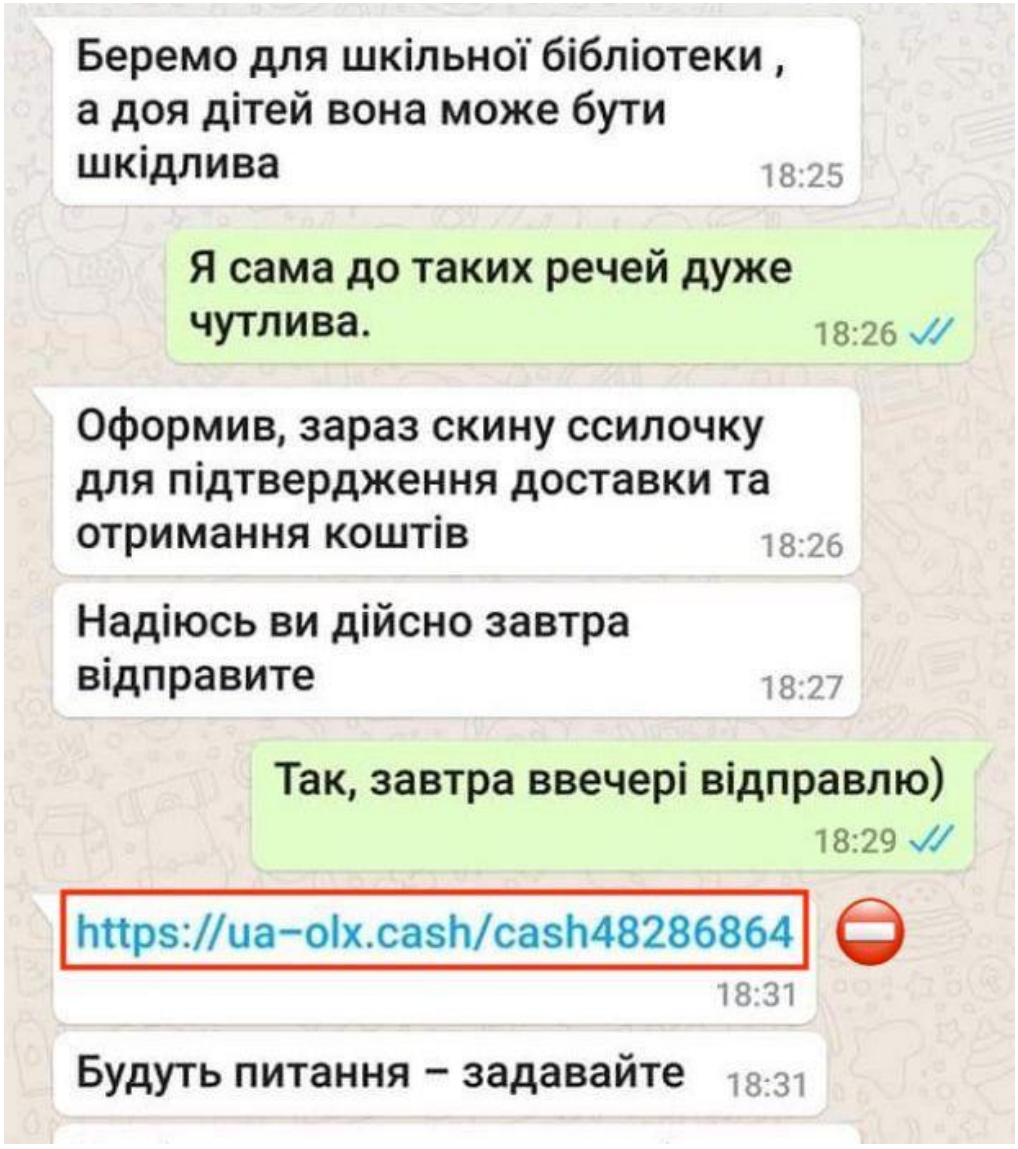
👌 Додатковий подарунок можна отримати за промокодом 🔔 **COSMOUA1**.

👍 18 👎 2 ❤️ 2 😄 1 6.9K 19:07

Отримати бонус 💸


GIF
00:23
30 СЕКУНД, что бы войти в VIP-канал! Подпишись БЕСПЛАТНО СЕЙЧАС и не плати потом.
✅Канал №1 в этой сфере
Даю ещё 50 бесплатных мест 👇
https://t.me/joinchat/2Yt9XWtDqL01OTRi
222 19:15
ЗАЙТИ
ОСТАЛОСЬ МЕСТ 34/50 ✅


Переслане повідомлення
від ! ! ! !
‼️Вам було зараховано 2200 грн
25.02.2023
✅Це підтримка від ООН для
українців.
Заберіть гроші доступним вам
шляхом 👇
20:04
На картку
Готівкою



Создана заявка на смену номера мобильного телефона. Если это были вы, не реагируйте на данное письмо. Номер +380*******93 будет изменен на +130*******85. Вы также можете отменить эту процедуру и создать код безопасности.

Отменить смену номера

Создать код безопасности

Дайджест вакансій тижня

Віддалено:
- Особистий помічник
- Адміністратор груп у Facebook
- Менеджер з продажу
- SMM Аналітик
- Менеджер з продажу
- Оператор чату перекладач
- Особистий помічник

Київ:
- Інформаційний спеціаліст
- Менеджер по роботі з клієнтами
- Sales – Manager
- Швея конструктор технолог
- Продавець консультант

Дніпро:
- Менеджер по роботі з клієнтами

Дубай:
- Фахівець у готельній і ресторанній сфері

Посилання на канал: https://t.me/+_i4s7zpUPKc4OWVi

12:12

Українські ліцензійні казино🇺🇦

👉 Новий турнір **Precious Prizes** в казино Pin-Up з призовим фондом *196 700 ₴*.

🚀 У турнірі від **Evoplay** розігрується *40 винагород*.

🍒 Переможцями стають ті, хто набирає найбільшу кількість балів.

🔔 Призова сума першого місця – *35 400 ₴*. Але поспішай, бо турнір скоро закінчиться.

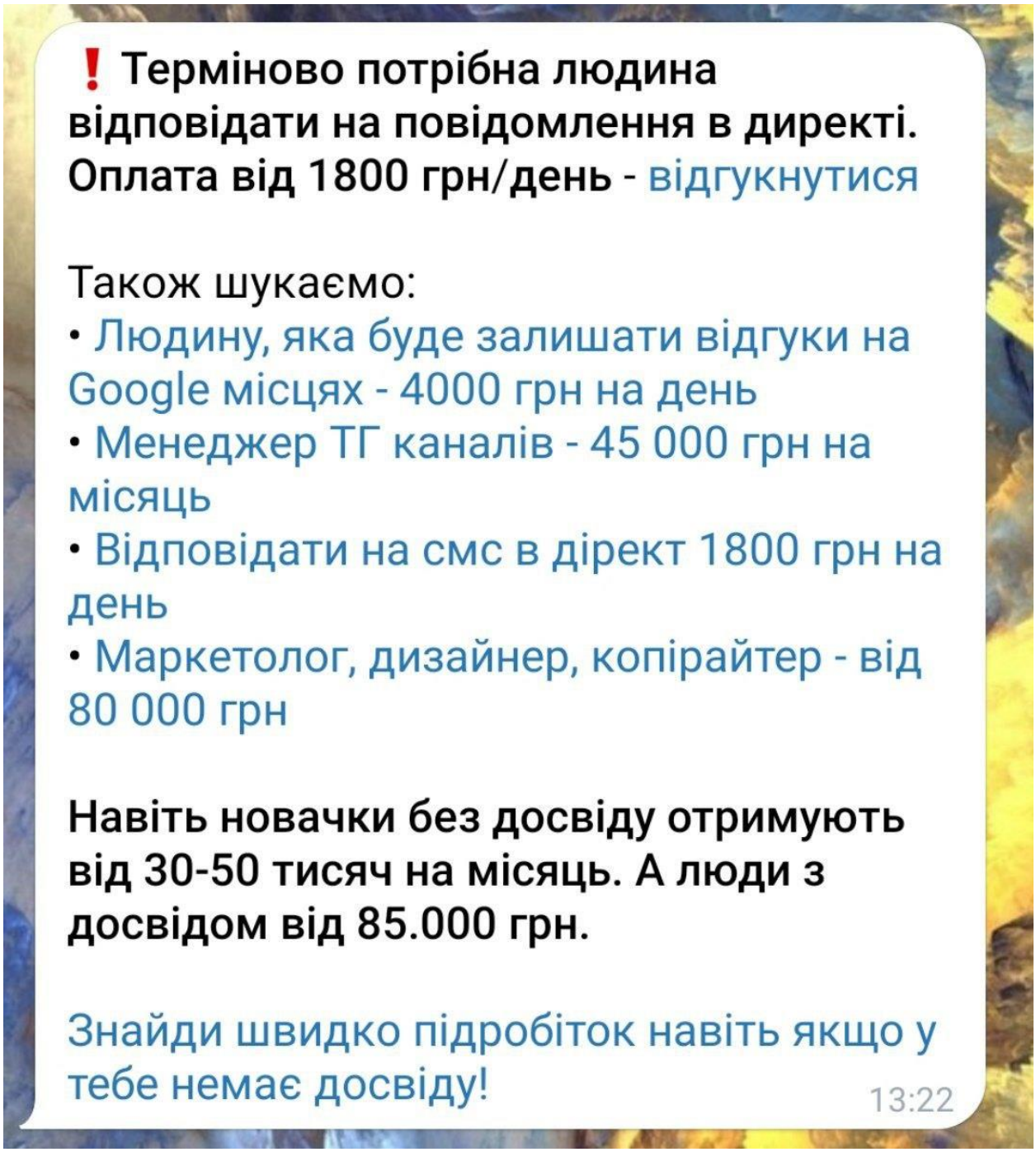
✈️ А ще скористайся промокодом **PIN2022**, щоб отримати подарунок.

👍 13 👎 3 😄 3 ❤️ 1 🤯 1

7.3K 17:00

До турніру 😎


LL SCANNER
❗ Встигніть першими
Відкриваємо у закритому форматі новий канал зі стажуванням та навчанням для наших підписників. Там ви знайдете:
■ віддалені вакансії в IT
■ стажування в топових компаніях
■ онлайн-курси, вебінари та інші можливості
Запрошення актуальне лише добу:
https://t.me/+y1GoCw3vvNw2NjUy
19:24
Прийняти запрошення


❗ Терміново потрібна людина відповідати на повідомлення в директі. Оплата від 1800 грн/день - відгукнутися
Також шукаємо:
• Людину, яка буде залишати відгуки на Google місцях - 4000 грн на день
• Менеджер ТГ каналів - 45 000 грн на місяць
• Відповідати на смс в діректі 1800 грн на день
• Маркетолог, дизайнер, копірайтер - від 80 000 грн
Навіть новачки без досвіду отримують від 30-50 тисяч на місяць. А люди з досвідом від 85.000 грн.
Знайди швидко підробіток навіть якщо у тебе немає досвіду!
13:22


19 березня
ДАЙДЖЕСТ ВАКАНСІЙ
Дайджест вакансій минулого тижня
Віддалено:
– Менеджер з продажу
– Перекладач
– Адміністратор сторінки
– Оператор онлайн чату
– Контент-менеджер
– Менеджер з продажу зі знанням болгарської мови
– Стрімер Liveme
– Контент мейкер
– Підробіток для школярів та студентів
Київ:
– Менеджер
– Менеджер з обробки даних
– Менеджер з логістики
– Менеджер по роботі з клієнтами
ЛЬвів:
– Спеціаліст по роботі з клієнтами
Дніпро:
– Менеджер по роботі з клієнтами
– Менеджер по роботі з клієнтами
#дайджест
17:22


🔍 Шукаємо людину, яка буде перекладати текст через Google перекладач за гроші! Знання англійської не потрібне. Зарплата 700 грн за день.
Також потрібні:
✔️ Переглядач телеграм каналів — 18 000 ₴
✔️ Контентмейкер в телеграм канал — 25 000 ₴
✔️ Водій з власним авто — до 40 000 ₴
✔️ Менеджер з продажу — до 112 000 ₴
✔️ Рієлтор — до 150 000 ₴
Ці та багато інших вакансій публікуємо на каналі SKILL SCANNER Зазвичай попит на такі пропозиції дуже високий, тому радимо не гаяти час.
👉 Підписуйтесь, та починайте заробляти достойно вже зараз
21:01

🎁 Ти вже отримав *вітальний подарунок* від казино за промокодом **UA1BONUS**?

😎 Тоді грай активніше та просувайся у програмі лояльності.

💰 За кожен рівень ти отримуватимеш **кеш-бонус** з *вейджром x10*:

👉 **Gold** – *300 ₴*
👉 **Platinum** – *1000 ₴*
👉 **Diamond** – *2500 ₴*
👉 **First Club** – *5000 ₴*

🚀 До речі, бонус за рівень **First Club** потрібно відіграти з *вейджером x1*.

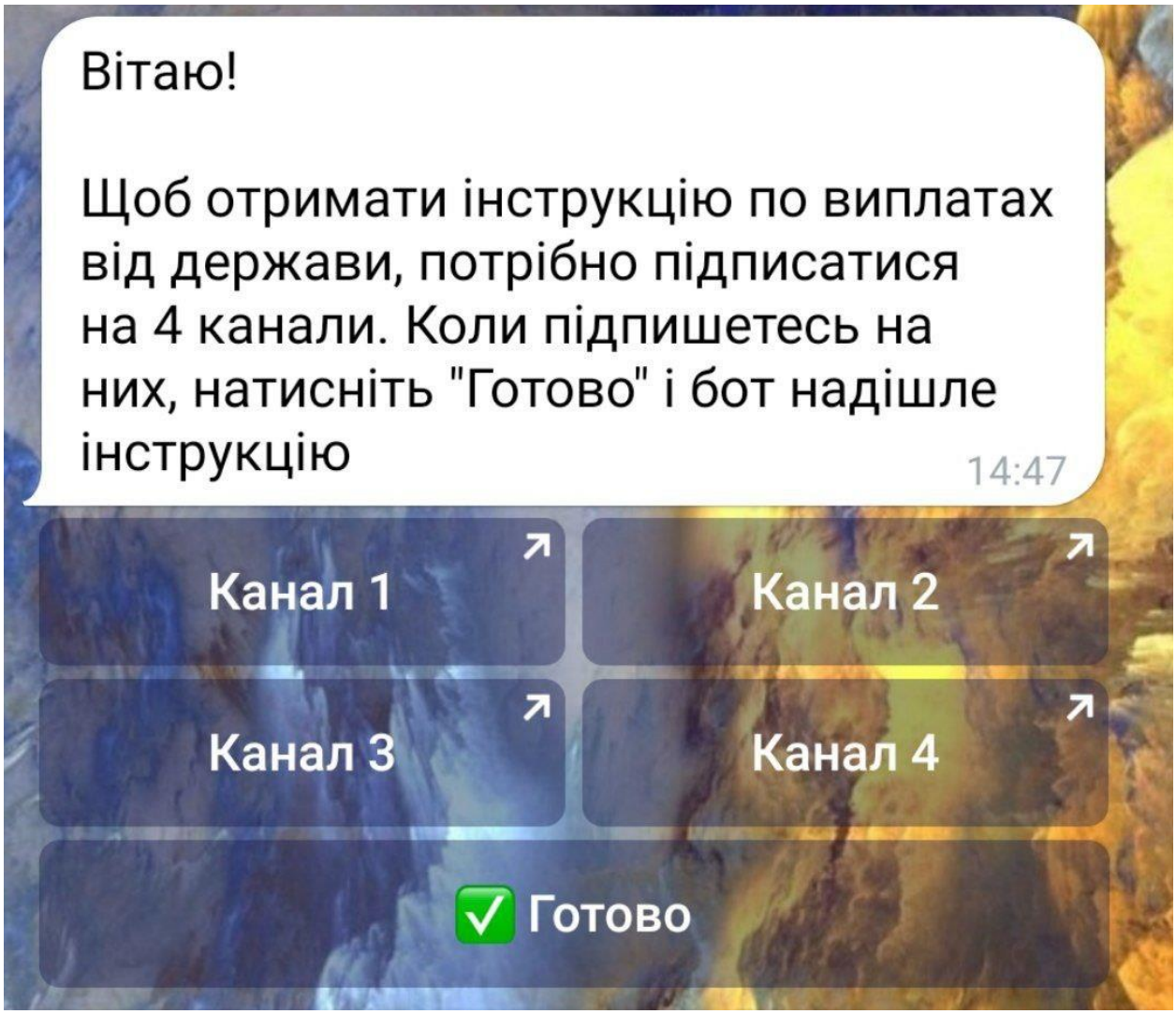
🎁 Ще більше **акцій та бонусів** шукай у нашому боті CasinoBonus!

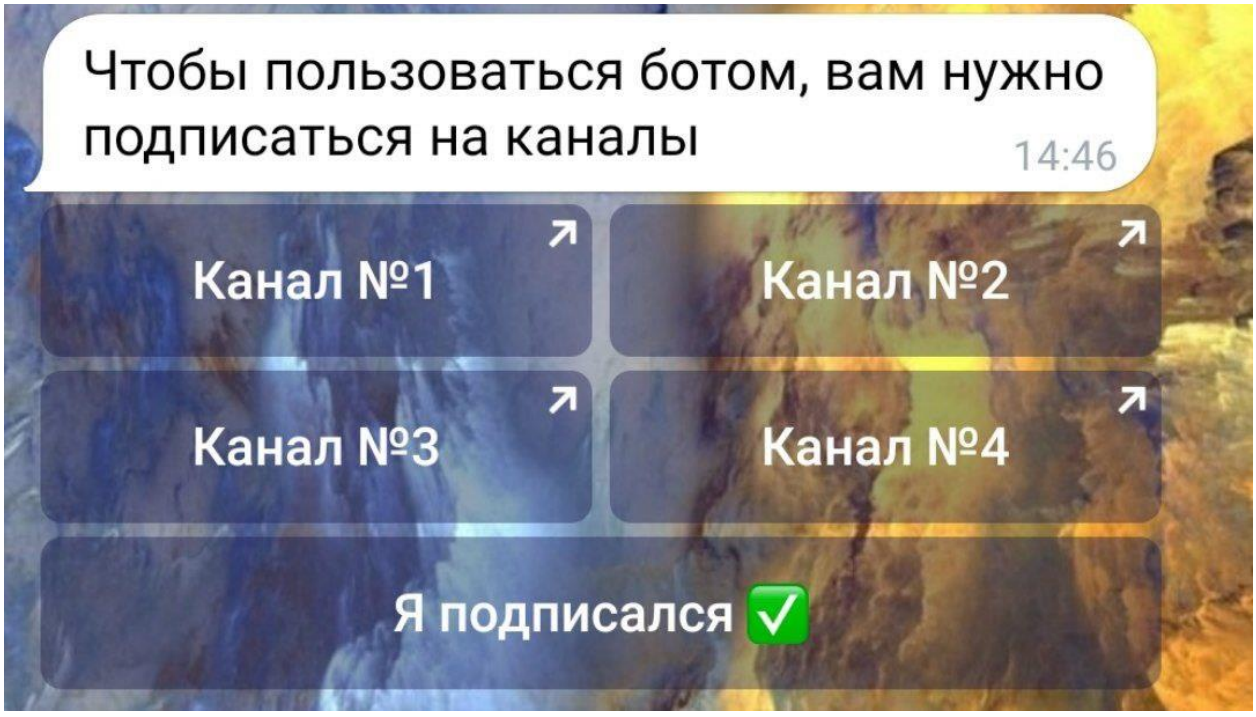
👍 23 👏 2 ❤️ 1

7.6K 12:43

Отримати бонус 😎


Терміново ❗ Потрібна людина на підробіток.
Той, хто зараз сидить без роботи, легко знайде її на The.Work
Свіжі! Перевірені! Актуальні вакансії! Які публікуються щодня.
Навіть люди без досвіду отримують по 30 000 грн. на місяць. А люди з досвідом до 124 000 грн. доходять.
Те саме посилання на закритий канал з палаючими вакансіями, підпишись на 👉 The.Work і знайди свою роботу:
🇺🇦 https://t.me/+ylaA1Ae1NdQ0MmQ6
17:14


Вітаю!
Щоб отримати інструкцію по виплатах від держави, потрібно підписатися на 4 канали. Коли підпишетесь на них, натисніть "Готово" і бот надішле інструкцію
14:47
Канал 1
Канал 2
Канал 3
Канал 4
✅ Готово


Чтобы пользоваться ботом, вам нужно подписаться на каналы
14:46
Канал №1
Канал №2
Канал №3
Канал №4
Я подписался ✅

💥 **В Україні запрацює єдиний номер для надання екстреної допомоги**

Внесено зміни до постанов КМУ від 28.10.2015 р. № 878 «Про затвердження Положення про Міністерство внутрішніх справ України» і від 14.11.2018 р. № 1024 «Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів» з метою приведення їх у відповідність до Законів України «Про систему екстреної допомоги населенню за єдиним телефонним номером 112» та «Про державну реєстрацію геномної інформації людини».

