ВЗАЄМОЗАЛЕЖНІСТЬ ОСОБЛИВОСТЕЙ ПСИХІКИ КОРИСТУВАЧІВ ІНТЕРНЕТ-СЕРЕДОВИЩА ТА МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

INTERDEPENDENCE OF PSYCHOLOGICAL FEATURES OF INTERNET USERS AND SOCIAL ENGINEERING METHODS

УДК 004.056.5:159.9
DOI https://doi.org/10.32782/2663-5208.2024.66.40

Терентьєва Н.О.
д.пед.н.,
професор кафедри психології
Чорноморський національний університет імені Петра Могили

Фалько Н.І.
студентка 6 курсу другого (магістерського) рівня вищої освіти за спеціальністю 053 – Психологія
Чорноморський національний університет імені Петра Могили

У статті розглядається вплив соціальної інженерії на психіку користувачів Інтернету в умовах стрімкого розвитку інформаційних технологій. У 2024 році кількість користувачів Інтернету досягла 5,44 мільярда осіб, що становить приблизно 67,1% від усього населення планети, що призводить до зростання випадків онлайн-шахрайства та кіберзлочинів. Поширення соціальної інженерії, що ґрунтується на маніпуляції емоціями та психологічними особливостями людей, сприяє створенню нових загроз.

Стаття наголошує на взаємозв'язок між особливостями людської психіки та методами соціальної інженерії. Підкреслюється, що сучасний стрес, викликаний як повсякденним життям, так і глобальними подіями (наприклад, війною), робить людей більш вразливими до маніпуляцій, наголошується на важливості підвищення обізнаності про методи соціальної інженерії, розвитку критичного мислення та обережності при спілкуванні в онлайн-просторі.

Дослідження аналізує ключові вразливості, зокрема довіру, страх, цікавість та емоційний стан користувачів, які зловмисники використовують для отримання доступу до конфіденційної інформації та фінансових ресурсів. Приділено увагу видам психологічних методів, що використовуються у шахрайстві, таким як тиск на час, авторитет, стадність і переконання. Доводиться, що визнаючи психологічні тригери та тривожні сигнали, пов'язані із соціальною інженерією, користувачі онлайн середовища зміцнюють свій захист від маніпулятивних кіберзлочинців.

Актуальність теми обумовлена збільшенням залежності від Інтернету та частотою кризових ситуацій, які послаблюють пильність користувачів. Автори акцентують на важливості розробки рекомендацій для захисту від шахрайства шляхом підвищення обізнаності та розвитку навичок критичного мислення. Стаття є внеском у поглиблення розуміння соціальної інженерії як загрози цифровій безпеці та пропонує основні принципи захисту користувачів у сучасному комунікаційному середовищі.

Ключові слова: *методи соціальної інженерії, вразливість, маніпуляція, стрес, психіка, шахрайство, кібербезпека, довіра, емпатія, авторитет.*

This article examines the influence of social engineering on the psyche of internet users amidst the rapid growth of information technology. In 2024, the number of internet users reached 5.44 billion, approximately 67.1% of the global population, leading to a surge in online fraud and cybercrime. The proliferation of social engineering, which exploits human emotions and psychological vulnerabilities, contributes to the emergence of new threats.

The article emphasizes the correlation between human psychological traits and social engineering techniques. It highlights how modern-day stress, induced by both daily life and global events (such as war), makes individuals more susceptible to manipulation. The importance of raising awareness about social engineering methods, fostering critical thinking, and exercising caution in online interactions is underscored.

The research analyzes key vulnerabilities, including trust, fear, curiosity, and emotional states, which cybercriminals exploit to gain access to confidential information and financial resources. The article delves into various psychological tactics employed in fraudulent schemes, such as time pressure, authority, social proof, and persuasion. It argues that by recognizing psychological triggers and red flags associated with social engineering, online users can strengthen their defenses against manipulative cybercriminals.

The timeliness of this topic is attributed to the increasing reliance on the internet and the frequency of crises that diminish user vigilance. The authors emphasize the importance of developing recommendations to protect against fraud by enhancing awareness and critical thinking skills. This article contributes to a deeper understanding of social engineering as a digital security threat and offers fundamental principles for safeguarding users in today's communication environment.

