



Звіт про кінцеве дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки



Звіт про кінцеве дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки



Підготовлено для Представництва
Фонду цивільних досліджень
та розвитку США в Україні



Дослідження проведено за підтримки Офісу
Координатора допомоги США Європі та Євразії
Державного департаменту США

2024

ЗМІСТ

Список аббревіатур і скорочень

Ключові результати

Висновки і рекомендації

Мета дослідження і методологія

Результати дослідження

Поведінка в інтернеті

Обізнаність з поняттями «кібербезпека» та «правила кібергігієни»

Ризикована поведінка

Здатність розпізнавати ризиковані ситуації

Досвід зіткнення із кіберзагрозами

Обізнаність із правилами кібербезпеки

Безпека поведінки в інтернеті

Інформаційні матеріали та оцінка динаміки поведінки

Оцінка інформаційних матеріалів

Виклики і перспективи

Додатки

Додаток 1. Опитувальник

Додаток 2. Портрет респондента

3

4

8

10

13

14

18

20

24

30

33

36

38

41

45

47

48

56

Список аббревіатур і скорочень

CAPI	Особисте опитування вдома у респондента за допомогою комп'ютера (computer assisted personal interview)
CATI	Телефонне опитування за допомогою комп'ютера (computer assisted telephone interview)
CAWI	Онлайн-опитування за допомогою комп'ютера (computer assisted web interview)
ВПО	Внутрішньо переміщені особи
ЦА	Цільова аудиторія
Baseline	Базове дослідження (перша хвиля опитування), проведено в серпні-вересні 2021 року
Midterm	Проміжне дослідження (друга хвиля опитування), проведено в березні 2023 року
Endline	Кінцеве дослідження (третья хвиля опитування), проведено в серпні-вересні 2024 року
В.п.	Відсоткові пункти

Поведінка в інтернеті

Частота користування інтернетом майже не змінилася: найактивніше інтернетом користуються підлітки і молодь (більше половини опитаних цих груп проводять в інтернеті більшу частину дня). Старша аудиторія (60+) переважно користується інтернетом щодня, але обмежується 1-2 сесіями. Але всі респонденти з доступом до інтернету (незалежно від віку) переважно користуються ним щоденно.

Серед інтернет-активностей першість, як і в baseline-замірі (2021 рік), посідають месенджери і соціальні мережі. Більше того, частота користування цими ресурсами зросла в усіх вікових групах. Також зросла частота користування інтернет-банкінгом і сплат за товари і послуги через інтернет. Підлітки частіше за інші аудиторії грають в онлайн-ігри (частота зросла). Для молоді і дорослих респондентів (18-25 років і 26-59 років) частотним залишається користування електронною поштою. Люди старшого віку не схильні вдаватися до інших інтернет-активностей, окрім спілкування у месенджерах або соціальних мережах.

До активностей, які можуть бути потенційно небезпечними (скачування ігор, програм або іншого контенту), вдається відносно незначна частка користувачів (до 10% роблять це щодня або кілька разів на тиждень).

Обізнаність з поняттями «кібербезпека» та «правила кібергігієни»

Обізнаність з поняттями «кібербезпека» та «правила кібергігієни» зросла в endline-замірі. Наприклад, 74% респондентів знають про поняття «кібербезпека» проти 69% в midterm-замірі і 62% в baseline-замірі. Утім, частка респондентів, які «дуже добре знають і можуть пояснити іншим», залишилася майже на рівні midterm-заміру (20% і 19% відповідно). Найбільший внесок в зростання обізнаності про поняття «кібербезпека» внесли вікові групи «Молодь» (18-25 років) і «Дорослі» (26-59 років). Серед інших груп зростання рівня обізнаності не можна назвати стрімким.

Обізнаність з правилами кібергігієни також зросла в endline-замірі, хоча зростання не таке суттєве, як було зафіксовано в midterm-замірі (39%, 55% і 59% відповідно знають про правила кібергігієни в трьох замірах). Зростання обізнаності в групах «Молодь» і «Дорослі» також є найбільш суттєвим порівняно до підлітків і старших респондентів.

Ризикована поведінка

Серед ознак ризикованої поведінки першість посідає відсутність звички робити резервні копії документів (82% респондентів не роблять це регулярно, з них 46% не роблять ніколи) та невикористання двофакторної автентифікації (69% не використовують її регулярно і 40% не використовують ніколи). Утім, частота використання двофакторної автентифікації поступово зростає — в 2021 році її ніколи не використовували 50% опитаних, а в 2023 році — 44%. Також у суспільстві продовжує переважати думка, що «пересічна» людина не є цікавою для інтернет-шахраїв: до неї схилиються хоча б частково 58% опитаних (утім, популярність цієї думки також поступово спадає: в 2023 році до неї схилилися 64% опитаних).

Досвід зіткнення із кіберзагрозами

Серед кіберзагроз, з якими респонденти стикалися особисто або знають про такий досвід від знайомих, першість посідають дії шахраїв, спрямовані на вимагання грошей, банківських або особистих даних методами соціальної інженерії:

КЛЮЧОВІ РЕЗУЛЬТАТИ

- Вимагання банківських даних, паролів та доступу до облікових записів банківських мобільних додатків, банківських рахунків;
- Кібершахраї вимагають гроші, використовуючи методи соціальної інженерії, а також особисті та родинні дані;
- Вимагання особистих даних через телефон, месенджери, поштові скриньки, облікові записи у соціальних мережах.

Утім, частота стикання з цими загрозами залишилася на рівні 2023 року.