✅ Покладено на **МВС України завдання щодо впровадження та забезпечення функціонування і розвитку системи екстреної допомоги населенню за єдиним телефонним номером 112**, управління нею в режимі повсякденного функціонування, здійснення обробки геномної інформації людини та забезпечення функціонування електронного реєстру геномної інформації людини. Визначено інформаційно-комунікаційну систему 112 та електронний реєстр геномної інформації людини як функціональні підсистеми єдиної інформаційної системи МВС.

- **договори, довіреності, акти керівного органу платника податку**, якими оформлено повноваження осіб, які одержують продукцію в інтересах платника податку для здійснення операції;
- **первинні документи** щодо постачання/придбання товарів/послуг, зберігання і транспортування, навантаження, розвантаження продукції, складські документи, інвентаризаційні описи, у тому числі рахунки-фактури/інвойси, акти приймання-передачі товарів (робіт, послуг) з урахуванням наявності певних типових форм і галузевої специфіки, видаткові накладні;
- **розрахункові документи** та/або банківські виписки з особових рахунків;
- **документи щодо підтвердження відповідності продукції** (декларації про відповідність, паспорти якості, сертифікати відповідності), наявність яких передбачено договором та/або законодавством.

> Вказаний перелік не є вичерпним.

🔥🔥🔥 Акція **Cash Race** від **Betsoft** в Vulkan Casino із призовим фондом 💸 *80 000 €*!

🎰 Крутезна акція від провайдера **Betsoft** вже чекає на 👌 тебе.

🚀 До *6 березня* ти маєш шанс виграти:

👉 *100 щоденних призів* **Take The Prize** на суму *2 750 €*.
👉 *1100 грошових призів* за період проведення **акції**.
👉 Взяти участь у **розіграші** призового фонду *50 000 €*.

🍒 Загальна сума виграшів – *80 000 €*.
💰 Призи нараховуються протягом 🕰 **24 годин**.

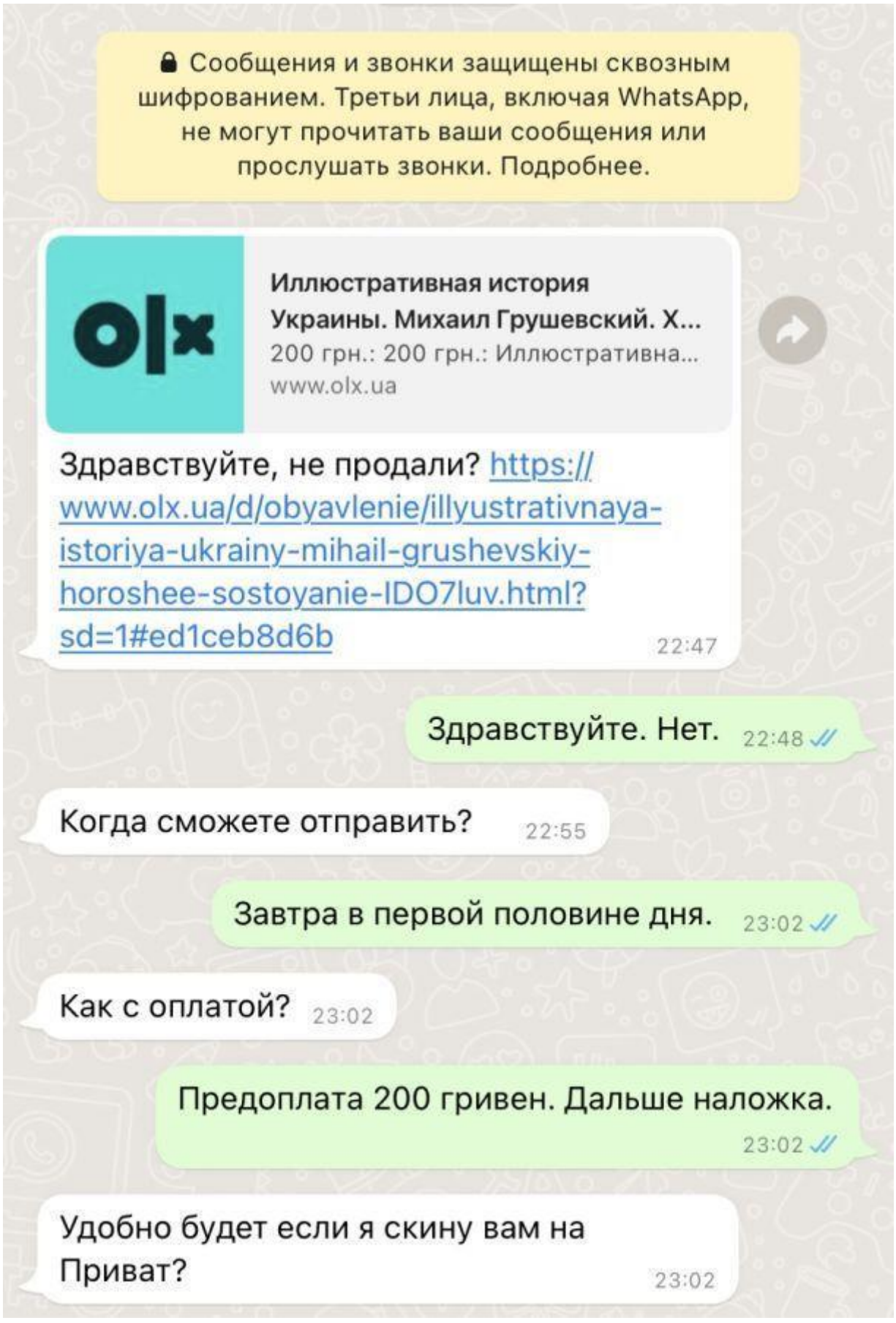
😎 Роби ставки в автоматах 🎰 розробника та накопичуй **бали**, щоб просуватися у табличці лідерів.

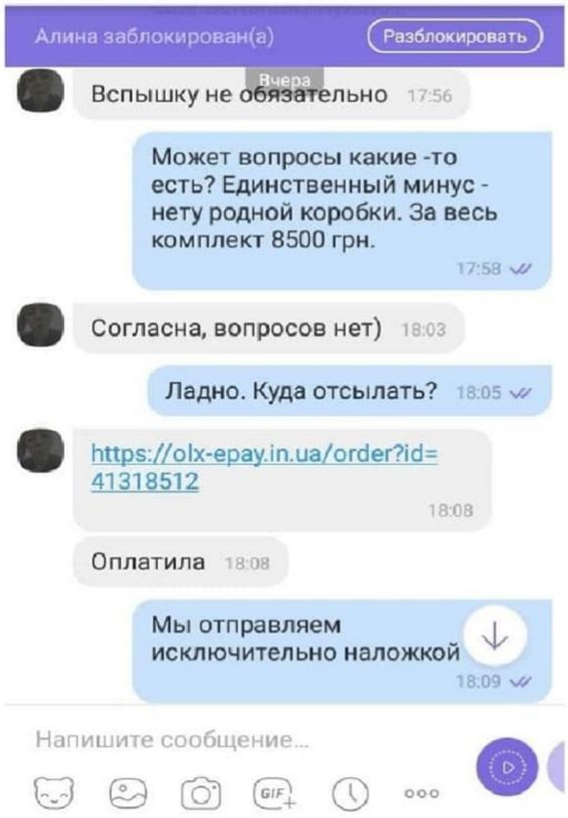
👍 12 ❤️ 1 😱 1

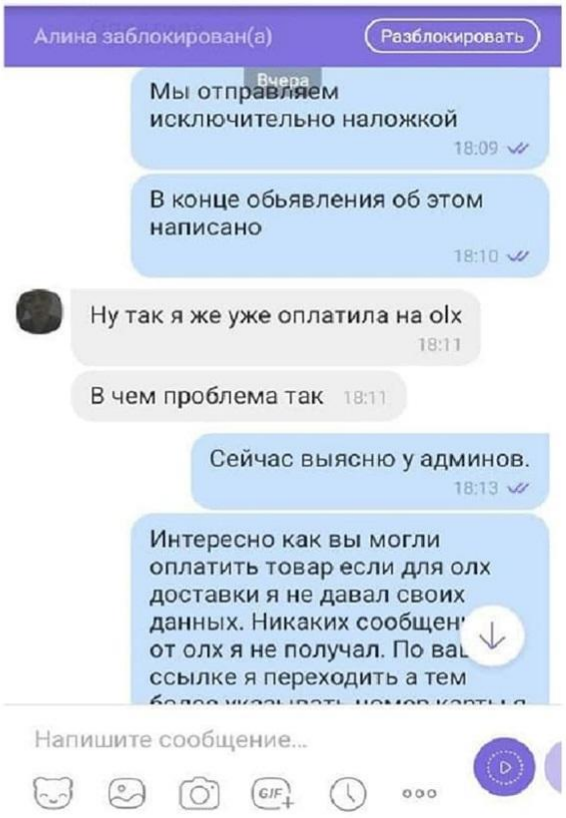
7.5K 17:00

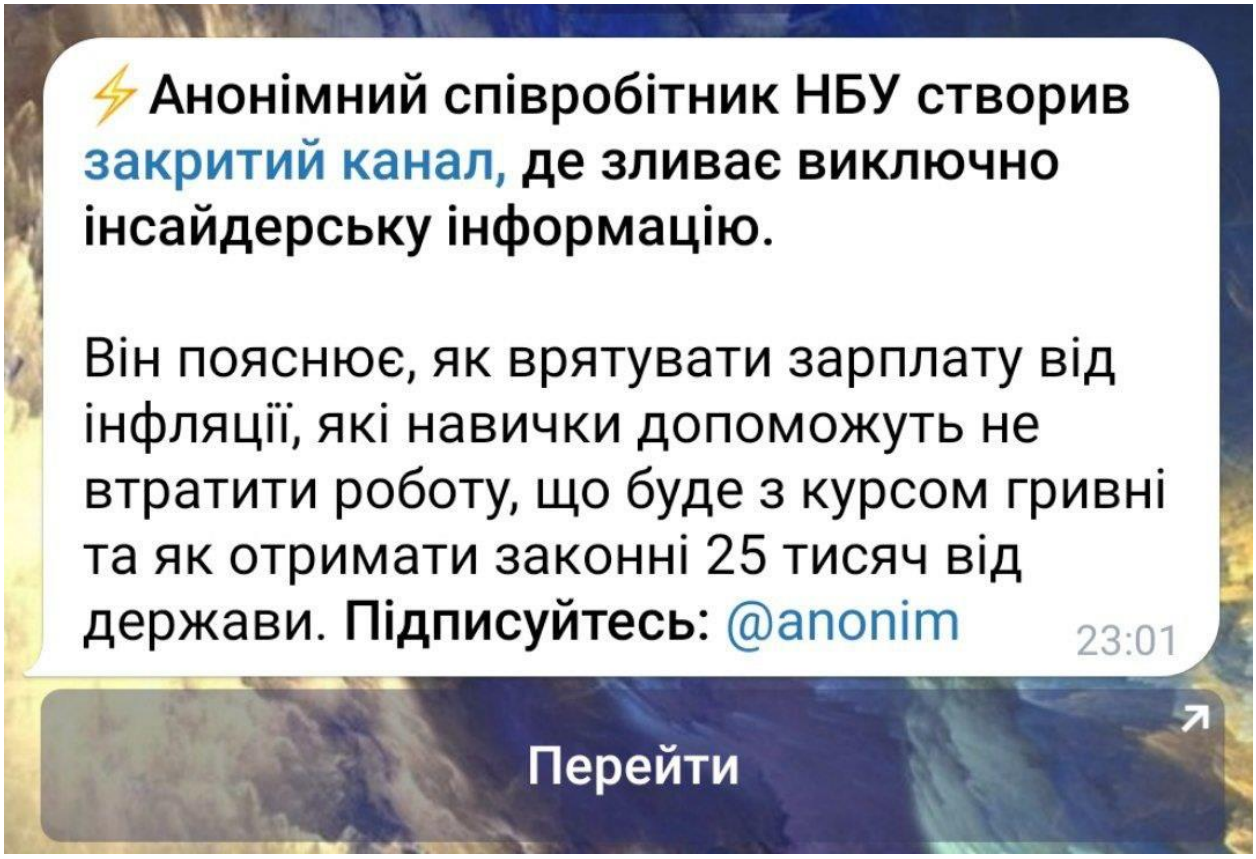
До акції 👌

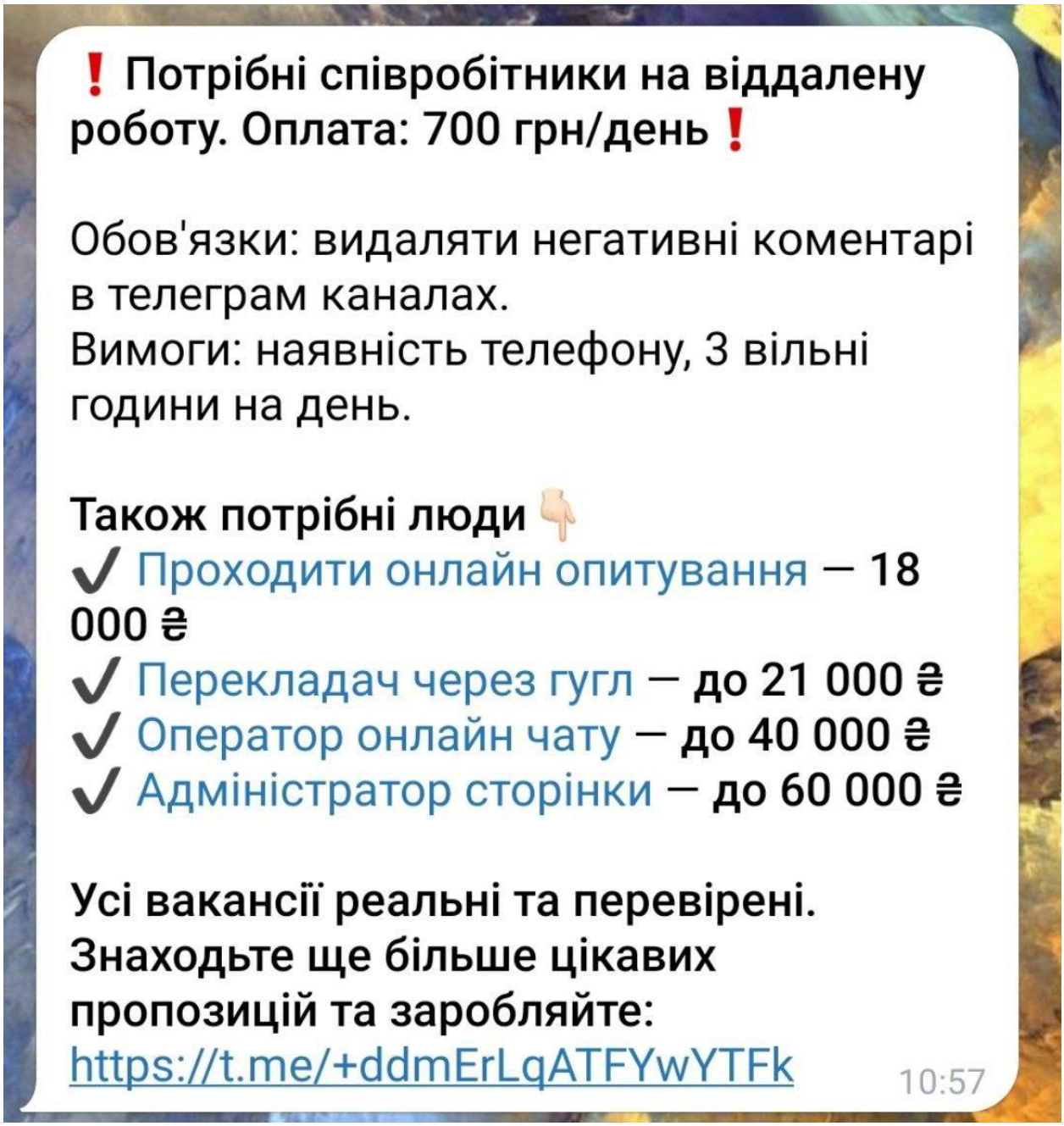

1997
єПідтримка - сервіс для допом...
бот
Сьогодні
/start 15:52
🇺🇦 СЛАВА УКРАЇНІ 🇺🇦
єПідтримка надає допомогу Змушено Внутрішньо Переміщенним Особам!
Используйте /off чтобы приостановить подписку. 15:52
Хотите создать своего бота? Вам сюда: @Manybot 15:52
💙Отримати💛 15:52
Інструкція для отримання:
🌕 Перейдіть у посилання трохи нижче.