Key words: *social engineering techniques, vulnerability, manipulation, stress, psyche, fraud, cybersecurity, trust, empathy, authority.*

Сучасне суспільство переживає надзвичайно швидкий розвиток інформаційних технологій, що значно змінює спосіб комунікації та взаємодії людей. Інтернет, як один із ключових аспектів цього розвитку, став важливим чинником в побуті і діяльності сучасного індивіда. За даними дослідження, проведеного корпорацією Google, у 2024 році кількість користувачів Інтернету досягла 5,44 мільярда осіб, що становить приблизно 67,1% від усього населення планети.[1] Водночас, разом із зростанням використання Інтернету, зростає і вплив соціальної інженерії на особливості психіки користувачів. Соціальна інженерія, визначена як маніпулювання людськими діями, зокрема через психологічні методи, набуває нових форм та вимагає уваги як з боку дослідників, так і з боку суспільства загалом.

Актуальність дослідження полягає у зростаючій залежності усіх сфер життєдіяльності людини від Інтернету, збільшенні кількості і видів онлайн-шахрайств, кіберзлочинів та розробки ефективних стратегій захисту; Розуміння того, які механізми використовуються в соціальній інженерії, дозволяє розробити рекомендації та інструменти для захисту користувачів від психологічних маніпуляцій, використовуючи знання та дослідження різних галузей науки, таких як психологія, соціологія, ІТ-технологія, кібербезпека. Щодо

актуальності теми наведемо лише один приклад. За матеріалами прес конференції «Підсумки платіжного шахрайства у 2023 році в Україні: статистика, тренди», яка відбулася 25 січня 2024 року у 2023-му році відбулося 209 382 звернення громадян щодо шахрайства. Серед найпоширеніших схем онлайн-шахрайства: недоставка товару після передплати в мережі, дзвінки від імені банків, фішинг, прохання про допомогу через соцмережі.[2]

Динаміка і ритм сучасного життя, прагнення до успіху вимагають від людини постійною зібраності, концентрації уваги, мобілізації усіх сил. Це, у свою чергу, є причиною виникнення у людини численних стресів, депресій, коливань психоемоційного стану. Стреси займають значне місце в житті людей. Вони впливають на здоров'я, поведінку людини, взаємовідносини з іншими людьми, стосунки в сім'ї, працездатність, а отже, на досягнення або недосягнення людиною успіху Війна, яка триває вже понад 2 роки, ще більш додали напруженості, психіка людини приходить в стресовий стан і запускаються адаптаційні процеси. Організм використовує резерви, які в нормі не задіяні, когнітивні функції стають обслуговуючими і реагують на емоційний стан, тому пам'ять і увага на якийсь період часу погіршуються. Наслідком цього може стати підвищена схильність до впливу шахраїв або соціальних інженерів. Якщо в звичайному стані людина не схильна вірити в «підозрілі транзакції», про які повідомляють з незнайомого номера, в стані стресу тривожність перемагає, і людина стає жертвою [5].

Соціальна інженерія опирається на психологічні особливості людини, такі як: я повинен зробити так, бо більшість так би і зробили (ми оцінюємо свою поведінку на фоні поведінки більшості); повага до авторитетних людей чи державних установ (ми будемо більше довіряти поліцейському, банківському працівнику, лікаря тощо аніж пересічній людині).

Усі види методів соціальної інженерії спираються на слабкість людської психології. Шахраї використовують емоції, щоб маніпулювати та обманювати своїх жертв. Людський страх, жадібність, цікавість і навіть готовність допомагати іншим обертаються проти них різними методами [7].

Ми розглядаємо такі установки, пов'язані з атаками соціальної інженерії: ставлення довіри, ставлення підозрілості та ставлення до ризику. Ці установки впливають на сприйнятливість людини до атак соціальної інженерії. Що стосується ставлення довіри, то високий рівень довіри створює високу сприйнятливість до атак соціальної інженерії і шахрайства. Для підозрілого ставлення особа з високою підозрілістю менш сприйнятлива до атак соціальної інженерії. Що стосується ставлення до ризику, то високе сприйняття ризику знижує сприйнятливість до атак соціальної інженерії, а низьке сприйняття ризику підвищує сприйнятливість до шахрайства [11].