А от частота стикання з крадіжками (зломом) облікових записів у соціальних мережах суттєво зросла (зростання фіксується другим замір поспіль): в 2021 про досвід такого шахрайства стосовно себе або стосовно знайомих повідомили 39% респондентів, в 2023 році — 52%, а в 2024 році — уже 60% (!). Зростання такого досвіду зафіксовано в групах «Молодь» і «Дорослі», але більшою мірою за рахунок досвіду знайомих, а не особистого досвіду.

Обізнаність із правилами кібербезпеки

Серед основних правил кібербезпеки найбільше вживаними третій замір поспіль залишаються загадані нижче (їх завжди дотримуються 90%, 87% та 82% опитаних відповідно, що близько до максимально можливого значення):

- Не відправляйте фото та скани банківських карток та особистих документів незнайомцям та сумнівним організаціям;
- Не залишайте ваш пристрій без нагляду, особливо коли він працює, у публічних місцях;
- Не відправляйте ваші контактні телефони, особисті фото незнайомцям, особливо тим, які просять оголені фотографії.

Щодо правила «Не панікуйте у разі телефонного дзвінка чи повідомлення у месенджері від підозрілих людей та організацій, які вимагають у вас гроші, аби врятувати вашу родину, тварину чи близьку людину. негайно повідомте відповідні органи чи своїх близьких у разі такого дзвінка» спостерігається зростання обізнаності і використання: 77% повідомили, що знають і використовують це правило, порівняно до 61% у 2023 році.

Правило використання двофакторної автентифікації знають і завжди використовують 43% опитаних (це на рівні midterm-заміру, але суттєво більше, ніж в baseline (28%).

Єдине правило кібербезпеки, щодо якого було зафіксовано спадання поширеності використання, — це правило оновлення пристрою. Люди стали ще більш підозріло ставитися до оновлень: в 2021 році цим правилом користувалися 53% опитаних, в 2023 році — 46%, у 2024 році — 41%.

Безпека поведінки в інтернеті

Загалом оцінка власної поведінки в інтернеті з точки зору її безпеки трохи змінилася порівняно до midterm-заміру: 27% вважають свою поведінку повністю безпечною (проти 25% у 2023 році), водночас 24% вважають свою поведінку небезпечною (20% в 2023 році). Молодь 18-25 років найрідше вважає свою поведінку небезпечною, більше того, частка молодих людей, які вважають свою поведінку небезпечною, скорочується (17%, 12% і 9% у 2021, 2023 і 2024 рр. відповідно). Одним з пояснень може бути те, що молодь найчастіше за інші групи помічає матеріали і публікації про правила безпечної поведінки в інтернеті (70% респондентів

КЛЮЧОВІ РЕЗУЛЬТАТИ

у віці 18-25 років сказали про це). Для порівняння: серед підлітків такі матеріали бачили 41%, серед дорослих 54%, а серед старших людей — лише 37%.

Підлітки найкраще за інших реагують на такі матеріали: 63% підлітків, які бачили такі матеріали, сказали, що їхня поведінка стала більш безпечною. Загалом здатність змінювати поведінку під впливом навчальних матеріалів зменшується з віком. Серед респондентів решти вікових груп, які стикнулися із навчальними матеріалами, змінили поведінку на більш безпечну 42%, 37% і 36% опитаних (відповідно серед молоді, дорослих і старших респондентів).

Утім, респонденти впевнені, що змінюють свою поведінку в інтернеті на більш безпечну самостійно: загалом 32% опитаних сказали, що за останній рік їхня поведінка стала більш безпечною (серед тих, хто стикався з навчальними матеріалами з кібербезпеки, цей показник трохи більший і становить 39%).

Оцінка інформаційних матеріалів Представництва Фонду цивільних досліджень та розвитку США в Україні

Для оцінки інформаційних матеріалів проєкту «Інформаційна кампанія про кібербезпеку» програми кібербезпеки Представництвом Фонду цивільних досліджень та розвитку США в Україні було проведено опитування респондентів онлайн, де їм демонструвалися елементи інформаційної кампанії. Майже 80% опитаних погодилися з твердженням, що після перегляду подібних інформаційних матеріалів їхня поведінка в інтернеті стає більш безпечною. Загалом 39% респондентів онлайн опитування сказали, що бачили матеріали Представництва Фонду цивільних досліджень та розвитку США в Україні раніше (здебільшого це зовнішня реклама в містах України). В цій аудиторії частка тих, хто змінив поведінку на краще, становить 44%. Цей показник є відображенням одного з основних індикаторів проєкту, а саме — відсоток населення, яке бачило освітні матеріали Кампанії, та змінило свою поведінку на краще.

Протягом періоду реалізації проєкту ми можемо засвідчити зростання таких показників в усіх досліджуваних вікових групах:

- Обізнаність з поняттями кібербезпеки і правила кібергігієни;
- Зниження ризикованої поведінки — особливо щодо використання двофакторної автентифікації і усвідомлення ризику стати жертвою кібер-шахрайства, а також використання російських ресурсів;
- Здатність розпізнавати ризиковані і безпечні ситуації;
- Деклароване використання правил кібербезпеки — особливо щодо використання двофакторної автентифікації.

Утім значущої динаміки в самооцінці населення власної поведінки в інтернеті не спостерігається — протягом 2020-2024 років 53-56% оцінювали безпеку власної поведінки на 8-9-10 балів за 10-бальною шкалою. Утім слід зауважити, що самооцінка поведінки в інтернеті залежить від знання та виконання правил кібербезпеки: чим вище людина оцінює безпеку своєї поведінки, тим краще вона знає і частіше виконує правила кібербезпеки. Значна частка респондентів, які впевнені у власній безпеці, не дає суттєвого простору для удосконалення власної поведінки (якщо людина почувається безпечно, то нема сенсу міняти шаблони звичної поведінки).