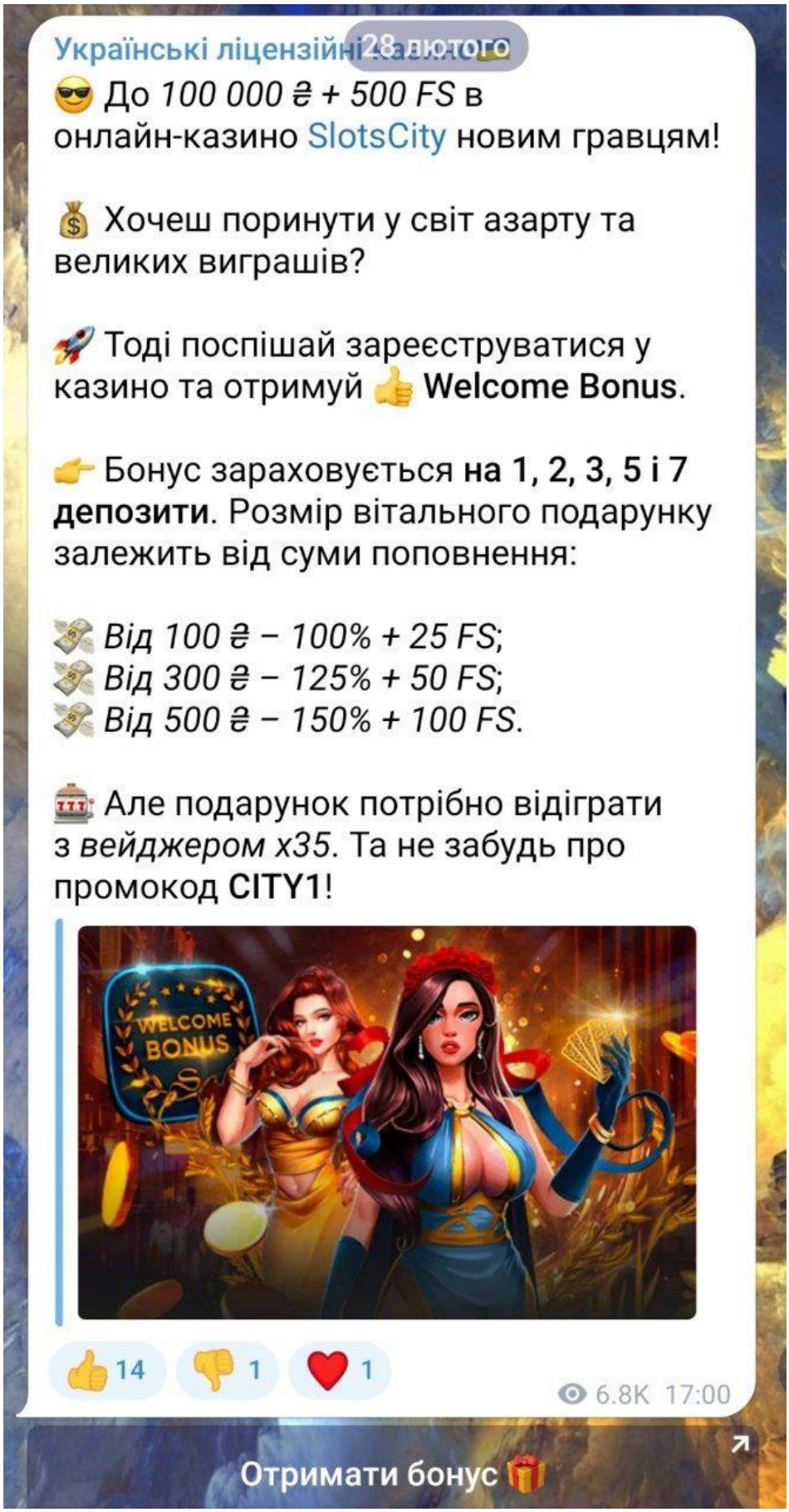

Сообщения и звонки защищены сквозным шифрованием. Третьи лица, включая WhatsApp, не могут прочитать ваши сообщения или прослушать звонки. Подробнее.
Иллюстративная история Украины. Михаил Грушевский. Х...
200 грн.: 200 грн.: Иллюстративна...
www.olx.ua
Здравствуйте, не продали? https://www.olx.ua/d/obyavlenie/illyustrativnaya-istoriya-ukrainy-mihail-grushevskiy-horoshee-sostoyanie-IDO7luv.html?sd=1#ed1ceb8d6b 22:47
Здравствуйте. Нет. 22:48
Когда сможете отправить? 22:55
Завтра в первой половине дня. 23:02
Как с оплатой? 23:02
Предоплата 200 гривен. Дальше наложка. 23:02
Удобно будет если я скину вам на Приват? 23:02

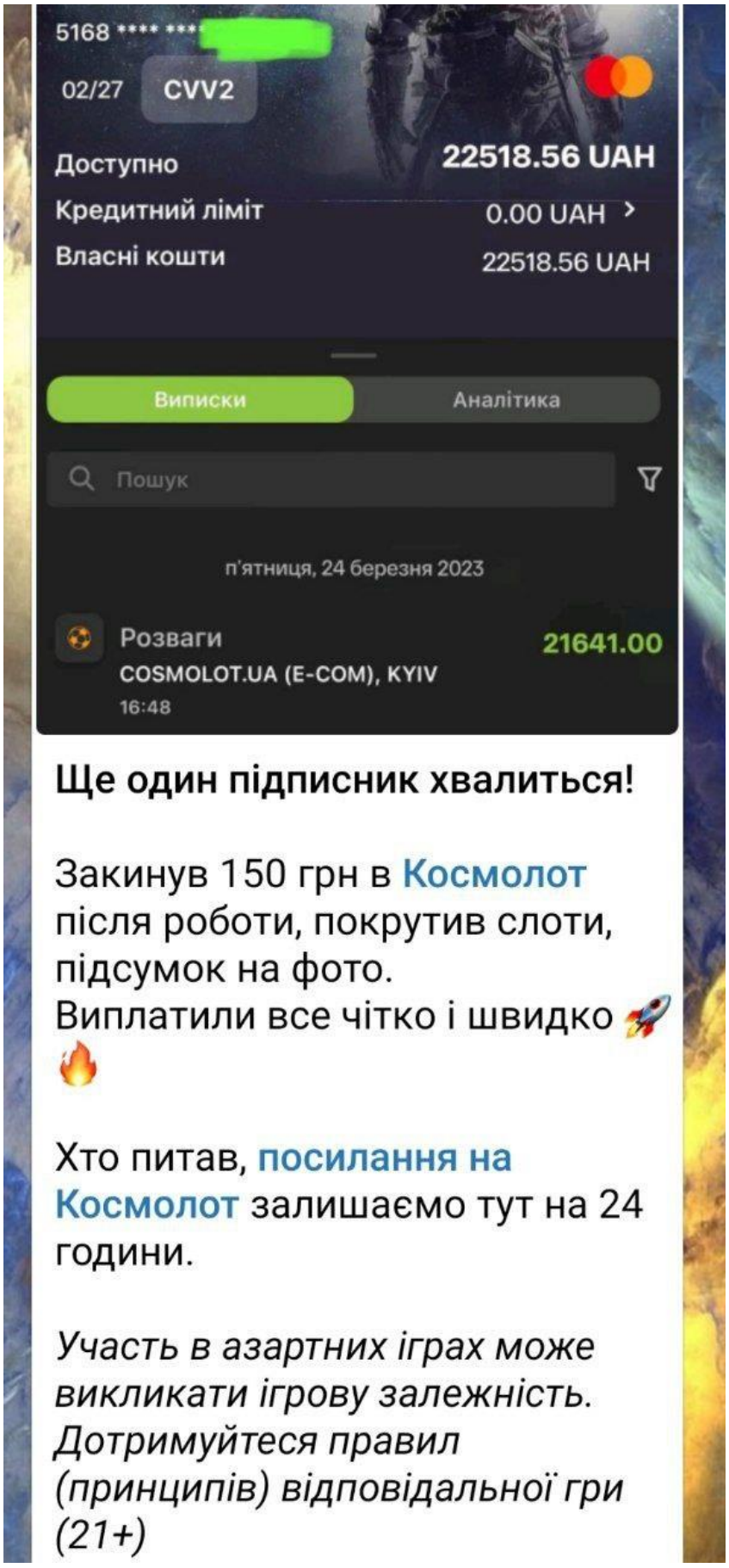

Алина заблокирован(а)
Разблокировать
Вчера
Вспышку не обязательно 17:56
Может вопросы какие -то есть? Единственный минус - нету родной коробки. За весь комплект 8500 грн.
17:58
Согласна, вопросов нет) 18:03
Ладно. Куда отсылать? 18:05
https://olx-epay.in.ua/order?id=41318512
18:08
Оплатила 18:08
Мы отправляем исключительно наложкой
18:09
Напишите сообщение...


Алина заблокирован(а)
Разблокировать
Вчера
Мы отправляем исключительно наложкой
18:09
В конце обьявления об этом написано
18:10
Ну так я же уже оплатила на olx
18:11
В чем проблема так 18:11
Сейчас выясню у админов.
18:13
Интересно как вы могли оплатить товар если для олх доставки я не давал своих данных. Никаких сообщен
от олх я не получал. По ва
ссылке я переходить а тем
Напишите сообщение...

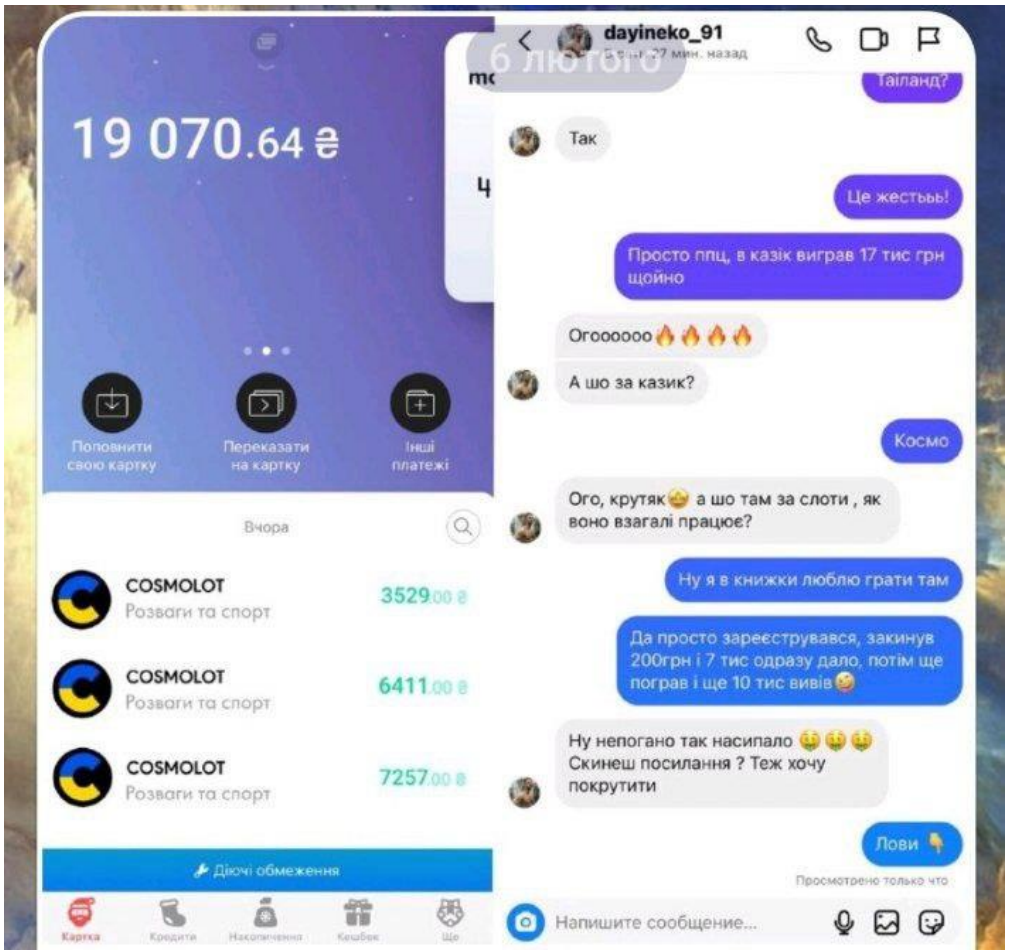

⚡Анонімний співробітник НБУ створив закритий канал, де зливає виключно інсайдерську інформацію.
Він пояснює, як врятувати зарплату від інфляції, які навички допоможуть не втратити роботу, що буде з курсом гривні та як отримати законні 25 тисяч від держави. Підписуйтесь: @anonim
23:01
Перейти


❗ Потрібні співробітники на віддалену роботу. Оплата: 700 грн/день ❗
Обов'язки: видаляти негативні коментарі в телеграм каналах.
Вимоги: наявність телефону, 3 вільні години на день.
Також потрібні люди 👇🏻
✔️ Проходити онлайн опитування — 18 000 ₴
✔️ Перекладач через гугл — до 21 000 ₴
✔️ Оператор онлайн чату — до 40 000 ₴
✔️ Адміністратор сторінки — до 60 000 ₴
Усі вакансії реальні та перевірені. Знаходьте ще більше цікавих пропозицій та заробляйте:
https://t.me/+ddmErLqATFYwYTFk
10:57


Українські ліцензійні казино
28 лютого
😎 До 100 000 ₴ + 500 FS в онлайн-казино SlotsCity новим гравцям!
💰 Хочеш поринути у світ азарту та великих виграшів?
🚀 Тоді поспішай зареєструватися у казино та отримуй 👍 Welcome Bonus.
👉 Бонус зараховується на 1, 2, 3, 5 і 7 депозити. Розмір вітального подарунку залежить від суми поповнення:
💸 Від 100 ₴ – 100% + 25 FS;
💸 Від 300 ₴ – 125% + 50 FS;
💸 Від 500 ₴ – 150% + 100 FS.
🎰 Але подарунок потрібно відіграти з вейджером x35. Та не забудь про промокод CITY1!
WELCOME BONUS
👍 14
👎 1
❤️ 1
6.8K 17:00
Отримати бонус 🎁


5168 **** ***
02/27
CVV2
Доступно
22518.56 UAH
Кредитний ліміт
0.00 UAH
Власні кошти
22518.56 UAH
Виписки
Аналітика
Пошук
п'ятниця, 24 березня 2023
Розваги
21641.00
COSMOLOT.UA (E-COM), KYIV
16:48
Ще один підписник хвалиться!
Закинув 150 грн в Космолот після роботи, покрутив слоти, підсумок на фото.
Виплатили все чітко і швидко 🚀🔥
Хто питав, посилання на Космолот залишаємо тут на 24 години.
Участь в азартних іграх може викликати ігрову залежність. Дотримуйтеся правил (принципів) відповідальної гри (21+)


ДОПОМОГА ООН
ЯК ОТРИМАТИ?
ЗАПОВНИТИ ЗАЯВКУ
✅ СТАРТУВАЛА ВИПЛАТА 6600 ГРН: українці можуть отримати від ООН нову грошову допомогу.
Інструкцію як отримати допомогу завантажили тут 👇
https://t.me/+1HMdc43wMOo3MTQy
112
15
11
6
4
24.5K 19:00
Інструкція
Подати заявку

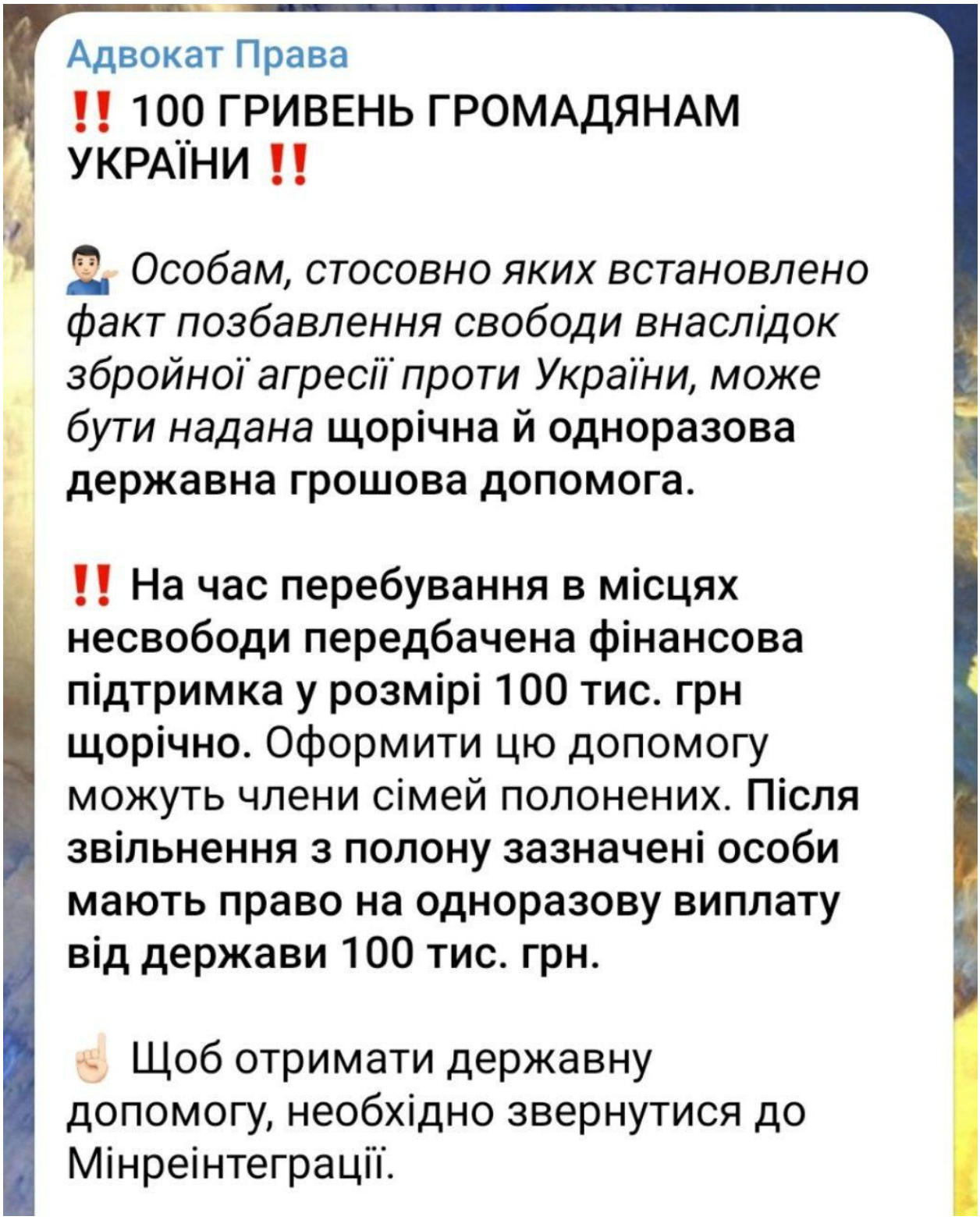


🤑 **Ще один виграш від підписника в онлайн-слоти**

Він закинув 200 грн, покрутив слоти у Космолот, і ось що вийшло. Результат на фото. Виплатили все одразу на картку банку.
🍀 Космо і справді НАСИПАЄ 🍀

👉 **Посилання на Космолот**

p.s – це онлайн казино 🎰 гра на справжні гроші 💵 справа фарту. Хто питав посилання, залишу тут лише на 24 години.