Щоб підвищити шанси на успіх, такі психологічні методи можуть бути використані для створення повідомлень: переконання, шахрайство, стимул і мотивація, а також інтуїтивний тригер. Переконання – це акт представлення аргументу, який спонукає індивіда поводитися бажаним чином. Шахрайство (або обман) – це акт подання аргументу з наміром створити хибне переконання. Стимули та мотиватори заохочують співпрацю, де стимули використовують зовнішні винагороди, а мотиватори – внутрішні психологічні властивості. Вісцеральні тригери – це мотиваційні маніпуляції, які викликають емоційну реакцію шляхом використання потреб і бажань [11].

Сальнікова А. Стверджує, що аферисти в основному використовують такі методи, як фактор часу. Вмовляють жертву швидко прийняти рішення, не залишаючи їй можливості раціонально оцінити ситуацію. А також фактор поваги авторитету. Психологічний тиск з боку шахрая. Використання нашої доброти проти нас самих – листи з благанням про допомогу. Фактор стадності базується на нашій схильності копіювати поведінку друзів або людей, які поруч з нами, з метою посипання нашої пильності.

В основі шахрайства лежить принцип маніпуляції нашою вірою. Але взагалі нікому не вірити не вихід. Потрібно вірити, але не бути занадто легковірними. Не слід бути занадто відвертими. Шахраї дуже вміло використовують будь-яку інформацію, щоби втертися в довіру. Особливо обережними потрібно бути з інформацією, яку користувачі повідомляють про себе в інтернеті, у соціальних мережах. Найбільше шансів у аферист тоді, коли користувач знаходиться у стані емоційного спаду. Психологи рекомендують не квапитися, раціонально осмислити те, що відбувається.

Пильність – це процес виділення когнітивних ресурсів для виконання складного завдання, такого як виявлення ознак, які можуть вказувати на оманливі наміри в повідомленні. Варто підкреслити, що на пильність впливає підозрілість.

Більшість людей асоціюють довіру в онлайн-просторі з поверхневими атрибутами, такими як професійний вигляд веб-сайту або наявність високоякісного та насиченого контенту. Довіра зменшує підозри, покращує переконливість повідомлення і підвищує сприйнятливість жертв до атак соціальної інженерії. Довіра до зловмисника характеризується такими атрибутами: спільність, репутація та надійність, які детально описані нижче. Спільність можна легко встановити в Інтернеті,

оскільки зловмисник може використовувати інформацію в соціальних мережах і на веб-сайтах, щоб побудувати спільну мову з жертвою. Така інформація, як упередження, вірування, норми та діалекти спільноти, корисна для зловмисника. Використовуючи таку інформацію, зловмисник може видати себе за учасника спільноти або знайомого на онлайн-форумах або в групах соціальних мереж. Репутація часто базується на мережі партнерів. Одним із методів покращення репутації зловмисника в кіберпросторі, яку сприймають інші, є збільшення зв'язків зловмисника в соціальних мережах із авторитетними особами. Шахрай може спиратися на сприйману спільність, щоб спонукати поважних осіб прийняти запрошення підключитися. Ще однією спокусою для залучення авторитетних людей у соціальних медіа є розмір соціальної мережі. Зловмисник може створювати широку соціальну мережу за допомогою ботів і підроблених персонажів. Надійність – це уявлення про те, що інша сторона діє добросовісно. Щоб показати надійність, зловмисник може включити в повідомлення артефакти (наприклад, посилання, зображення, графіку). Інтернет-середовище впливає на довіру жертви та сприйняття ризику. Сприйняття ризику – це індивідуальна оцінка ризику, пов'язаного з дією, і сприйняття ризику впливає на те, який ризик людина готова прийняти. Жертва в кіберпросторі також характеризується такими атрибутами: знання предметної області, пильність. По-перше, знання в сферах, відмінних від кібербезпеки, не зменшує сприйнятливість до атак соціальної інженерії в кіберпросторі. Це пояснюється тим, що вони часто покладаються на візуальні елементи та емоції, коли приймають рішення, пов'язані з ризиком. Крім того, сприйняття онлайн-ризику неекспертами формується передбачуваною вигодою від діяльності, а онлайн-діяльність, яка вважається корисною, сприймається як менш ризикована та виконується частіше. По-друге, застосування знань предметної галузі для розпізнавання атак соціальної інженерії в кіберпросторі є когнітивно вимогливим, оскільки розвиток знань про предметну область часто передбачає шаблони навчання, які вказують на зловмисні наміри. Загальні методи ідентифікації шаблонів (наприклад, розбір URL-адрес) вимагають вирішення технічних складнощів, що є когнітивно вимогливим, схильним до помилок і може сприяти надмірній довірі. Це розумно, оскільки коли ризик високий, але ситуацію важко оцінити, довіра є альтернативою для зменшення складності прийняття рішень. По-третє, пильність вимагає уваги, на яку впливають два компоненти, а саме перемикання та збереження уваги. Переключення уваги – це процес перенаправлення уваги з одного завдання на інше, тоді як підтримка уваги – це процес виділення когнітивних ресурсів для обробки інформації. Переключення уваги є попередником підтримки уваги та призводить до центральної обробки. Виразні подразники викликають переключення уваги. У звичайних обставинах увага людини спрямована на виконання основного завдання, яке підтримує його цілі (наприклад, керування електронною поштою, відвідування веб-сайтів або пошук інформації в Інтернеті). Щоб виявити ознаки обману в повідомленні соціальної інженерії, потрібно перенаправити свою увагу, щоб помітити невідповідності в повідомленні, де невідповідності мають бути достатньо помітними, щоб їх виявити та запустити перемикання. Як наслідок, пильність «присипається» та впливають індивідуальні характеристики (наприклад, комп'ютерні звички) [11].