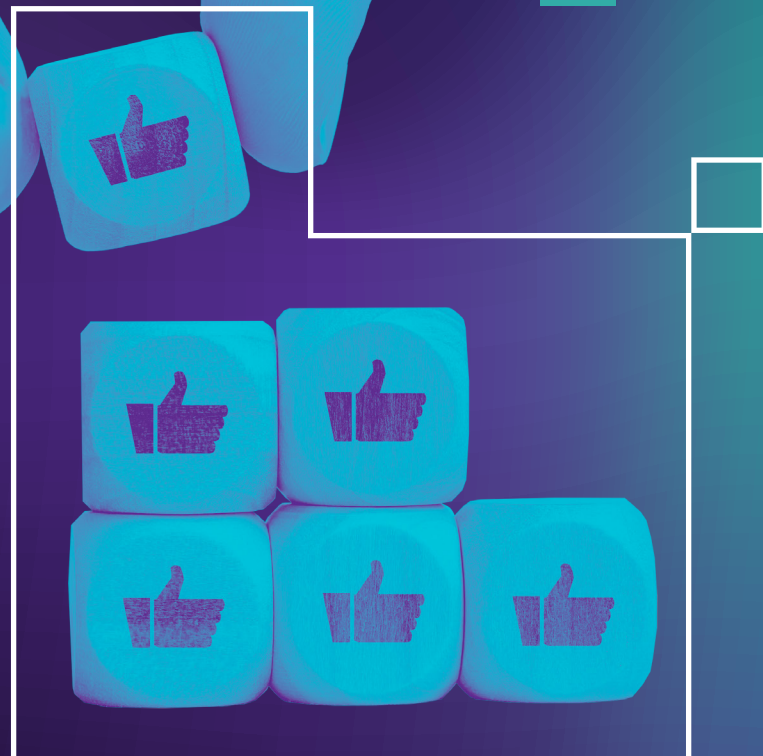
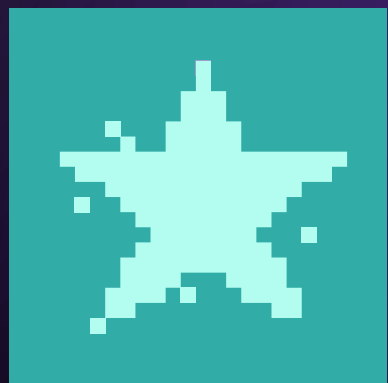
Одним з чинників зміни поведінки в інтернеті є інформаційні матеріали, які розповсюджують різні проєкти і ініціативи. Такі матеріали можуть інкорпороватися у навчальні матеріали для школярів і студентів, а також бути частиною корпоративного навчання. Частка тих, хто уже змінив або готовий змінювати свою поведінку під впливом інформаційних матеріалів досить суттєва: так, одразу після перегляду матеріалів 70%-85% опитаних заявляють, що готові змінювати свою поведінку (в залежності від типу матеріалу, зрозумілості його основної думки тощо). Загалом майже 80% опитаних погоджуються з твердженням, що після перегляду подібних інформаційних матеріалів їхня поведінка в інтернеті стає більш безпечною. Проте декларативні показники відрізняються від об'єктивних: лише 32% опитаних сказали, що за останній рік їхня поведінка стала більш безпечною, а більшість (57%) зауважили, що їхня поведінка не змінилася.

Утім серед тих, хто бачили хоч один з матеріалів інформаційної кампанії Представництва Фонду цивільних досліджень та розвитку США в Україні раніше, частка тих, хто змінив поведінку на краще, становить 44%, що можна вважати індикатором успішності інформаційної кампанії.

Для подальшого просування шаблонів безпечної поведінки рекомендовано звернути увагу на наступне:

- Кампанія з просування правил кібергігієни має бути присутньою в інформаційному просторі тривалий час, можливо на хвильовій основі, але це повинні бути постійні, а не точкові інтервенції.
- Найбільш вразливою аудиторією, згідно даних дослідження, виступають літні люди (вони менше за молодшу аудиторію знаються на інформаційних технологіях, гірше розрізняють ризиковані ситуації, гірше знають правила кібербезпеки). Водночас вони є найбільш вдячною аудиторією з точки зору ефективності навчання — якщо літня людина засвоїла певне правило, вона з більшою ймовірністю буде його виконувати.
- Недостатній рівень здатності розрізняти безпечні і ризиковані ситуації може бути бар'єром для використання правил безпечної поведінки і вибудови здорової стратегії власних поведінкових шаблонів.
- Певні технологічні рішення підтримки кібербезпеки залишаються незрозумілими для населення (VPN, регулярне оновлення застосунків, менеджери паролів) — таким чином користування ними сприймається як ризиковане. Таким чином інформаційна кампанія в підтримку кібербезпеки має також виконувати освітню функцію щодо сучасних інформаційних рішень.

ВИСНОВКИ І РЕКОМЕНДАЦІЇ



МЕТА ДОСЛІДЖЕННЯ І МЕТОДОЛОГІЯ

Визнаючи ризики, пов'язані із чимраз більшою цифровізацією світу, Представництво Фонду цивільних досліджень та розвитку США в Україні у 2019 році розпочала програму покращення кібербезпеки в Україні, Молдові та на Західних Балканах. Програма присвячена запобіганню кібератакам шляхом створення міцної кіберінфраструктури та посилення кібербезпеки. Ця програма підтримується *Офісом Координатора допомоги США Європі та Євразії Державного департаменту США*.