Адвокат Права
‼️ 100 ГРИВЕНЬ ГРОМАДЯНАМ УКРАЇНИ ‼️
💁🏻‍♂️ *Особам, стосовно яких встановлено факт позбавлення свободи внаслідок збройної агресії проти України, може бути надана* **щорічна й одноразова державна грошова допомога.**
‼️ **На час перебування в місцях несвободи передбачена фінансова підтримка у розмірі 100 тис. грн щорічно.** Оформити цю допомогу можуть члени сімей полонених. **Після звільнення з полону зазначені особи мають право на одноразову виплату від держави 100 тис. грн.**
☝🏻 Щоб отримати державну допомогу, необхідно звернутися до Мінреінтеграції.

Українські ліцензійні казино🇺🇦

👉 Казино PokerMatch оголошує акцію **Wazdan Mystery Drop**.

💸 Долучайся й ти та бери участь у розіграші *250 000 €*.

⚡ До *6 березня* грай у слоти 🎰 від **Wazdan** та забирай свій випадковий приз 💰 *до 500 €*.

🔔 Мінімальної ставки для участі в акції **немає**!

😎 Приз може випасти будь-якої миті 👋 в процесі гри.

🚀 Крім того, скористайся промокодом 👉 **PMCASINO**, щоб отримати бонус 🎁.

👍 15 ❤️ 1 🔥 1

7.2K 17:00

Акція Mystery Drop 👌


UNHCR
The UN Refugee Agency
🇺🇦 ❗ ГРОШОВІ ВИПЛАТИ ❗ 🇺🇦
Грошова виплата від Фонду "Європи" у зв'язку з ситуацією в країні, які стартували з 1 березня.
Кожен Українець може отримати одноразову виплату у розмірі 12000 гривень.
15:00

OLX

Спасибо за заказ! Ожидайте подтвержения. Детали: goo.gl/O0syzz

Ваш заказ на OLX подтвержден! Детали: goo.gl/GRD3QJ

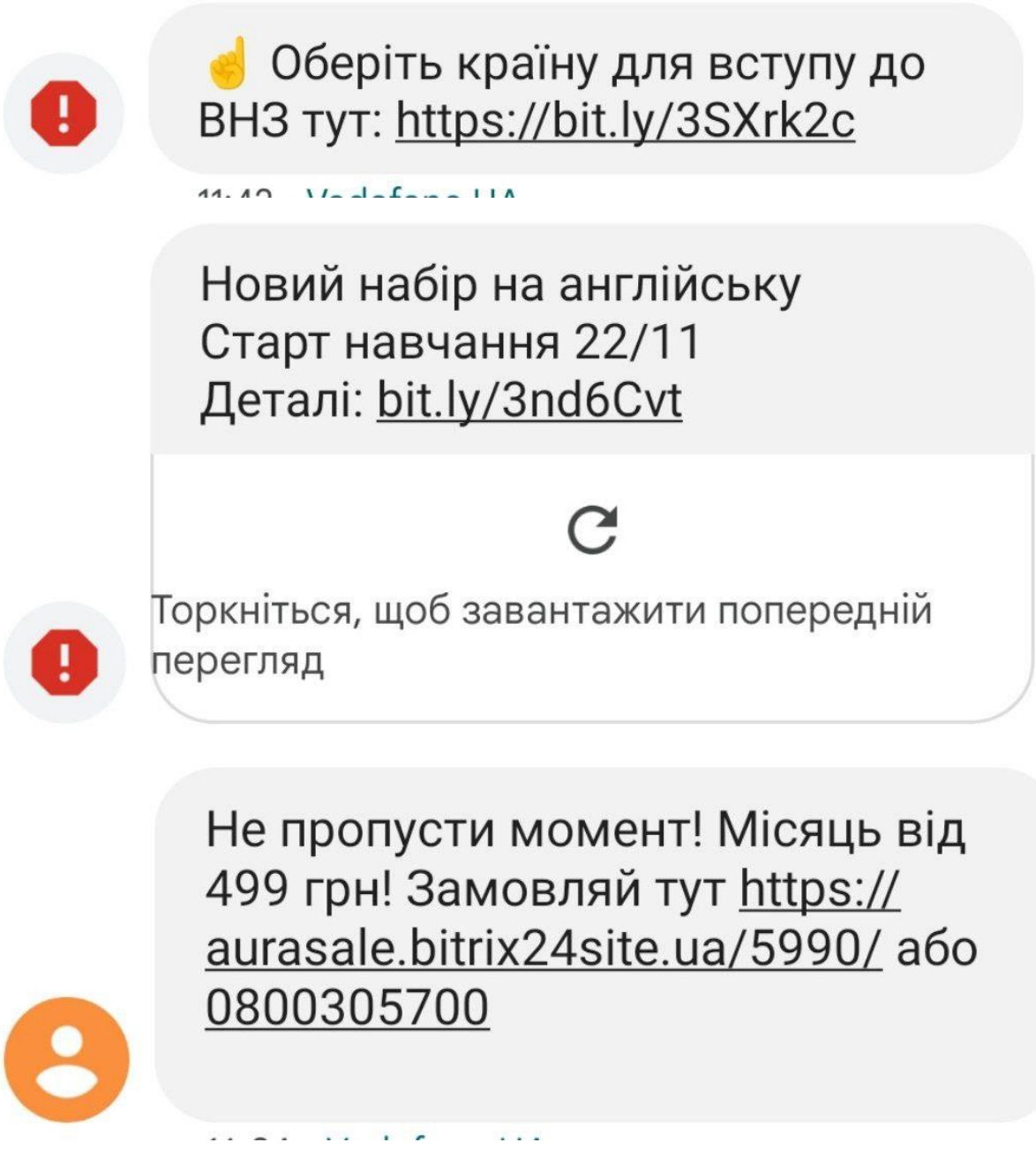
2 04.09 21:15

Push-уведомления отключены. Заказ заморожен. Детали: cutt.ly/PfbCde4

Заказ в обработке. Получен ответ от оператора OLX: cutt.ly/KfbCWbp

2 04.09 21:34

Ваш заказ сформирован агентом поддержки OLX. Оформить: cutt.ly/ifbC2KA


☝ Оберіть країну для вступу до ВНЗ тут: https://bit.ly/3SXrk2c
Новий набір на англійську
Старт навчання 22/11
Деталі: bit.ly/3nd6Cvt
Торкніться, щоб завантажити попередній перегляд
Не пропусти момент! Місяць від 499 грн! Замовляй тут https://aurasale.bitrix24site.ua/5990/ або 0800305700

ТРЕТЯ ХВИЛЯ ВСТУПУ ❗
На ДЕННУ, заочну, ДИСТАНЦІЙНУ форми навчання
Вступ на 1,2,3 КУРС ТА МАГІСТРАТУРУ без ЗНО та НМТ!
👨PR і ЖУРНАЛІСТИКА
🎬Кіно і телебачення
🎭Театральне мистецтво
🏬Туризм. Готельно-ресторанний бізнес
🎨Дизайн, 3D-моделювання
💻Інтернет-маркетолог
🎭Івент-менеджмент, фешн і шоу-бізнес
💃Балетмейстер-хореограф
🎤Естрадний спів
РЕЄСТРАЦІЯ:
bit.ly/KUK_abiturient
☎Консультація:
0985973413
0957536734
МОЛОДЬ ОБИРАЄ УНІВЕРСИТЕТ КУЛЬТУРИ ❗
@POPLAVKIY_MICHAIL

Торкніться, щоб завантажити попередній перегляд

Українські ліцензійні казино🇺🇦

💸 **Вітальний бонус** *до 50 000 ₴ + 300 FS* в онлайн-казино Космолот!

💥 Якщо ти новачок, отримай подарунок за перші **5 депозитів**.

👉 Вітальний бонус доступний одразу після ⚡ реєстрації ⚡ за депозит *від 100 ₴*.

🎁 На тебе чекає *до 650% і 300 безкоштовних обертів*.

👍 А ще ти можеш обрати **VIP Пакет** із подарунком *625%* на депозит і *500 FS*, якщо поповниш рахунок на суму *від 2000 ₴*.

😎 Відіграти отримане заохочення потрібно з **вейджером x35**.

👍 14 🤗 2 ❤️ 1 6.3K 17:00

Отримати бонус 🎁

☝ Оберіть країну для вступу до ВНЗ тут: https://bit.ly/3SXrk2c

Торкніться, щоб завантажити попередній перегляд

11:42 • Vodafone UA

Запрошуємо!

❗ 25/02 презентація Міжнародного ліцею >> bit.ly/3Xz9mng

12:49 • Vodafone UA

Коснитесь, чтобы сбросить ваш пароль в Instagram: https://instagram.com/accounts/password/reset/confirm/2uerpu1/4rx-8b775e4703d69d83752a23632a87c498/

Захарченко Яна Іванівна, нагадуємо про необхідність внесення платежу в ТОВ "ТАЛІОН ПЛЮС" СЬОГОДНІ. 0800215017 Таліон Плюс

Отримувач ТОВ "ТАЛІОН ПЛЮС" ЄДРПОУ: 39700642. Поточний рахунок: UA823052990000026 502016200157, МФО 305299. Банк отримувача: АТ КБ "ПРИВАТБАНК". Призначення платежу: ІПН боржника , Захарченко Яна Іванівна, Договір № 845009818 Деталі: 0800215017 Таліон Плюс

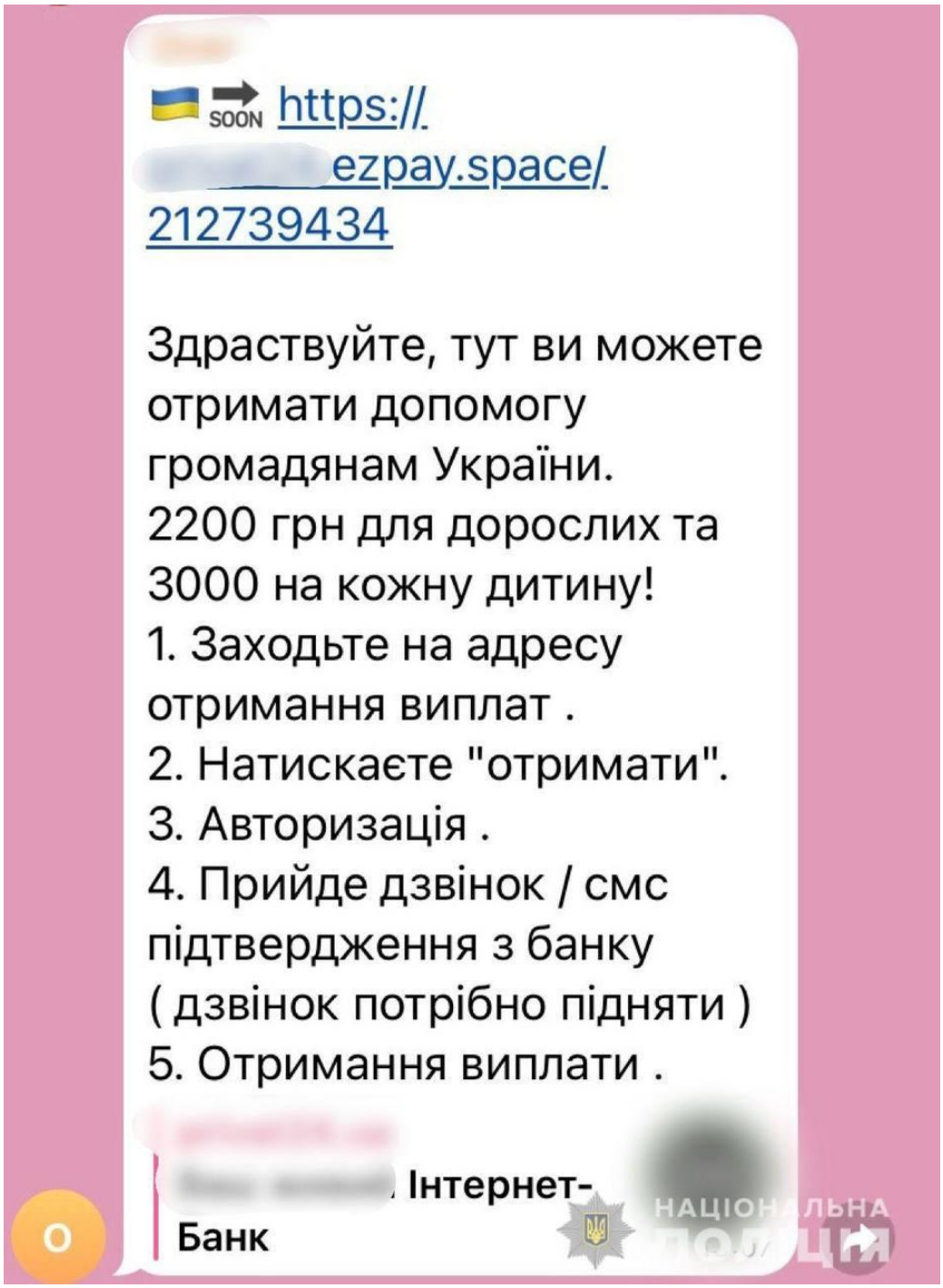
Заберіть 370000 грн. готівкою. Дзвоніть: 0 800 30 50 20 (безкоштовно)

11:14 • Vodafone UA

Захарченко Яна Іванівна, нагадуємо про необхідність внесення платежу в ТОВ "ТАЛІОН ПЛЮС" СЬОГОДНІ. 0800215017 Таліон Плюс

Відсутність оплати буде розцінюватись як ухилення від виконання зобов’язань по кредиту. 0800215017 Таліон Плюс
ТП1

17:17 • Vodafone UA



Українські ліцензійні казино🇺🇦

🎰 **Леприкони** вже чекають у казино Vulkan Casino!

😎 Мчіть на повну в турнір **Lucky Race** від 👉 провайдера *Gamzix*!

💰 Ти отримаєш можливість показати свої навички та позмагатися за частину 💸 від *20 000 €*.

🎰 Долучайся прямо зараз!

👉 Дістанься фінішу або стань одним із *50 щасливчиків*.

🍒 Та не забувай про промокод **UA1VULKAN**, щоб отримати 🎁 бонус!

👍 13 ❤️ 5 💯 2 🤪 1

5.7K 17:00

До турніру 💣

16:17

+380 (91) 938 51 61

16:18

Shanovnuy klient,vasha kartka bude blokovana,na 90 bankivskih dniv.Na sud ekspertizu.Vam neobhidno za telefonuvatu.inf-0919385161. Z povagouy sluzba bezpeki banku.

Українські ліцензійні казино🇺🇦

🔥🔥🔥 Казино-турнір у Vbet вже розпочався!

💸 Крути барабани слотів **Yggdrasil** і виграй свою частку від *1 500 000 ₴*.

🔔 Що потрібно робити?

👉 Обирай автомати провайдера.
👉 Виконуй місії.
👉 Збирай необхідні символи.
👉 Займай законне місце у таблиці лідерів.

💰 Мінімальної ставки для кваліфікації немає. Завершуй місії та забирай *шалені гроші*.

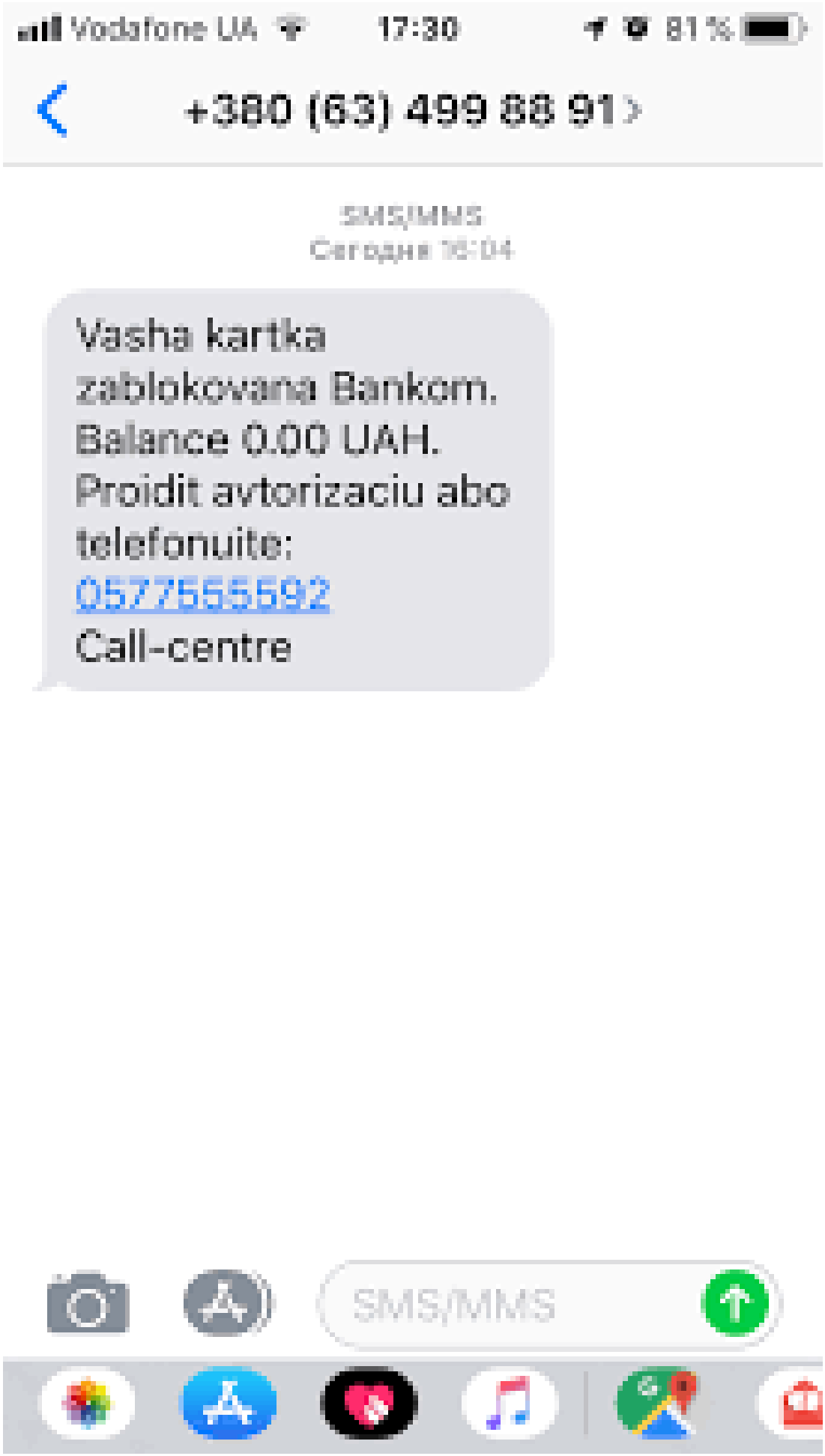
😏 Ще більше **подарунків** ти знайдеш у нашому боті CasinoBonus!