Користувача, який потрапив під вплив методів соціальної інженерії можна характеризувати як особу довірливу, цікаву, також часто експлуатується люб'язність, лінь і навіть ентузіазм. До основних рис також можна віднести прагнення особи заощадити. Шахрайство по відношенню до фізичних осіб можна розділити на три групи. Відносно найменш захищених верств населення, що мають низький рівень фінансового достатку і кіберграмотності (пенсіонери, жителі невеликих міст) [3]. Для економічно активної частини населення, яка користується інтернетом, шахраї вибирають спам-розсилки листів, що містять інформацію про уявні знижки, отримання пільг, компенсацій, соціальних виплат. Такі повідомлення містять шкідливі програми або посилання на фішингові сайти, в результаті використання яких відбувається зараження пристрою і компрометація платежів його власника. До останньої групи можна віднести осіб, які активно користуються сучасними мобільними пристроями з операційними системами Android та IOS. Зловмисники використовують шкідливе програмне забезпечення для отримання доступу до встановлених на пристрої додатків, які містять конфіденційні дані. Це дозволяє їм здійснювати фінансові операції, такі як перекази грошових коштів з карт жертви. Такий підхід до шахрайства з використанням соціальної інженерії має різні варіації і полягає у використанні людських слабкостей. Висока поширеність таких атак підкреслює важливість своєчасного інформування про загрози, що є ключовим моментом у захисті користувачів віртуального середовища.

Соціальна інженерія нематеріальна, її неможливо усунути фізично. Найдієвіший спосіб не стати жертвою шахрайства – це не втрачати пильності і не дозволяти шахраєві себе провести [9].

Соціальні інженери використовують ці вразливості, щоб змусити людей розголошувати конфіденційну інформацію, виконувати

певні дії або приймати рішення, які приносять користь зловмиснику.

Ґрунтовний аналіз ключових вразливих місць людини, на які соціальні інженери часто орієнтуються, зустрічається у праці адвоката з кібербезпеки Еммануеля Окайвеле (Okaiwele E.)

1. Довіра: люди схильні довіряти іншим, особливо коли вони вірять, що мають справу з надійними джерелами або особами з авторитетом. Соціальні інженери часто видають себе за довірених осіб або діячів, таких як IT-підтримка, керівники або правоохоронні органи, щоб завоювати довіру та співпрацю.

2. Допитливість: люди від природи цікаві й можуть виникнути спокуса вивчити незнайому чи інтригуючу інформацію чи пропозиції. Соціальні інженери використовують цю цікавість, щоб спонукати людей натискати шкідливі посилання, відкривати заражені файли або брати участь у ризикованій поведінці.