Частиною програми кібербезпеки Представництва Фонду цивільних досліджень та розвитку США в Україні є проєкт «Інформаційна кампанія про кібербезпеку», основна мета якої — покращити обізнаність широкого загалу українців про загрози кібербезпеки.

Даний звіт представляє узагальнену оцінку індикаторів у динаміці за результатами трьох хвиль опитування: baseline¹, miderm² та endline.

Дослідження має на мені оцінити:

- рівень поінформованості цільових аудиторій про кіберзагрози;
- рівень обізнаності про основні правила кібергігієни та їх застосування у повсякденному житті;
- особистий досвід користувачів щодо кіберзагроз за останні місяці;
- здатність вирізняти потенційно загрозливі з точки зору кібербезпеки ситуації;
- зміни поведінки в інтернеті на більш безпечну.

Цільова аудиторія основного дослідження — громадяни України, які користуються інтернетом щонайменше кілька разів на місяць.

Цільові групи респондентів:

- Підлітки 11-17 років;
- Молодь 18-25 років;
- Дорослі 26-59 років;
- Люди старшого віку від 60 років.

Основний метод проведення дослідження — **кількісне опитування** за структурованим опитувальником (методика опитування дозволяє здійснювати коректну оцінку динаміки показників за хвилями).

Географія дослідження: вся Україна, включно із селами, за винятком АР Крим та територій, які не контролюються українською владою. Опитування проводилося в серпні-вересні 2024 року, аналіз даних і підготовка звіту — у вересні 2024 року.

Загальна кількість респондентів основного опитування третьої хвилі: 1227.

Кількість респондентів за цільовими групами:

- Підлітки 11-17 років: 324 респонденти;
- Молодь 18-25 років: 198 респондентів;
- Дорослі 26-59 років: 403 респонденти;

¹ https://www.sapiens.com.ua/publications/socpol-research/196/crdf_baseline_obiznanist-auditorii-pro-kiberbezpeku_ukr.pdf

² <https://www.sapiens.com.ua/publications/socpol-research/321/promizhne-doslidzhennya-shhodo-informovanosti-pro-osnovni-aspekty-kiberbezpeky-1.pdf>

- Люди старшого віку від 60 років: 302 респонденти.

Попередньо було заплановано провести однакову кількість інтерв'ю з усіма цільовими групами (по 300 інтерв'ю). Проте під час опитування дослідники стикнулися із низьким рівнем відгуку у цільовій групі молоді (люди віком 18-25 років). Було прийнято рішення скоротити цільову кількість інтерв'ю до 198 за рахунок збільшення цільової кількості інтерв'ю у групі 26-59 років до 403 інтерв'ю.

Метод опитування:

- для цільової групи «Підлітки» — застосовувався метод особистого опитування вдома у респондента за допомогою комп'ютера (CAPI — computer assisted personal interview);
- для решти цільових груп — телефонне опитування за допомогою комп'ютера (CATI — computer assisted telephone interview).

Вибірка випадкова із контролем квот за статтю, віком, регіоном та розміром населеного пункту. В рамках кожної цільової групи вибірка є репрезентативною, структура відповідає структурі інтернет-користувачів за статтю, віком, регіоном та розміром населеного пункту відповідно до даних Державної служби статистики України про довоєнне проживання (станом на січень 2022 року).

Для аналізу по вибірці загалом було застосовано зважування, яке привело структуру вибірки у відповідність до структури населення України за віком.

Максимальна статистична похибка вибірки становить:

- Вибірка загалом: 2,8% ймовірністю 95%;
- Підлітки 11-17 років: 5,4% ймовірністю 95%;
- Молодь 18-25 років: 7,0% ймовірністю 95%;
- Дорослі 26-59 років: 4,9% ймовірністю 95%;
- Люди старшого віку від 60 років: 5,6% ймовірністю 95%.

Додатково було проведено **кількісне онлайн-опитування** для визначення ефективності рекламних та комунікаційних інтервенцій, що проводилися в рамках проекту:

- Населення України віком 18+, яке користується інтернетом: 3065 респондентів.

Метод кількісного опитування: онлайн-інтерв'ю з тестуванням візуальних матеріалів. Опитування проводилося по власній онлайн-панелі Info Sapiens.

Кількісні опитування проводилося за структурованими опитувальниками (див. Додаток 1).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