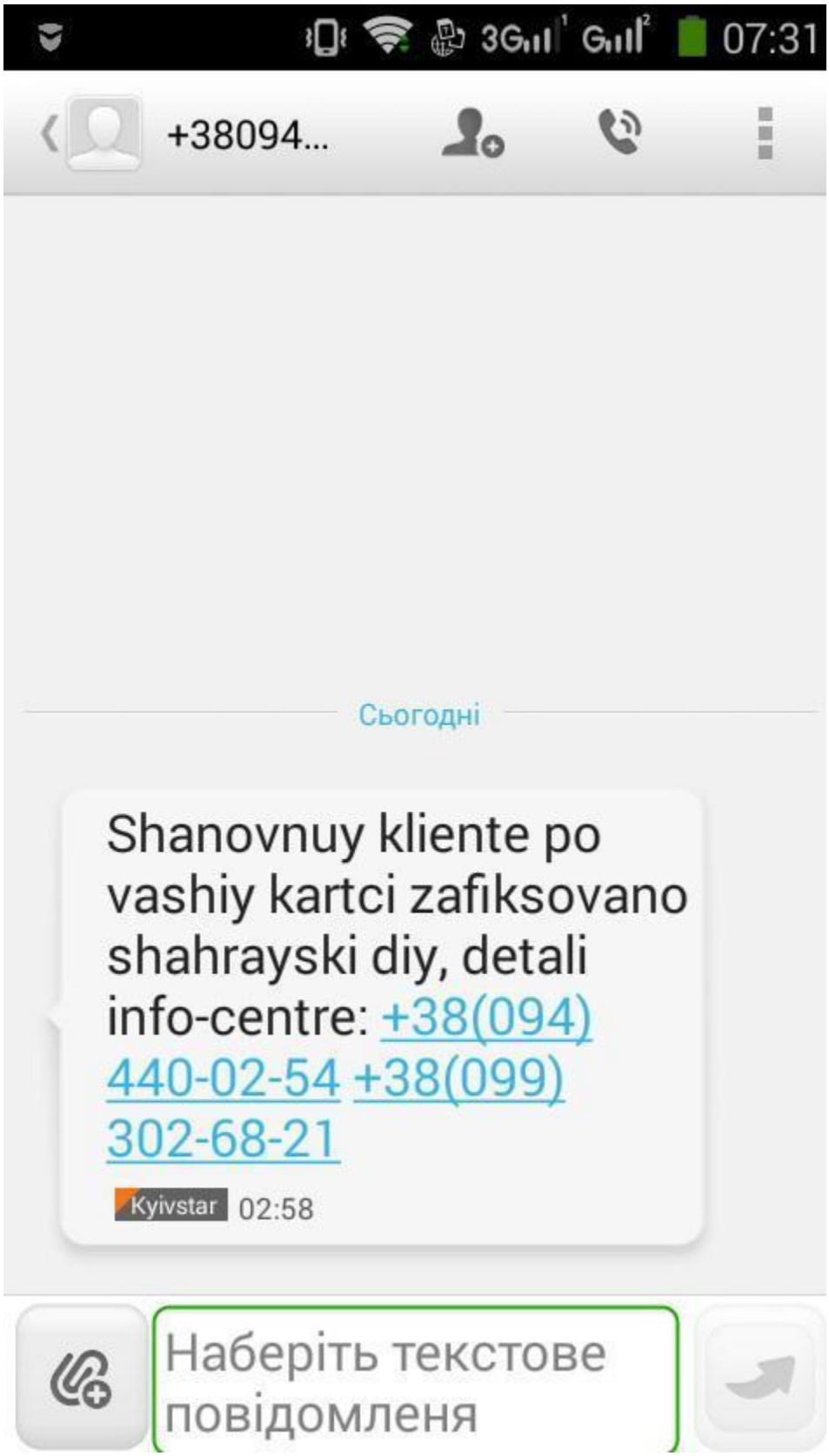
👍 10 🤪 2

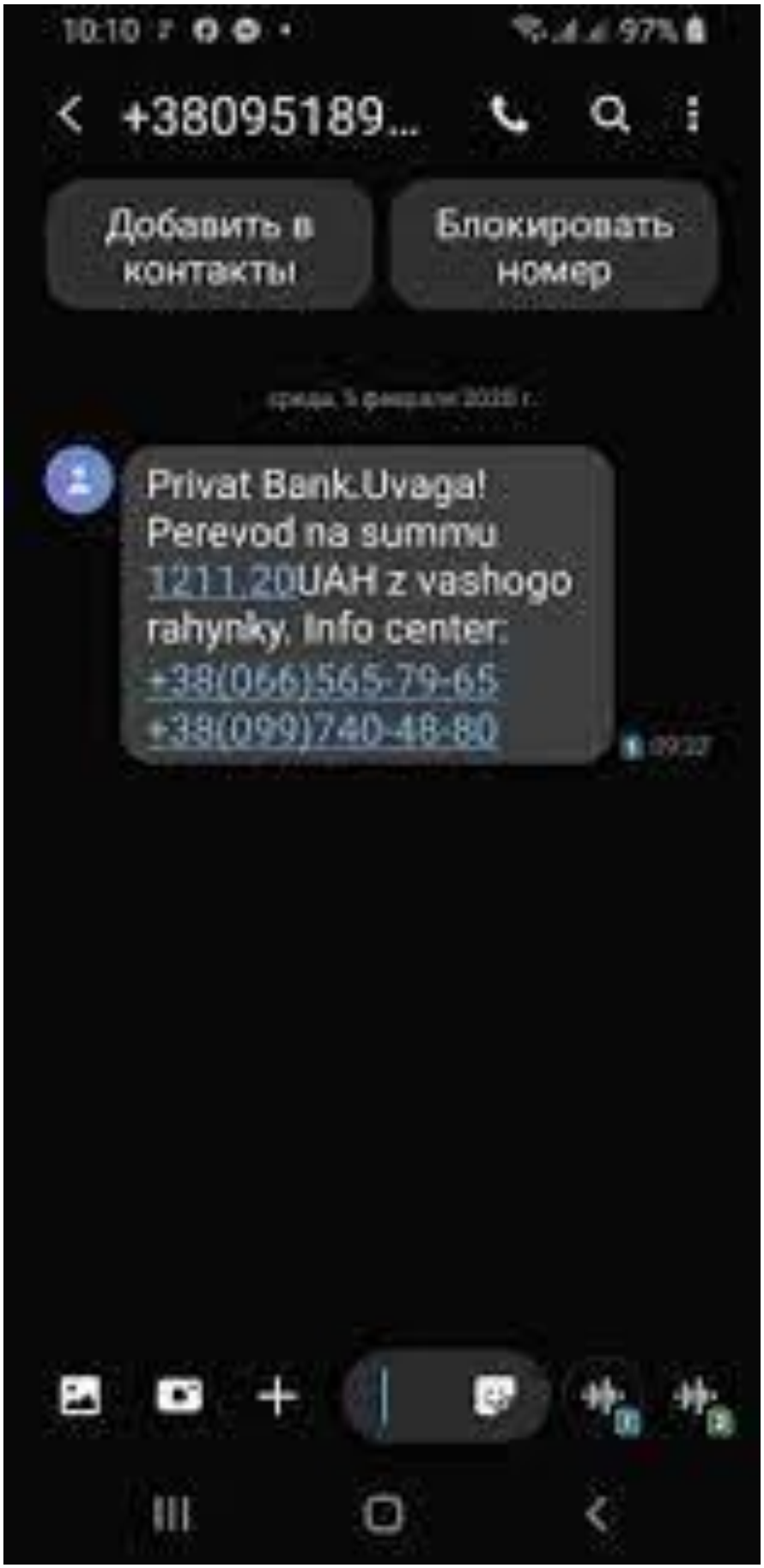
6.4K 16:32

До турніру 🚀


●●●●● Vodafone UA 3G
14:25
96 %
2
+380 (91) 985 27 09
SMS/MMS
Сегодня 14:24
"OSHADBANK" VASHU KARTKU ZABLOKOVANO Dlya razblokyvanya zvernicya do kontakt-centru za nom. 0919852709 goryacay liniya OSHADBANKA
SMS/MMS


Vodafone UA
17:30
81 %
+380 (63) 499 88 91
SMS/MMS
Сегодня 16:04
Vasha kartka zablokovana Bankom. Balance 0.00 UAH. Proidit avtorizaciu abo telefonuite:
0577555592
Call-centre
SMS/MMS


07:31
+38094...
Сьогодні
Shanovnuy kliente po vashiy kartci zafiksovano shahrayski diy, detali info-centre: +38(094) 440-02-54 +38(099) 302-68-21
Kyivstar 02:58
Наберіть текстове повідомленя


10:10
97%
+38095189...
Добавить в контакты
Блокировать номер
Privat Bank.Uvaga! Perevod na summu 1211,20UAH z vashogo rahynky. Info center: +38(066)565-79-65 +38(099)740-48-80


❤️ До **Дня Валентина** ігровий клуб дарує *до 200%* закоханим та азартним.
⚡ Щоб отримати подарунок, виконай кілька дій:
👉 Авторизуйся у профілі.
👉 Відкрий розділ з бонусами.
👉 Введи промокод.
👉 Поповни депозит.
🔥 З кодом **CUPID23** за поповнення *від 400 ₴* ти отримаєш *100%*. А якщо покладеш на рахунок *600 ₴* та введеш код **FOREVER23**, активуєш *200%*.
💕 Пропозиція діє *до 14 лютого*, тому поспішай!
✈️ А також використовуй промокод **PIN2022**, щоб отримати додатковий подарунок під час реєстрації.
👍 11
👎 2
🔥 2
6.6K 17:00
Отримати бонус ❤️

Українські ліцензійні казино🇺🇦

👑 **Зала Слави** СлотоКінг вже чекає на тебе!

💰 Стань легендою онлайн-казино та забирай *нагороди*.

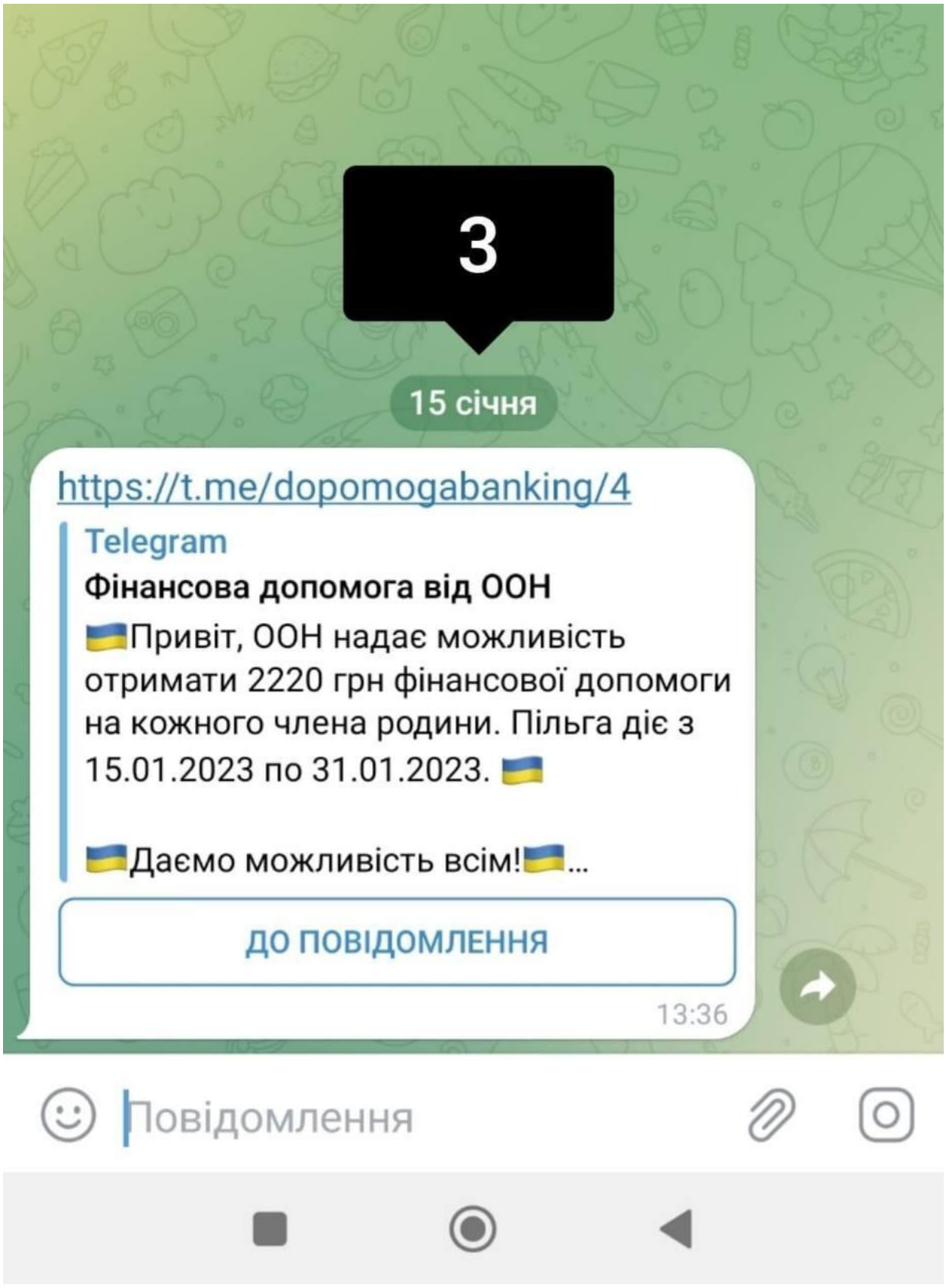
😎 Встановити власний рекорд дуже легко:

👉 Грай в автомати зі ставкою *від 0,9 ₴*.
👉 Просувайся в **рейтингу** та покращуй результат.
👉 Отримай *приз* у кінці тижня.

🚀 Серед номінацій ти можеш посісти своє почесне місце у *Топ-20* як **Марафонець**, **Капітан ІКС** або **Чорнокнижник**.

👌 Автоматично отримай приз – *фріспіни*. А якщо будеш наполегливим, зможеш розраховувати одразу на **кілька нагород**!

💸 Та обов'язково використай промокод **UA1BONUS**, щоб отримати крутий бонус.


3
15 січня
https://t.me/dopomogabanking/4
Telegram
Фінансова допомога від ООН
🇺🇦Привіт, ООН надає можливість отримати 2220 грн фінансової допомоги на кожного члена родини. Пільга діє з 15.01.2023 по 31.01.2023. 🇺🇦
🇺🇦Даємо можливість всім!🇺🇦...
ДО ПОВІДОМЛЕННЯ
13:36
Повідомлення

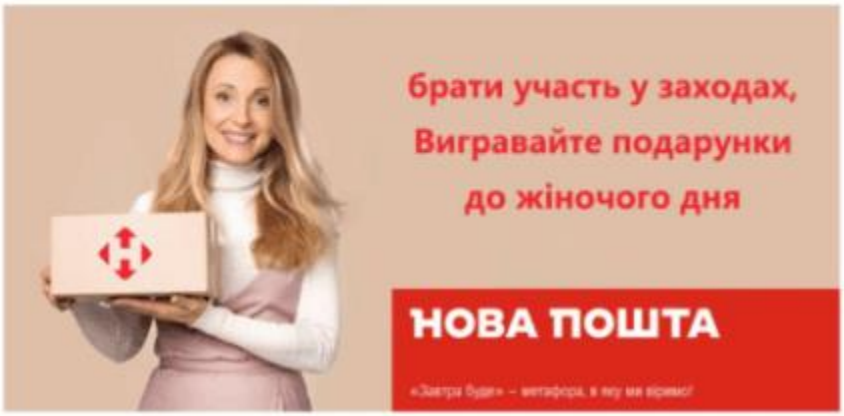
НОВА ПОШТА

Нова пошта подарунок до жіночого дня 8 березень, 2023

Щиро вітаю!

Нова пошта подарунок до жіночого дня

Через анкету ви матимете шанс отримати 6000 гривен .



Запитання 1 із 4: Ви знаєте Нова пошта?

так

ні

Варвара Игнатова
26 грудня 2022 р. о 14:47 ·

❗ВАЖЛИВА ІНФОРМАЦІЯ❗
Грошова виплата у зв'язку з енергетичною ситуацією в країні, які стартували з 20.12.2022р. кожен Українець може отримати одноразову виплату у розмірі 3000 гривень.
Інструкція як отримати кошти:
1. Переходячи по адресу для отримання виплат.
2. Натискаєте "Отримати".
3. Авторизація в особистому кабінеті банку.
4. Отримання виплати протягом 15-ти хвилин.
Адреса для отримання 3000 гривень ⬇️
✅ ОЩАДБАНК:https://oschad.pay-xec.me/opersonal/2996749160
✅ ПриватБанк:https://next24.pay-xec.me/personal/3737460418
✅ А-БАНК:https://a-bank.pay-xec.me/apersonal/7663747612
✅ ПУМБ:https://pumb.pay-xec.me/ppersonal/6994370065
✅ РАЙФАЙЗЕН:https://raif.pay-xec.me/rpersonal/2389095075

💸 Кешбек до 60% в онлайн-казино GGPoker для кожного!

🐟 Зустрічай крутезну програму лояльності **Fish Buffet**, яка дозволить повертати гроші від 🍒 програшних ставок.

💰 На тебе чекає **5 рангів**, кожен з яких підвищує кешбек:

👉 **Platinum Fish** – *20%*
👉 **Platinum Octopus** – *35%*
👉 **Platinum Whale** – *50%*
👉 **Platinum Shark** – *55%*
👉 **GGPlatinum** – *60%*

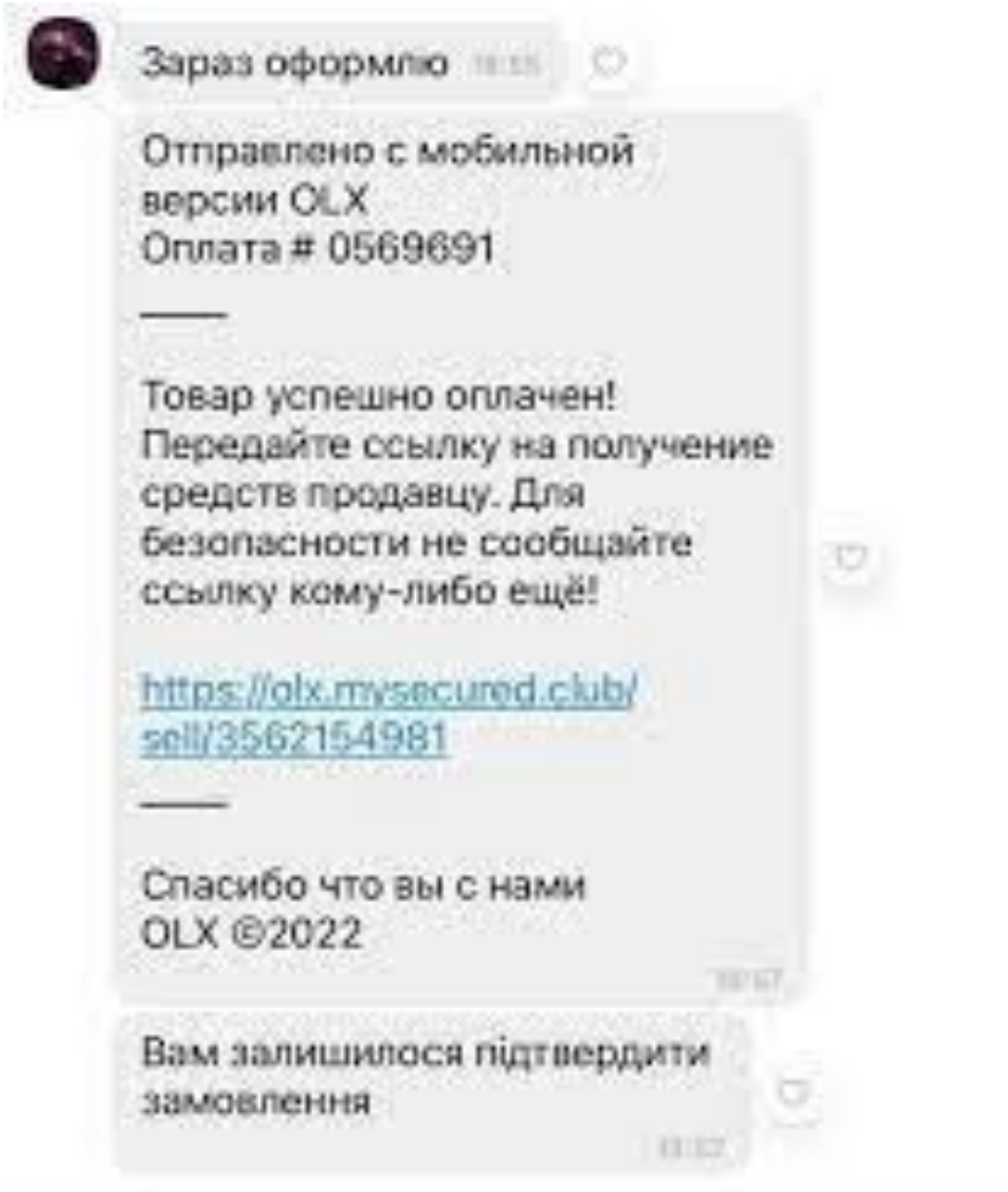
🚀 Грай в ігри з реальними круп'є та у будь-які слоти 🎰.