3. Страх і занепокоєння: страх перед негативними наслідками, такими як судовий позов, втрата роботи або фінансові штрафи, може переважити раціональне судження. Соціальні інженери використовують страх, створюючи термінові або загрозливі сценарії, які спонукають до негайного виконання вимог, наприклад, фальшиві сповіщення безпеки або юридичні загрози.

4. Бажання винагород: людей приваблюють потенційні винагороди чи стимули. Соціальні інженери використовують обіцянки винагород, як-от призи, знижки або ексклюзивний доступ, щоб маніпулювати людьми, щоб вони надали інформацію або вжили дій, яких вони б інакше уникали.

5. Контроль імпульсів: у ситуаціях сильного стресу або емоційно насичених людей може бути важко контролювати свої імпульси та приймати імпульсивні рішення. Соціальні інженери створюють термінові та емоційні тригери, щоб використовувати цю вразливість.

6. Недостатня обізнаність: багато людей не знають про різні тактики, які застосовуються під час атак соціальної інженерії, що робить їх більш сприйнятливими. Освіта та обізнаність можуть допомогти людям розпізнати таку тактику та протистояти їй.

7. Інформаційне перевантаження: у сучасну цифрову епоху людей засипають інформацією та повідомленнями. Соціальні інженери використовують це на свою користь, знаючи, що люди можуть не ретельно перевіряти кожне повідомлення, яке вони отримують.

8. Довіра до технологій: люди часто довіряють технологічним системам, щоб захистити їх. Соціальні інженери використовують цю довіру, використовуючи фішингові електронні листи, підроблені веб-сайти та інші цифрові методи, які здаються законними.

Щоб захиститися від атак соціальної інженерії, окремі особи та організації повинні сприяти обізнаності та освіті про ці вразливості [8].

Одна з цитат з книги «Ghost in the Wires: My Adventures as the World's Most Wanted Hacker» Кевіна Мітника, зазначає про важливість захисту від маніпуляцій: «Хочете знати найкращий спосіб захистити себе від маніпуляцій? Пам'ятайте, що найпотужніший інструмент у вашій арсеналі – це ваш розум. Завжди ставте під сумнів будь-яку ситуацію, в якій вас просять виконати щось, що вас не зручно, або в якій вам пропонують щось, що здається надзвичайно вигідним або легким. Навчіться розрізняти справжні можливості від обману. Пам'ятайте, що кращий захист – це свідомість» [9].

Висновки. Техніки соціальної інженерії різноманітні, але їх спільною рисою є використання когнітивних спотворень, таких як людська наївність та неуважність. Останнім часом спостерігається збільшення випадків шахрайства за допомогою соціальної інженерії, що передбачає незаконний доступ до інформації без використання технічних засобів. Це передбачає маніпулювання поведінкою людини, яке змушує її здійснити дії, що сприяють крадіжці коштів або отриманню особистих даних. Такі методи включають фальшиві SMS-розсилки, злом даних для входу на популярні інтернет-ресурси, фішинг, квіпрокво і інші.

Високий рівень розповсюдженості цього виду шахрайства підкреслює важливість своєчасного інформування про загрози як ключового захисного механізму для користувачів сучасних комунікаційних засобів. Хоча соціальна інженерія являє собою нематеріальну загрозу, уникнути стати її жертвою можна, утримуючи пильність і не дозволяючи шахраям провести себе [4].

Атаки соціальної інженерії є постійною загрозою в цифровому світі, але розуміння психології цих тактик може допомогти окремим особам і організаціям захиститися від них. Визнаючи психологічні тригери та тривожні сигнали, пов'язані із соціальною інженерією, ми можемо зміцнити свій захист і захистити наше цифрове життя від маніпулятивних кіберзлочинців [10].

Людина не може одразу виявити, що перед нею шахрай через те, що істинний аферист-віртуоз своєї справи. Він ні до чого не змушує. Він робить вас співучасниками власного краху. Він не краде – користувач віддає. Він не випитує – люди самі розповідають йому свою історію. Ми віримо, бо хочемо повірити. Тому проаналізувавши основні методики, що використовує соціальна інженерія в онлайн – просторі, виявлені взаємозв'язки між особливостями людської психіки та методами соціальної інженерії.