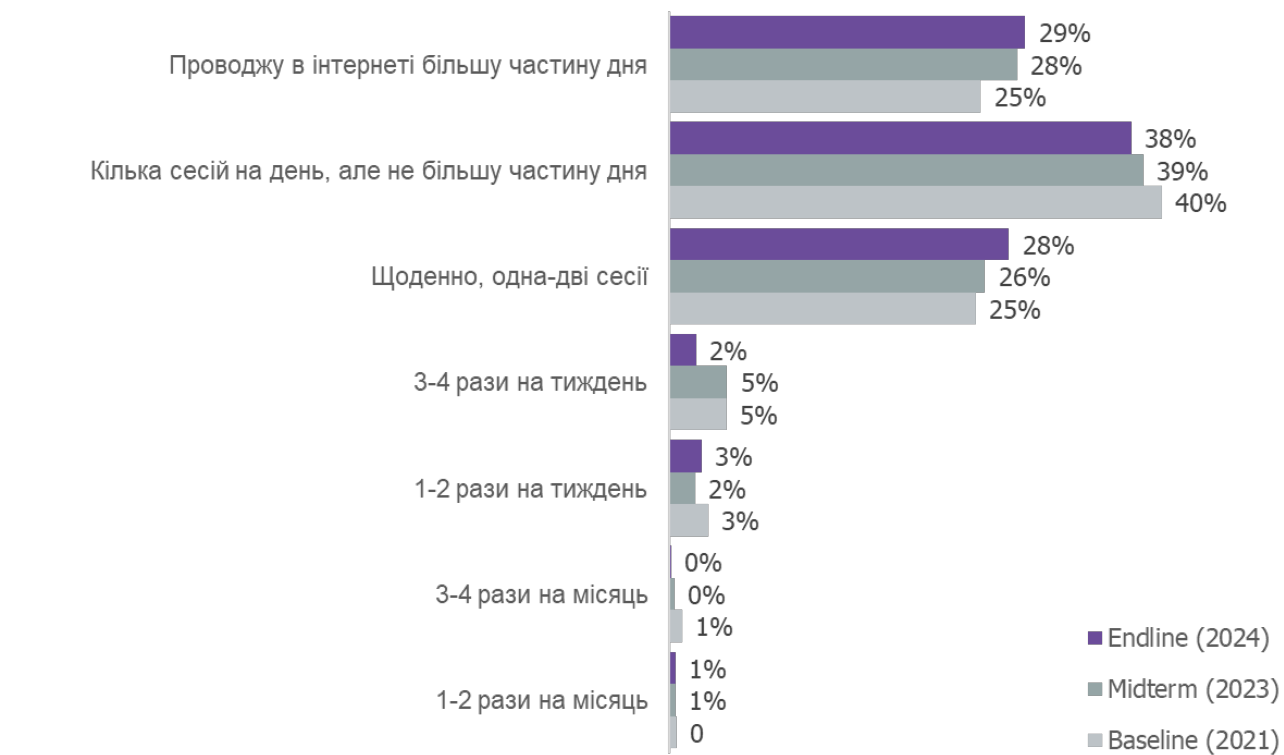


Поведінка в інтернеті

Умовою участі в опитуванні було користування інтернетом — респондентами могли виступати люди, які користуються інтернетом щонайменше раз на місяць. Утім, переважна частка опитаних (близько 95%), користуються інтернетом щодня (це справедливо для всіх вікових груп) (Діаграма 1).

Частка людей, які проводять більшу частину дня в інтернеті, поступово зростає за рахунок тих, хто має кілька сесій щоденно.

Діаграма 1. Як часто ви користуєтеся інтернетом? (% відповідей)

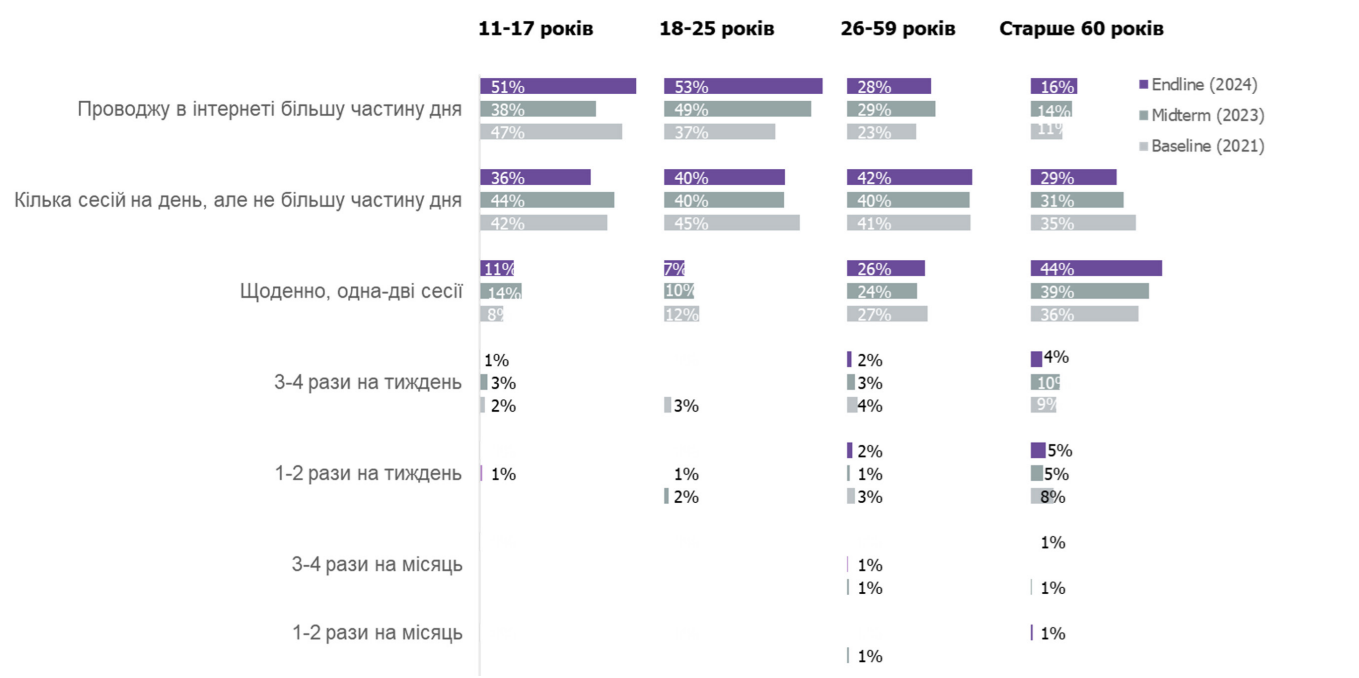


Чим старші респонденти, тим менше часу вони проводять в інтернеті. Ця тенденція була зафіксована у baseline-дослідженні у 2021 і збереглася у 2023-2024 роках (Діаграма 2).

Серед підлітків 11-17 років більшу частину дня в інтернеті проводить 51% респондентів. Зафіксовано суттєве зростання порівняно до 38% у 2023 році. Різниця в оцінках може бути пов'язана з тим, що midterm-дослідження проводилося під час навчального року, а baseline та endline дослідження — під час літніх канікул у серпні 2021 і 2024 років.