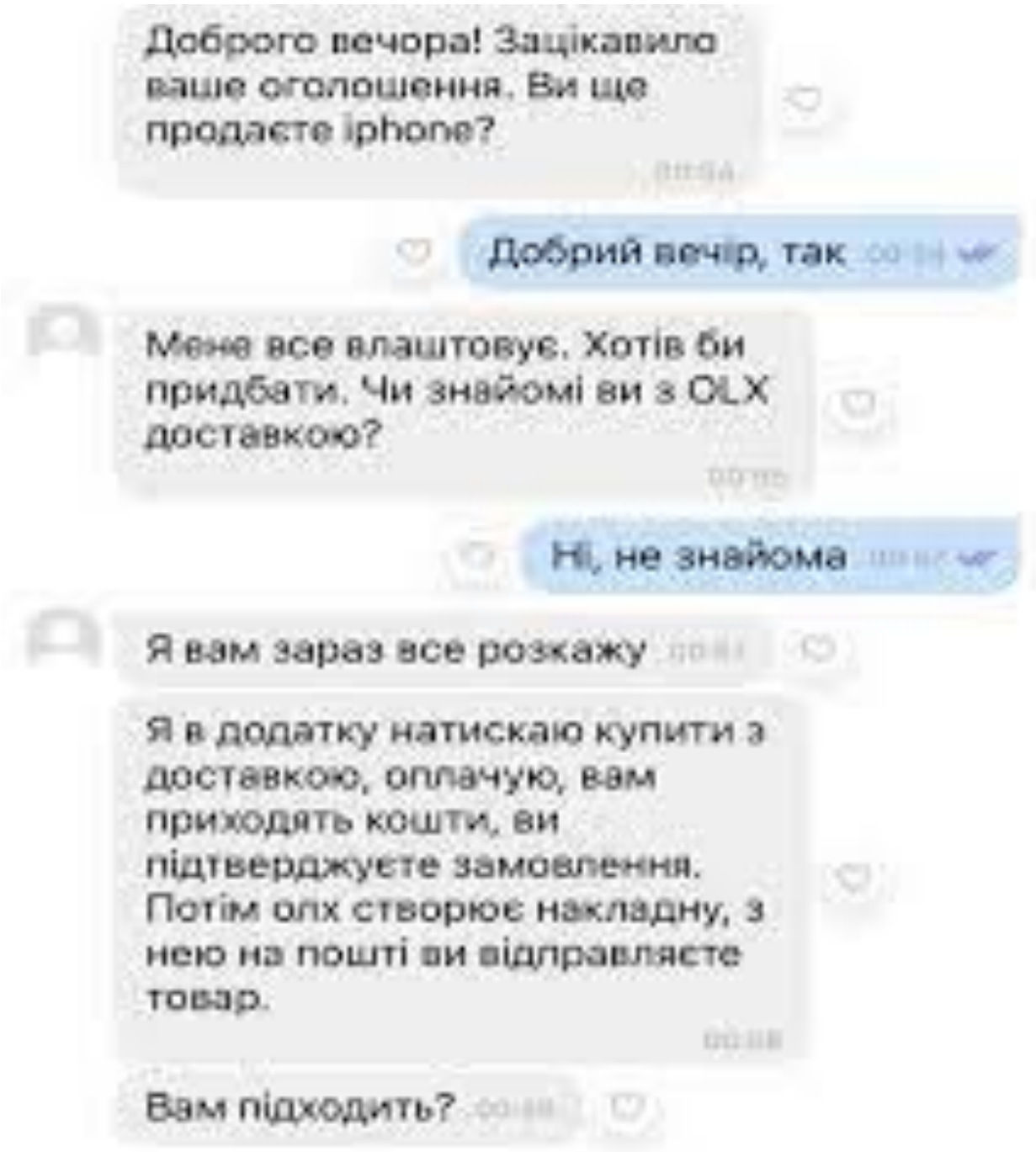
👌 Набирай бали та підвищуй ранг, щоб отримати максимальний 💰 **кешбек**.

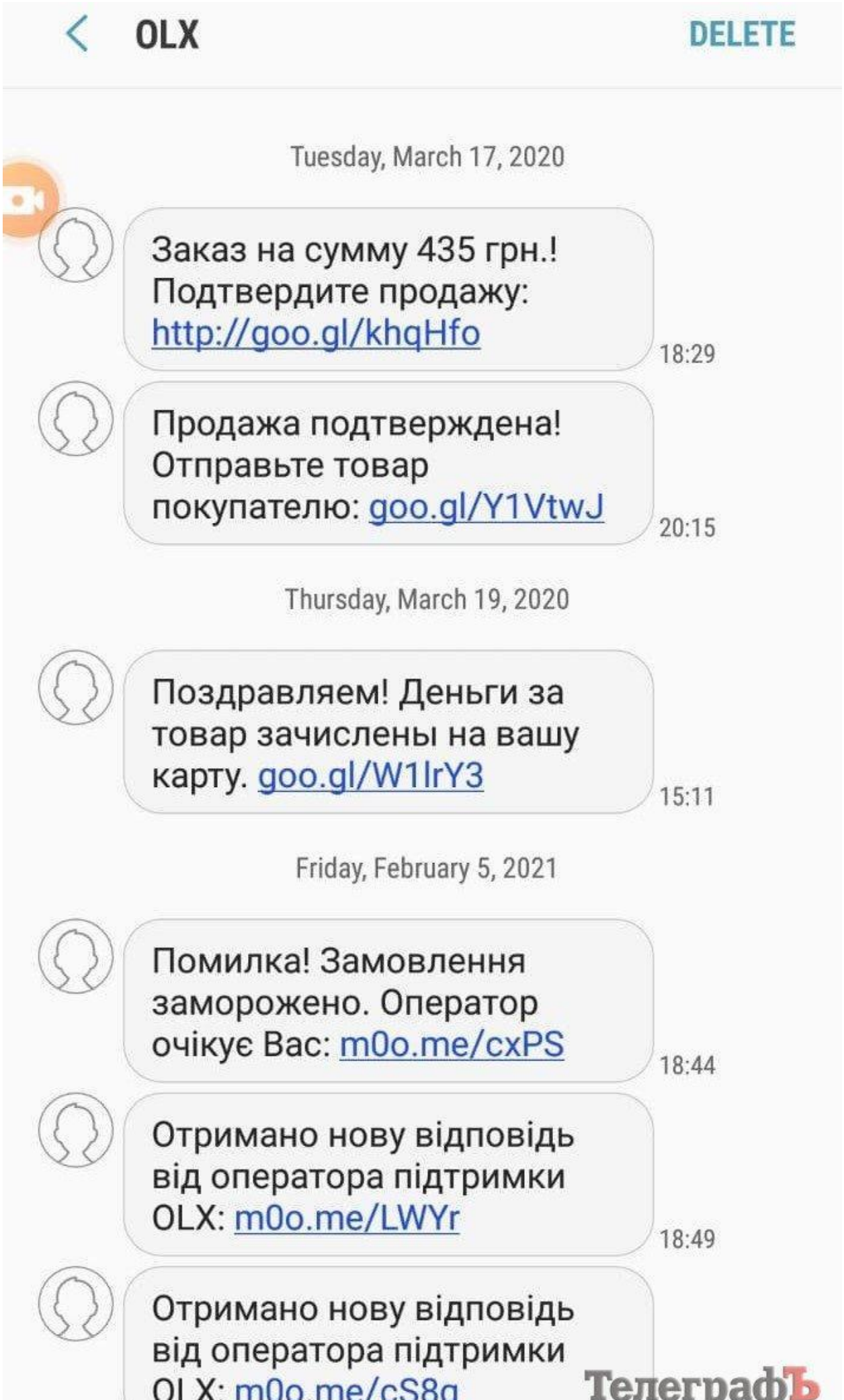
👍 14 ❤️ 7 ❤️‍🔥 1

4.9K 21:23

Кешбек Fish Buffet 🐟


Зараз оформлю
Отправлено с мобильной версии OLX
Оплата # 0569691
———
Товар успешно оплачен! Передайте ссылку на получение средств продавцу. Для безопасности не сообщайте ссылку кому-либо ещё!
https://olx.mysecured.club/sell/3562154981
———
Спасибо что вы с нами
OLX ©2022
Вам залишилося підтвердити замовлення


Доброго вечора! Зацікавило ваше оголошення. Ви ще продаєте iphone?
Добрий вечір, так
Мене все влаштовує. Хотів би придбати. Чи знайомі ви з OLX доставкою?
Ні, не знайома
Я вам зараз все розкажу
Я в додатку натискаю купити з доставкою, оплачую, вам приходять кошти, ви підтверджуєте замовлення. Потім олх створює накладну, з нею на пошті ви відправляєте товар.
Вам підходить?


OLX
DELETE
Tuesday, March 17, 2020
Заказ на сумму 435 грн.! Подтвердите продажу: http://goo.gl/khqHfo
18:29
Продажа подтверждена! Отправьте товар покупателю: goo.gl/Y1VtwJ
20:15
Thursday, March 19, 2020
Поздравляем! Деньги за товар зачислены на вашу карту. goo.gl/W1lrY3
15:11
Friday, February 5, 2021
Помилка! Замовлення заморожено. Оператор очікує Вас: m0o.me/cxPS
18:44
Отримано нову відповідь від оператора підтримки OLX: m0o.me/LWYr
18:49
Отримано нову відповідь від оператора підтримки
ТелеграфЪ

Українські ліцензійні казино🇺🇦

🎰 Новий автомат в First Casino вже чекає на тебе.

😉 Крута новина, яку ти мусиш знати! У казино з'явився слот 💰 **Cash Streak** від *Endorphina*.

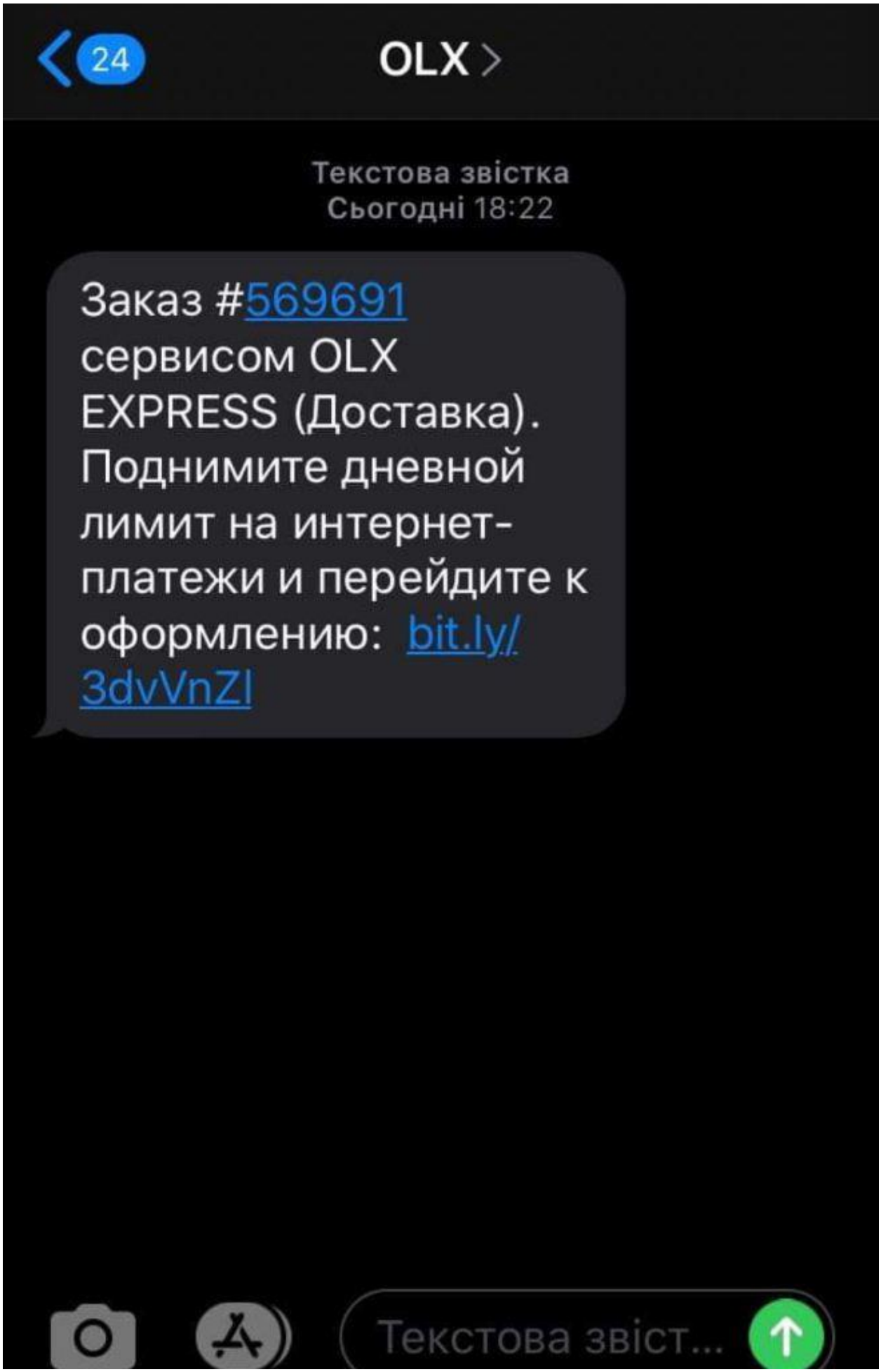
👉 Цей автомат має показник віддачі понад 96%. Тому тобі буде дуже легко виграти 💸.

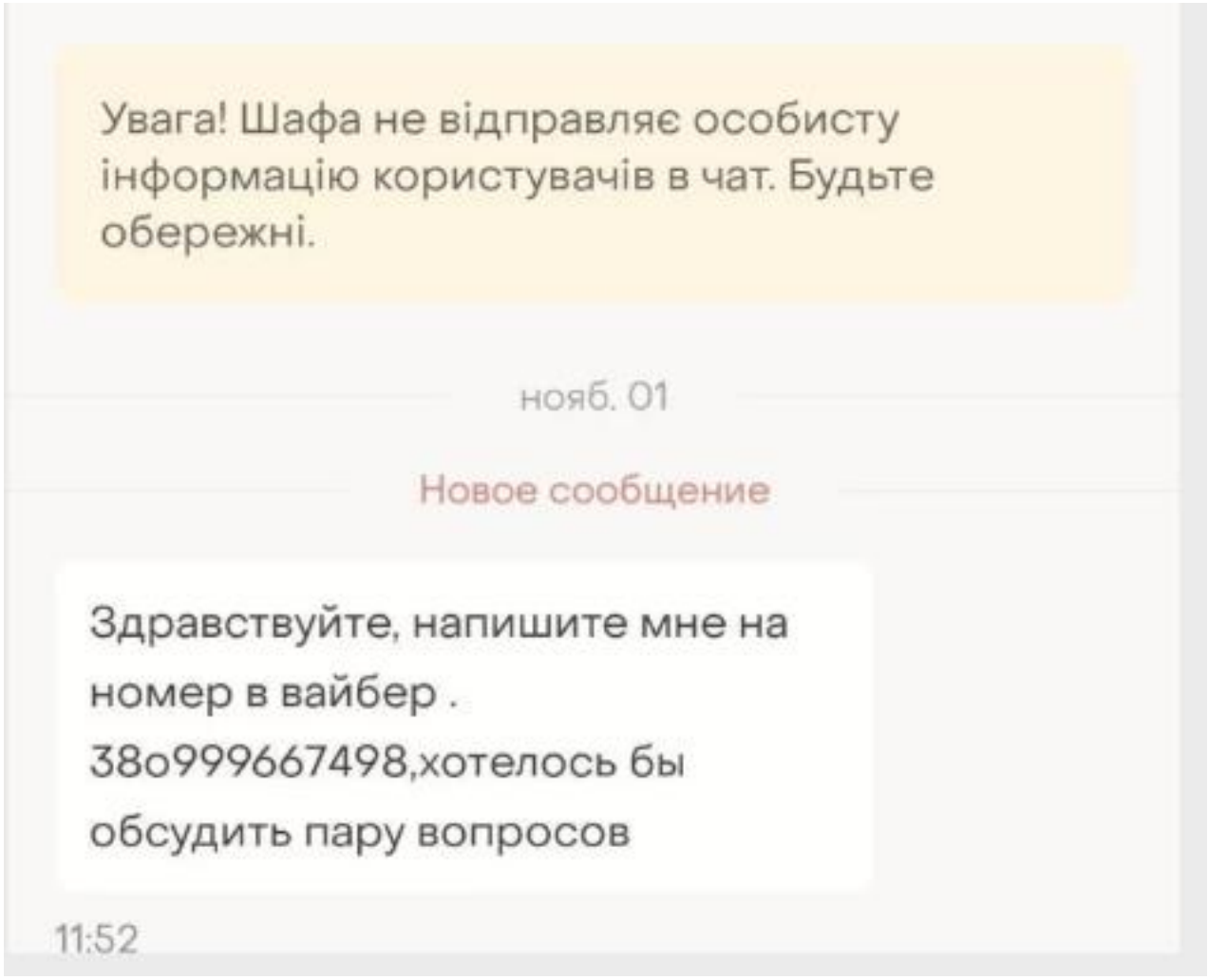
🍒 Крім того, на тебе чекають 🚀 **множники x2**, 😎 **фріспіни** та 💣 **додаткова гра**.