Згідно аналізу наукових джерел з'ясовано, що шахраї активізуються саме у складні, кризові періоди життя суспільства, оскільки критичне мислення людини знижується, вона втрачає пильність і через занурення у свої думки не помічає небезпеки. Єдине, що може допомогти у цій ситуації – самоконтроль. Шахраї розраховують якраз на емоційну незрілість. Вони тиснуть на слабкі місця людей. А ще вони дуже спостережливі: відстежують у соціальних мережах, що зараз актуально, на що реагують люди. Відповідно до цього створюють контент – зі зворушливою історією та вразливою картинкою, щоб це було емоційно, щоб зачіпало за живе.

Зазначимо, що у третьому кварталі 2023 року компанія Vade виявила значне збільшення кількості фішингових і шкідливих атак. Обсяги фішингу зросли на 173% порівняно з попереднім кварталом (493,2 млн проти 180,4 млн). Malware також спостерігалося стрімке зростання порівняно з кварталом (110%), досягнувши 125,7 мільйонів електронних листів порівняно з 60 мільйонами у другому кварталі.[6] Це свідчить про важливість питань, розглянутих у статті.

ЛІТЕРАТУРА:

1. Анісімов А.А. Цифрова автентифікація: досягнення та перспективи. Стенограма доповіді на засіданні Президії НАН України 31 травня 2023 року. Вісник Національної академії наук України. № 8. 2023. URL: https://doi.org/10.15407/visn2023.08.065 (дата звернення: 09.04.2024)

2. Дзюба О. У 2023 році середня сума шахрайської операції з «веденням клієнта» – 8500 грн. Ось інші важливі цифри щодо онлайн-зловмисників. URL: https://dev.ua/news/v-2023-rotsi-serednia-suma-shakhraiskoi-operatsii-z-vedenniam-kliienta-8500-hrn-os-inshi-vazhlyvi-tsyfry-shchodo-onlain-zlovmysnykiv (дата звернення: 06.04.2024)

3. Козар А. В. Соціальна інженерія як спосіб шахрайства. Протидія кіберзлочинності та торгівлі людьми: збірник матеріалів міжнародної наук.-практ. конф. (м. Харків, 18 травня 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. – с. 24–25.

4. Колісник Т., Ющенко Я. Актуальні проблеми кібербезпеки: небезпека соціальної інженерії в кіберпросторі. Протидія кіберзлочинності та торгівлі людьми: збірник матеріалів міжнародної наук.-практ. конф. (м. Харків, 18 травня 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ ; ГС «Глобальний центр взаємодії в кіберпросторі». – Харків : ХНУВС, 2021. – с. 63–65.

5. Селіванова, А., Левитський, Ю. Дослідження методів соціальної інженерії. Частина І. Вплив на здоров'я людини. Automation of Technological and Business Processes, 14 (2), с. 56–62. URL: https://doi.org/10.15673/atbp.v14i2.2334 (дата звернення: 09.04.2024)

6. Шевченко А. Звіт про тенденції загроз фішингу. URL: https://top-ai.com.ua/news/zvit-pro-tendencziyi-zagroz-fishyngu/ (дата звернення: 08.04.2024)

7. Що таке соціальна інженерія? Напади, методи та запобігання. Cyber Witcher. URL: https://hackyourmom.com/kibervijna/shho-take-soczialna-inzheneriya-napady-metody-ta-zapobigannya/ (дата звернення: 05.04.2024)

8. Mitnick Kevin та Simon William L. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker Little, Brown and Company, 2011. 412 с.

9. Mitnick Kevin та Simon William L. The Art of Deception: Controlling the Human Element of Security. Wiley, 2003. 368 с.

10. Okaiwele E. The Psychology of Social Engineering Attacks. URL: https://developerehis.medium.com/the-psychology-of-social-engineering-attacks-ac0e 551a5612 (дата звернення: 28.03.2024)

11. Rodriguez R., Atyabi A., Xu S. Social engineering attacks and defenses in the physical world vs. cyberspace: a contrast study. URL: https://www.researchgate.net/publication/359130132_Social_Engineering_Attacks_and_Defenses_in_the_Physical_World_vs_Cyberspace_A_Contrast_Study (дата звернення 10.04.2024)