Серед молоді 18-25 років більшу частину дня в інтернеті проводить більше половини опитаних (53% проти 37% в baseline-дослідженні). У цільовій групі 26-59 років частка тих, хто проводить в інтернеті більшу частину дня, також збільшилася порівняно до baseline-дослідження, але залишається на рівні midterm-дослідження). Літні люди старше 60 років найчастіше мають 1-2 інтернет-сесії щоденно, і лише 16% «живуть» в інтернеті більшу половину дня. Втім, частка активних користувачів серед літніх людей також поступово зростає.

Діаграма 2. Як часто ви користуєтеся інтернетом? (% відповідей, за цільовими групами)



Основна частина інтернет-активностей припадає на спілкування в месенджерах і відвідування соціальних мереж (Діаграма 3). Частота користування цими ресурсами зросла порівняно до базового дослідження в 2021 році, при цьому зростання зафіксовано в усіх вікових групах (Таблиця 1). Також суттєве зростання зафіксовано щодо користування інтернет-банкінгом, що може бути пов'язано із практиками грошових донатів і зборів (в групах молоді і дорослих щоденне користування інтернет банкінгом зросло удвічі порівняно до 2021 року).

Діаграма 3. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей)



Таблиця 1. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей «Щодня», за цільовими групами)

Частка відповідей «Щодня»	Вік респондента							
	11-17 років		18-25 років		26-50 років		Більше 60 років	
	Endline (2024)	Baseline (2021)	Endline (2024)	Baseline (2021)	Endline (2024)	Baseline (2021)	Endline (2024)	Baseline (2021)
Користуєтеся месенджерами	84,65%	80,63%	88,99%	83,86%	83,77%	73,40%	56,43%	49,16%
Заходите на сторінки, читаєте стрічки соціальних мереж	81,55%	73,27%	79,54%	74,90%	65,34%	62,86%	50,46%	36,39%
Користуєтеся електронною поштою	18,32%	10,91%	43,61%	29,53%	32,51%	30,13%	8,39%	13,34%
Користуєтеся інтернет-банкінгом	11,09%	4,23%	47,34%	22,91%	28,23%	14,91%	7,24%	5,48%
Граєте в ігри онлайн	44,01%	32,13%	16,31%	13,62%	8,95%	8,42%	7,41%	6,73%
Сплачуєте за товари або послуги банківською картою через інтернет	7,87%	1,36%	16,40%	8,08%	8,37%	4,66%	6,18%	2,35%
Завантажуєте відео, музику, статті, книги, інші матеріали	15,81%	17,97%	10,44%	14,93%	6,52%	4,52%	6,97%	3,47%
Допишете або розмішуете фотографії в соціальних мережах	16,05%	22,02%	2,34%	6,96%	2,05%	1,77%	4,18%	3,34%
Підключаєтеся до публічних вай-фай мереж	11,34%	9,76%	7,19%	4,72%	3,10%	4,04%	1,13%	2,50%
Користуєтеся VPN	5,62%	2,00%	3,12%	5,69%	1,58%	5,91%	1,92%	2,66%
Скачуєте безкоштовні програми, ігри	8,70%	6,13%	1,64%	2,25%	0,97%	0,73%	1,19%	1,84%
Встановлюєте різні програми, доповнення до браузерів	3,38%	1,37%	1,54%	1,61%	1,52%	0,64%	0,62%	0,93%
Купуєте товари в інтернет-магазинах	5,58%	3,27%	0,73%	1,80%	0,95%	0,33%	0,00%	0,49%
Робите покупки з ігрових акаунтів	1,66%	0,78%	0,31%	0,52%	0,39%	0,18%	0,00%	0,00%

Обізнаність з поняттями «кібербезпека» та «правила кібергігієни»

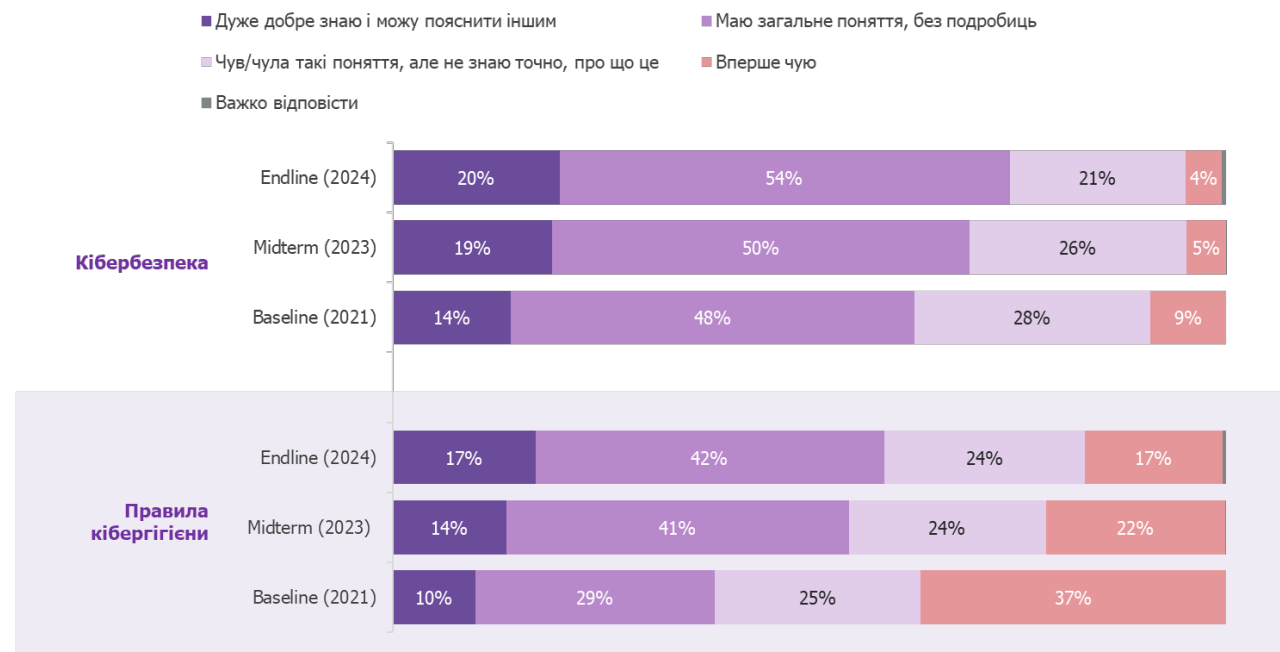
Індикатор обізнаності українців із поняттями «кібербезпека» та «правила кібергігієни» заміряється третю хвилю поспіль через пряме запитання. Утім, перевірка, наскільки декларативне знання відповідає реальному, не входить у цілі дослідження.