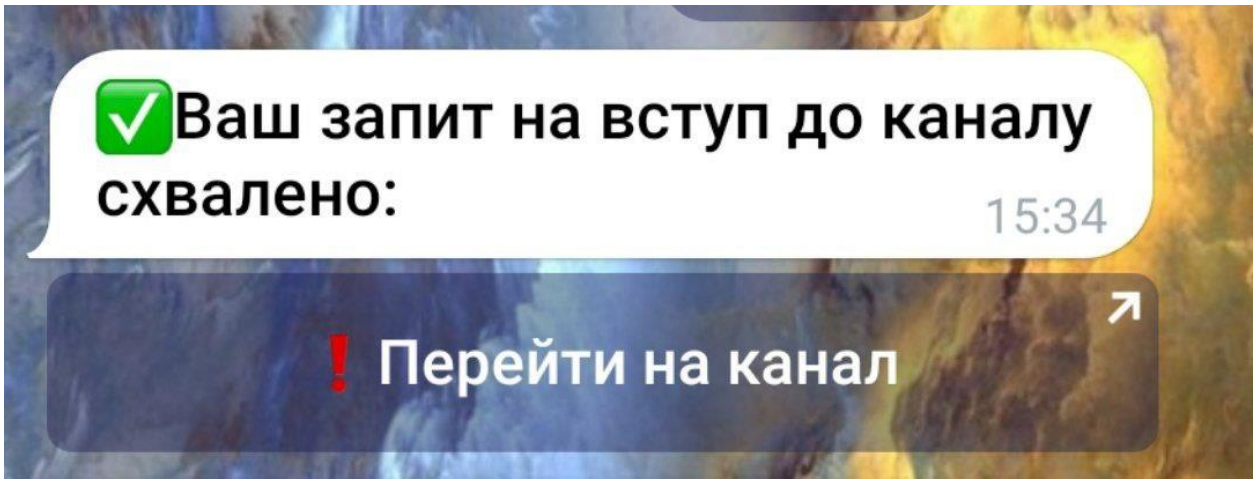
🎁 А також використай промокод **UA1BONUS**, щоб отримати бонус!

👍 19 ❤️ 2 😄 2 🥰 1 🤪 1

3.9K 15:00


24
OLX
Текстова звістка
Сьогодні 18:22
Заказ #569691 сервисом OLX EXPRESS (Доставка). Поднимите дневной лимит на интернет-платежи и перейдите к оформлению: bit.ly/3dvVnZl
Текстова звіст...


Увага! Шафа не відправляє особисту інформацію користувачів в чат. Будьте обережні.
нояб. 01
Новое сообщение
Здравствуйте, напишите мне на номер в вайбер . 38o999667498,хотелось бы обсудить пару вопросов
11:52


✅Ваш запит на вступ до каналу схвалено:
15:34
❗ Перейти на канал

Поняла вас, я сейчас вам объсяню как работает доставка от шафа

13:52

shafa

powered by shafa

Как работает оплата заказа и доставка?

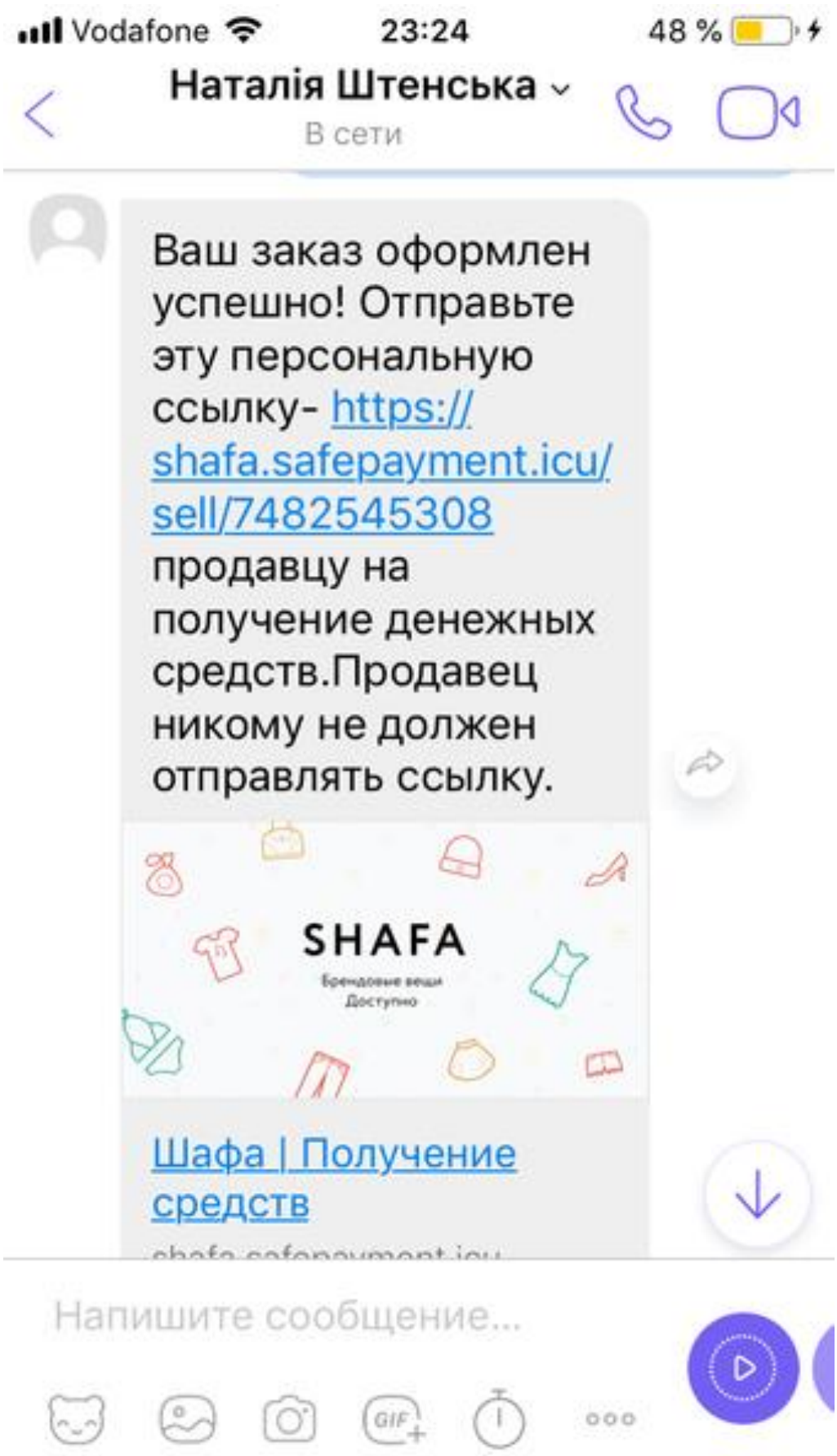
Покупатель выбирает понравившийся товар и оформляет доставку

Покупатель оплачивает товар и доставку, получая ссылку на заказ, которую передает продавцу

Продавец подтверждает заказ и получает денежные средства на банковскую карту

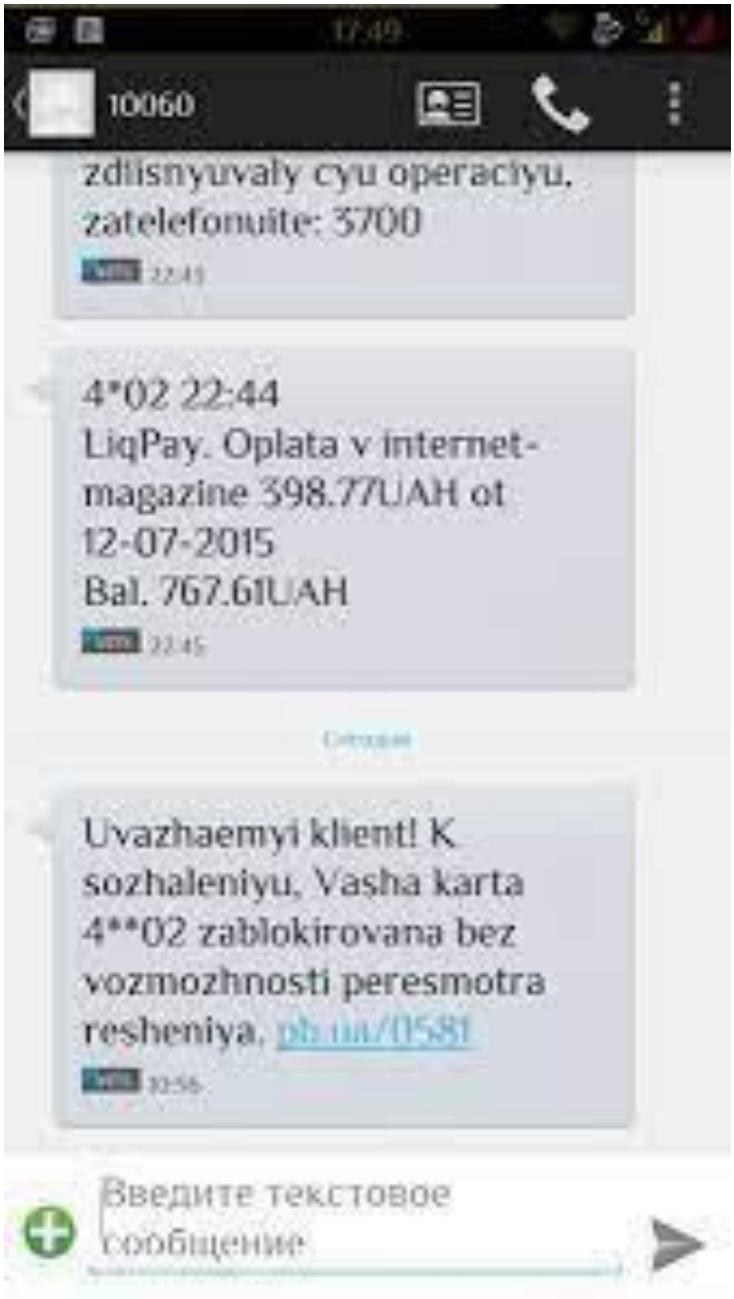
Продавец отправляет посылку в отделении “Нова Пошта” или встречается с курьером

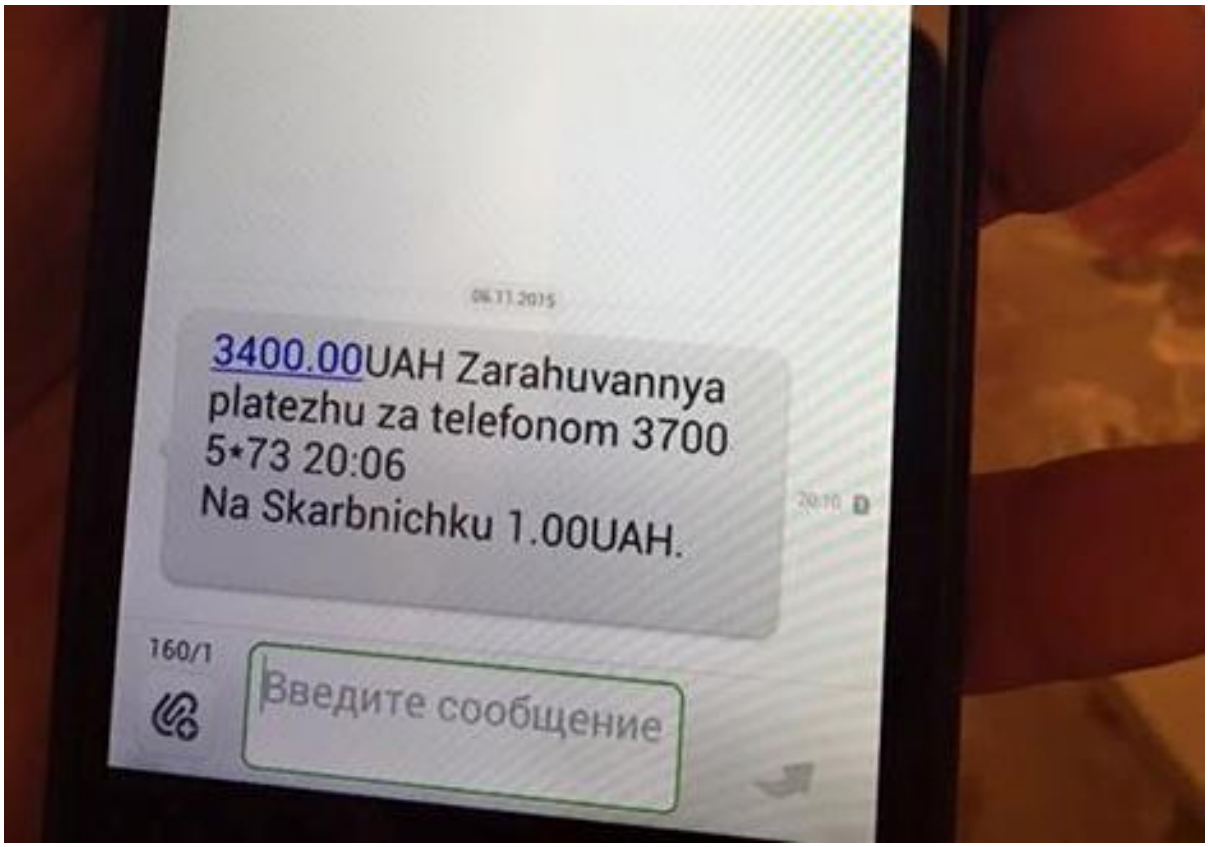
13:52

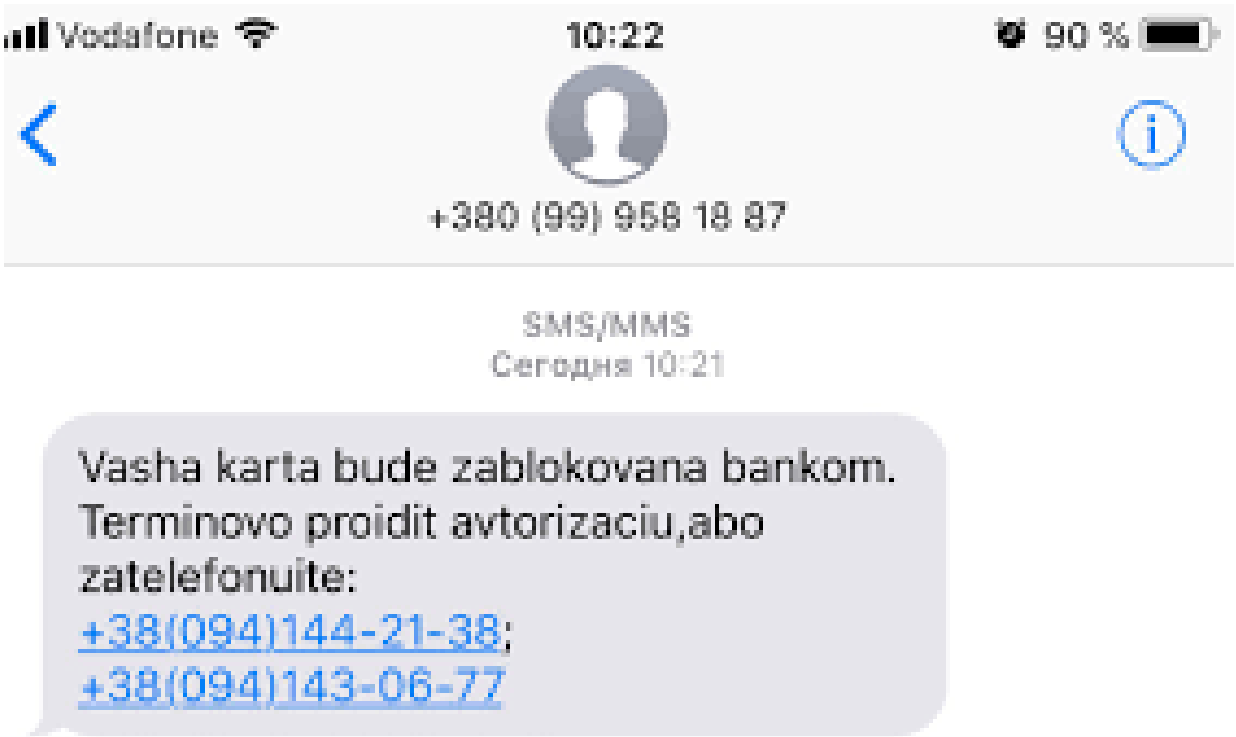

Vodafone
23:24
48 %
Наталія Штенська
В сети
Ваш заказ оформлен успешно! Отправьте эту персональную ссылку- https://shafa.safepayment.icu/sell/7482545308 продавцу на получение денежных средств.Продавец никому не должен отправлять ссылку.
SHAFA
Брендовые вещи
Доступно
Шафа | Получение средств
Напишите сообщение...

Сегодня 15:20

Дарим 1000 UAH своим преданным клиентам. Подробнее: prlvatbank24.pw



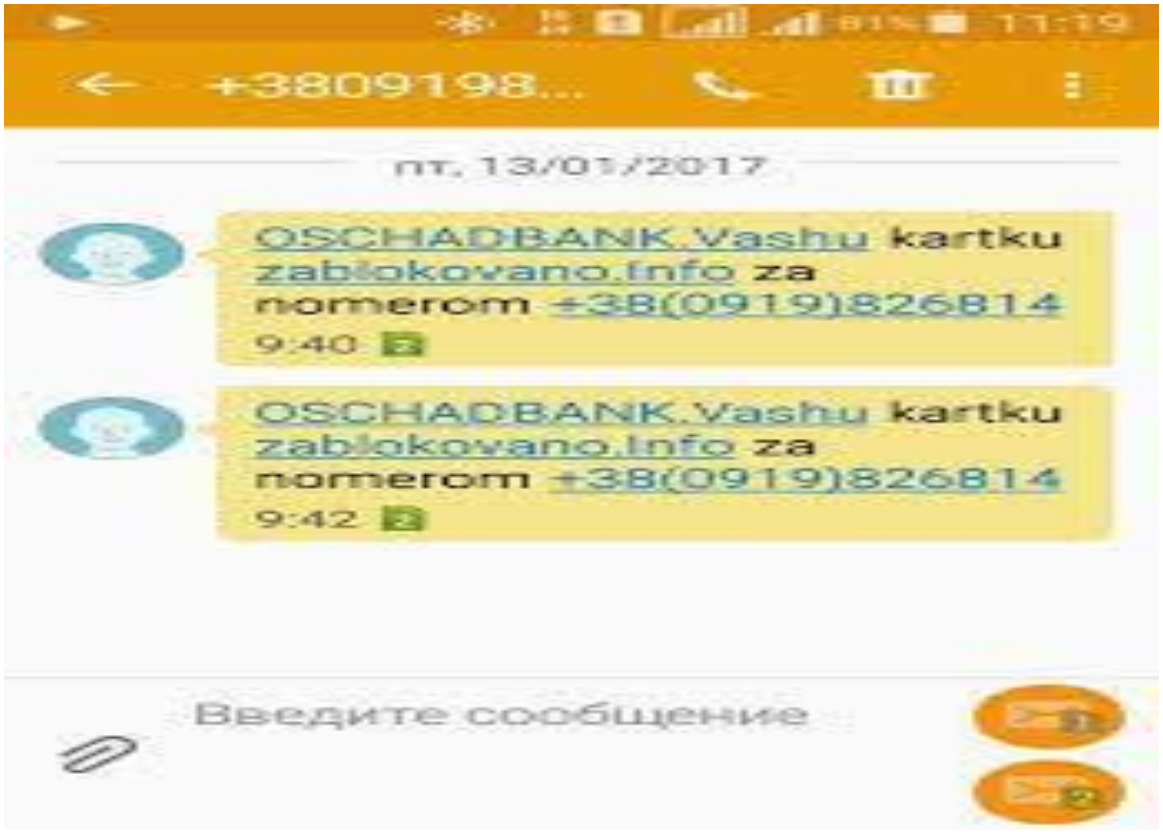

3400.00UAH Zarahuvannya platezhu za telefonom 3700 5*73 20:06
Na Skarbnichku 1.00UAH.
160/1
Введите сообщение


Vodafone
10:22
90 %
+380 (99) 958 18 87
SMS/MMS
Сегодня 10:21
Vasha karta bude zablokovana bankom. Terminovo proidit avtorizaciu,abo zatelefonuite:
+38(094)144-21-38;
+38(094)143-06-77

Текстова звістка
сб, 31 бер., 14:12

Vasha kartka bude zablokovana bankom. Terminovo proidit avtorizaciu,abo zatelefonuite +(380)-44-332-97-91 +(380)-44-221-35-91

ВОЛИНСЬКІ НОВИНИ



Українські ліцензійні казино🇺🇦

💣 Акція **Drops & Wins** в онлайн-казино Vulkan Casino!