Загалом рівень обізнаності про поняття «кібербезпека» та «правила кібергігієни» підвищився порівняно з даними baseline та midterm-досліджень. У 2024 році відповідь «дуже добре знаю і можу пояснити іншим» щодо понять «кібербезпека» та «правила кібергігієни» обрали 20% та 17% опитаних відповідно (Діаграма 4).

Поняття «кібербезпека» краще знайоме українцям, ніж поняття «правила кібергігієни». Уявлення про нього (тобто обрали відповіді «дуже добре знаю...» і «маю загальне поняття...») мають 74% респондентів (що на 5 в.п. більше, ніж у 2023 році, і на 12 в.п. більше, ніж у 2021 році). Зауважимо, що в 2024 році зростання обізнаності відбулося за рахунок частки відповідей «маю загальне поняття...».

Уявлення про «правила кібергігієни» хоча б в загальних рисах мають 59% (що на 4 в.п. більше, ніж у 2023 році, і на 20 в.п. більше, ніж у 2021 році). Тут зростання відбулося за рахунок збільшення обох показників — і «дуже добре знаю...» і «маю загальне поняття...». В 2024 році продовжилося скорочення частки відповідей «вперше чую» про правила кібергігієни, що свідчить про проникнення цієї концепції у суспільство.

Діаграма 4. Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека» та «правила кібергігієни»? (% відповідей)

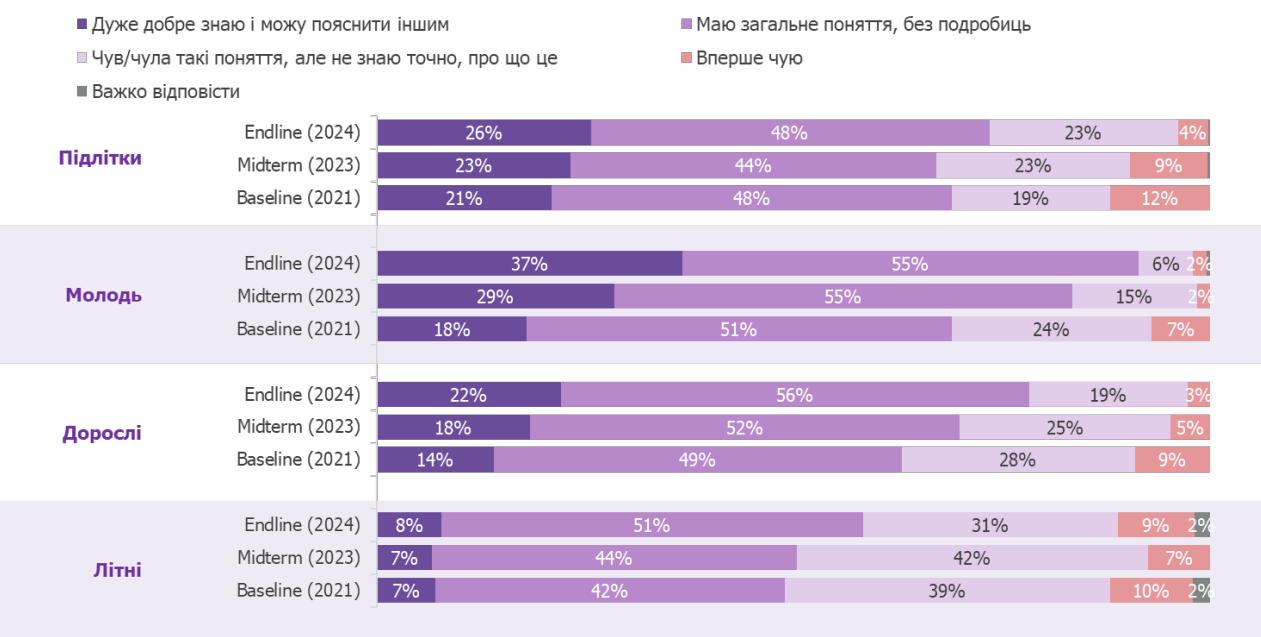


Зростання показників знання про кібербезпеку відбувається в усіх вікових групах (Діаграма 5). Найбільшим драйвером зростання є молодь: у цій віковій групі частка опитаних, які знайомі з поняттям «кібербезпека», становить понад 90% (!), при цьому частка «добре обізнаних» становить 37% (що удвічі більше, ніж у baseline-дослідженні).