🔥 Долучайся до турнірів від провайдера 🔔 **Pragmatic Play** та бери участь у розіграшах:

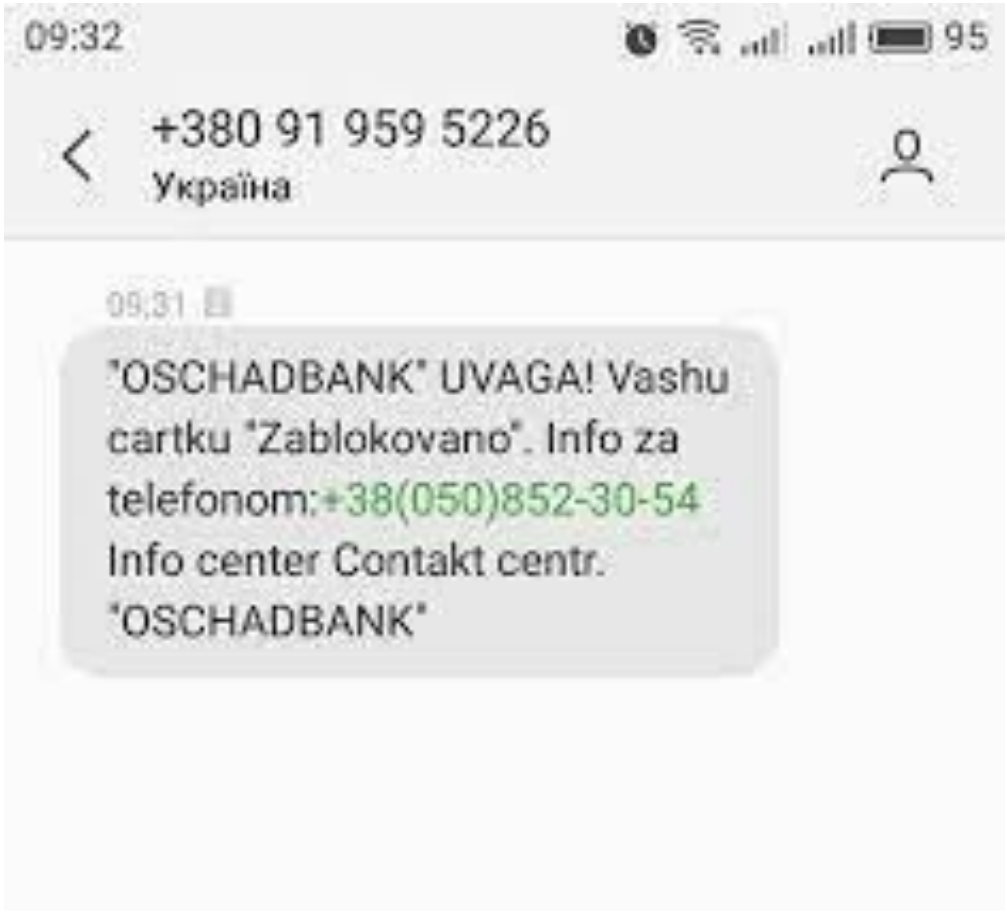
👉 **12 турнірів щотижня** з виграшним банком в *2 418 000 ₴*.
👉 **84 щоденних розіграшів** з призовим фондом в *351 000 ₴*.
👉 **Фінальний Drops & Wins**, у якому розігрується *58 500 000 ₴*.

🎁 Акція діє до *3 травня 2023 року*.

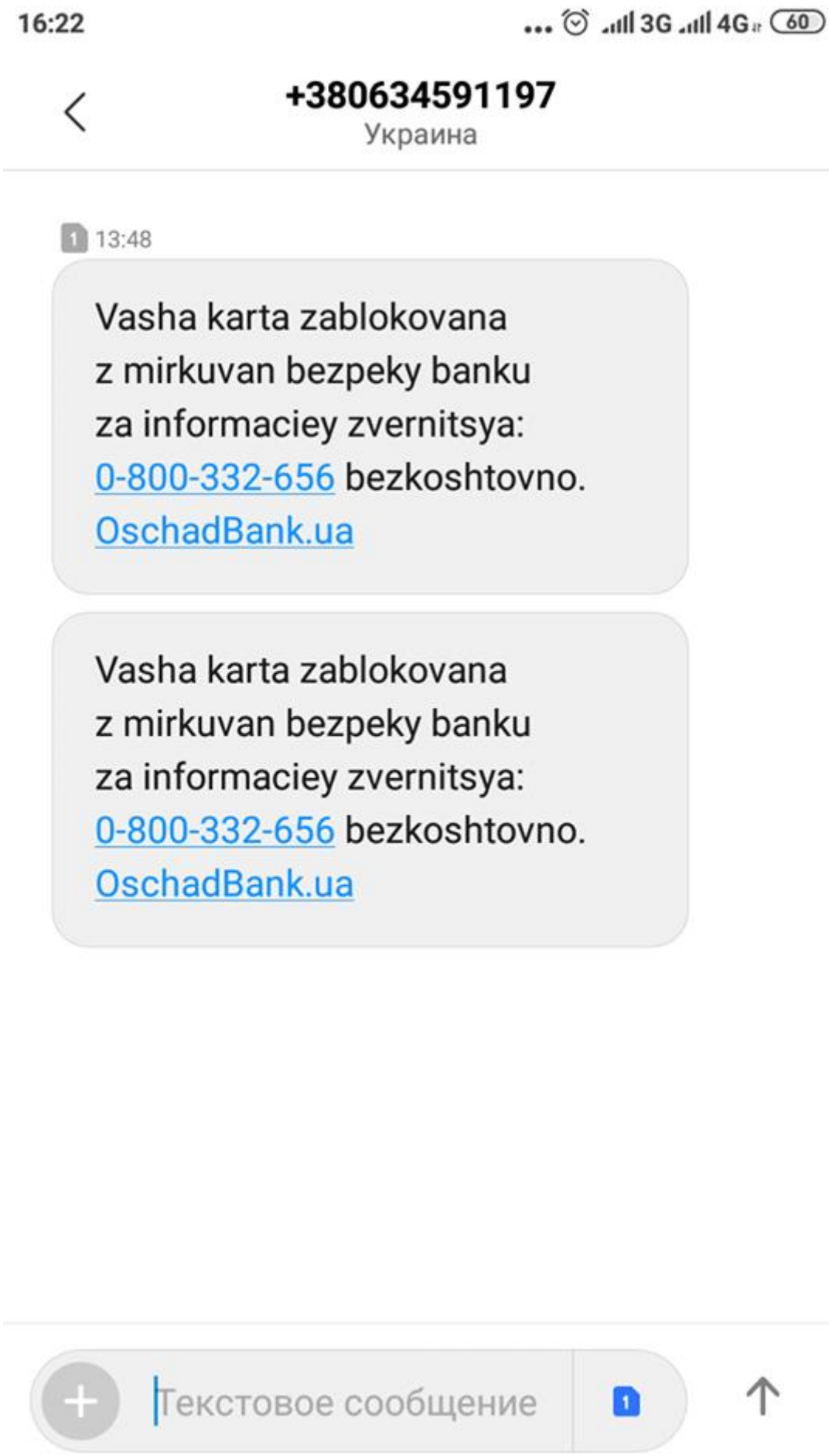
😎 Грай у слоти провайдера, накопичуй бали та вигравай 💰 великі гроші.

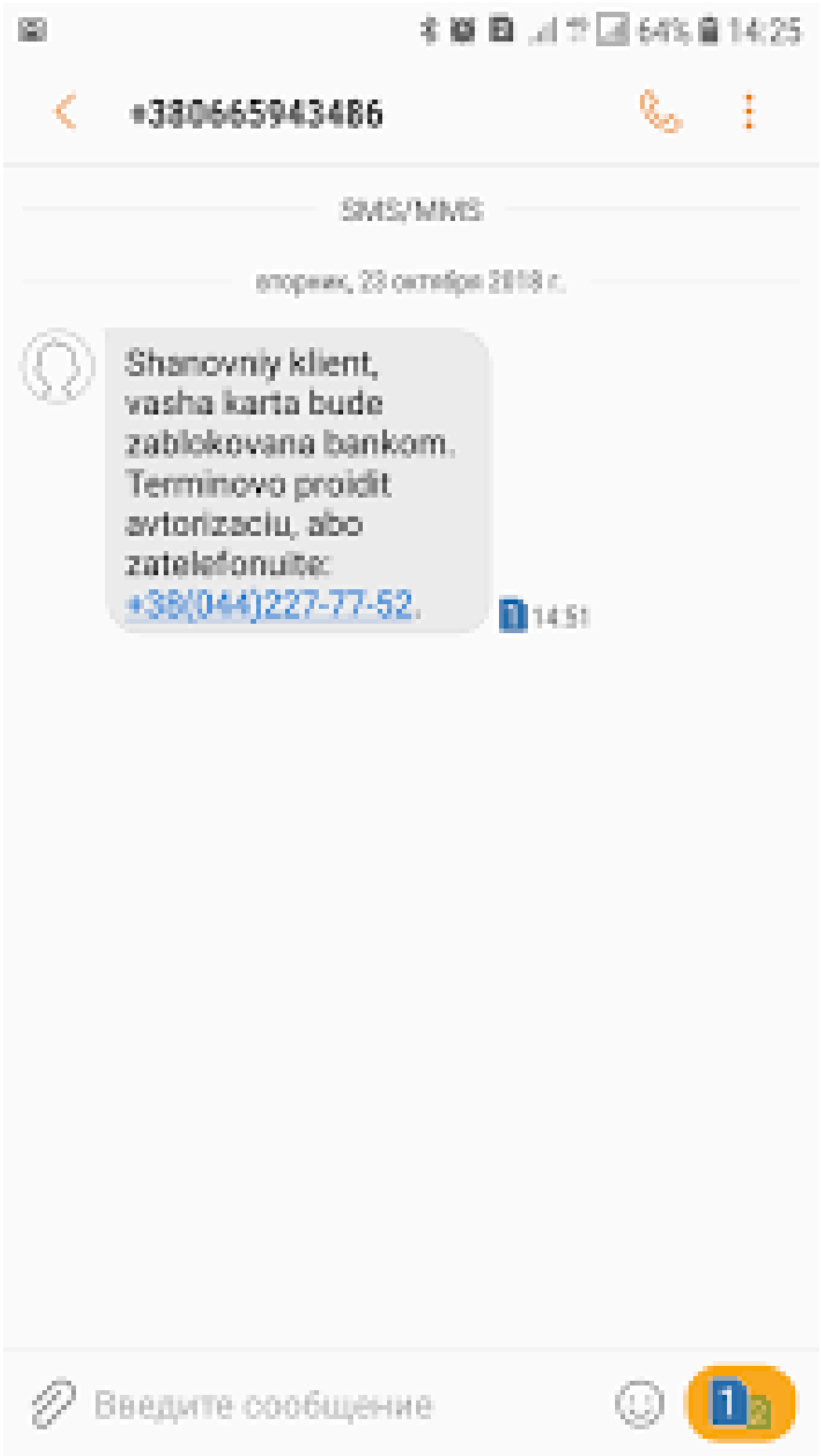
👍 11 ❤️ 1 👏 1

3.7K 18:00


09:32
95
+380 91 959 5226
Україна
09:31
"OSCHADBANK" UVAGA! Vashu cartku "Zablokovano". Info za telefonom:+38(050)852-30-54 Info center Contakt centr. "OSCHADBANK"


+380919384727
Украина
SMS/MMS
27-2 12:35
Uvaga! Vaha kartka zablokovana. Za dopomogoy telefonuyte za nomerom +380950868894 abo www.ohadbank.ua


16:22
3G 4G 60
+380634591197
Украина
13:48
Vasha karta zablokovana
z mirkuvan bezpeky banku
za informaciey zvernitsya:
0-800-332-656 bezkoshtovno.
OschadBank.ua
Vasha karta zablokovana
z mirkuvan bezpeky banku
za informaciey zvernitsya:
0-800-332-656 bezkoshtovno.
OschadBank.ua
Текстовое сообщение


64% 14:25
+380665943486
SMS/MMS
вторник, 23 октября 2018 г.
Shanovniy klient, vasha karta bude zablokovana bankom. Terminovo proidit avtorizaciu, abo zatelefonuite: +38(044)227-77-52.
14:51
Введите сообщение

‼️ОФІЦІЙНО

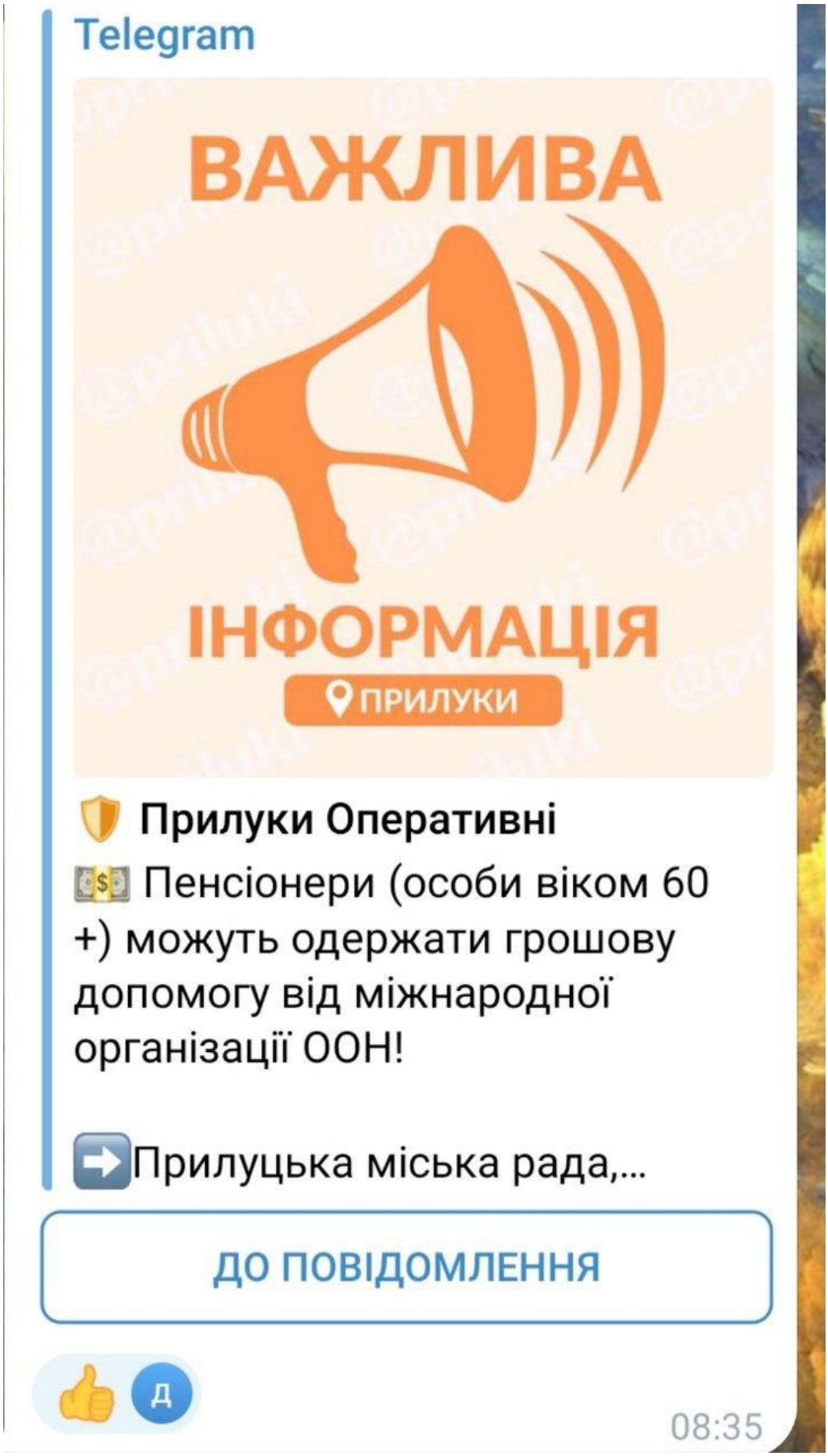
⚡Українські сім'ї можуть отримати грошову допомогу в **33 000 гривень**

🔴 ЧІТКА ІНСТРУКЦІЯ, ЯК ПОДАТИ ЗАЯВКУ ТА ОТРИМАТИ ВИПЛАТУ

***ВАЖЛИВО:** *Родина отримає одноразову виплату на вказаний банківський рахунок чи дебетову картку протягом 4 тижнів з моменту подання заявки. Переконайтеся, що у вас є доступ до рахунка перед поданням заявки.*

💩 1.5K 👍 221 👎 214 🤬 55
😁 31 🤔 28 🤢 27 👏 7 🥰 6
🔥 3

👁 150.1K 19:00


Telegram
ВАЖЛИВА
ІНФОРМАЦІЯ
ПРИЛУКИ
Прилуки Оперативні
Пенсіонери (особи віком 60 +) можуть одержати грошову допомогу від міжнародної організації ООН!
Прилуцька міська рада,...
ДО ПОВІДОМЛЕННЯ
08:35


#реклама
❗ ВІДНОВЛЕНО ВИПЛАТУ 6600 ГРН: українці можуть отримати від ООН грошову допомогу.
➡️Як правильно подати заявку на грошову допомогу від УВКБ ООН розповіли тут 👇
https://t.me/+hM6MjRceCoE4ZmY6
87
16
16
12
5
4
3
18K 17:00
Ознайомитися