Літні люди, незважаючи на зростання обізнаності, залишаються найменш обізнаними: один з десяти респондентів вперше почули про кібербезпеку під час опитування.

Діаграма 5. Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека»? (% відповідей, за цільовими групами)

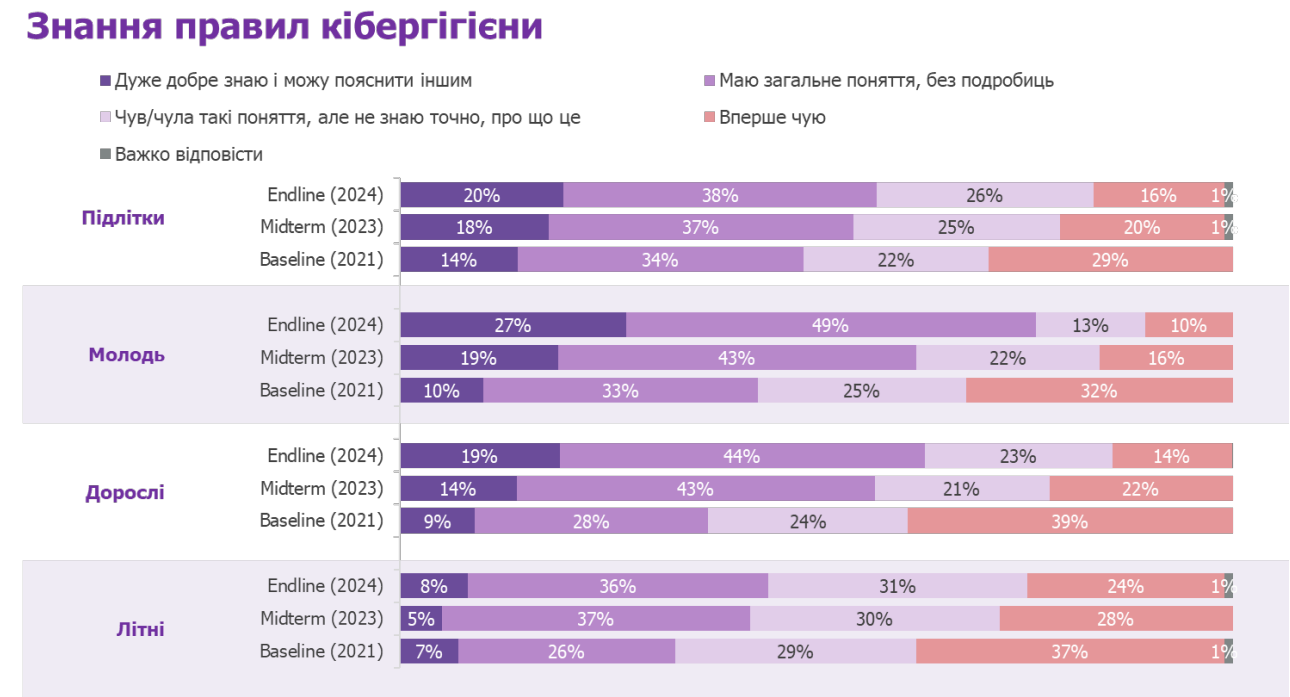
Загальний рівень знань про кібербезпеку



Обізнаність щодо правил кібергігієни нижча в усіх вікових групах (Діаграма 6). Як і щодо кібербезпеки загалом, молодь є найбільш обізнаною групою: хоча б загальне поняття про правила кібербезпеки мають 76% респондентів віком 18-25 років.

Найповільніше рівень знання про кібербезпеку і правила кібергігієни зростає у цільовій групі літніх людей (старше 60 років) — протягом усієї історії замірів частка респондентів, які «добре знають і можуть пояснити іншим», залишається на рівні 5-8%, а зростання обізнаності відбувається за рахунок відповідей «маю загальне поняття».

Діаграма 6. Скажіть, будь ласка, наскільки вам знайомі поняття «правила кібергігієни»? (% відповідей, за цільовими групами)



Ризикована поведінка

У рамках даного дослідження було запропоновано оцінити кілька варіантів ризикованої поведінки в інтернеті. Респонденти відповідали, наскільки ці поведінкові шаблони схожі на їхню власну поведінку. Порівнюючи результати замірів 2021-2044 років, незмінними лідерами ризикованої поведінки є три шаблони (Діаграма 7):

- Відсутність резервних копій документів та даних (46% їх не роблять);
- Невикористання двофакторної автентифікації (40% не використовують);
- Впевненість, що користувач є нецікавим для інтернет-шахраїв (58% впевнені у цьому хоча б частково, 21% впевнені точно).

Утім, позитивним сигналом є те, що частка респондентів, які не використовують двофакторну автентифікацію, а також вважають, що вони нецікаві для інтернет-шахраїв, поступово скорочується. Щодо останнього яскрава позитивна динаміка спостерігається у групі літніх людей (старше 60 років). Якщо під час baseline-заміру і midterm-замірів у 2021 і 2023 рр. більше половини цієї цільової групи були впевнені, що вони не цікаві для інтернет-шахраїв, то в 2024 році частка таких відповідей склала 45% (Таблиця 2). Зауважимо, що серед інших вікових груп впевненість у власній «нецікавості» або залишилася на рівні 2021 року, або навіть зросла.

Щодо інших шаблонів ризикованої поведінки, то порівняно з 2021 роком суттєво знизилось (хоч і не зникло) відвідування російських сайтів і соціальних мереж, а також зменшилась кількість поштових скриньок на російських серверах та скачування матеріалів з російських ресурсів.

Діаграма 7. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей)



Таблица 2. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей «Це точно про мене» + «Частково про мене», за цільовими групами)

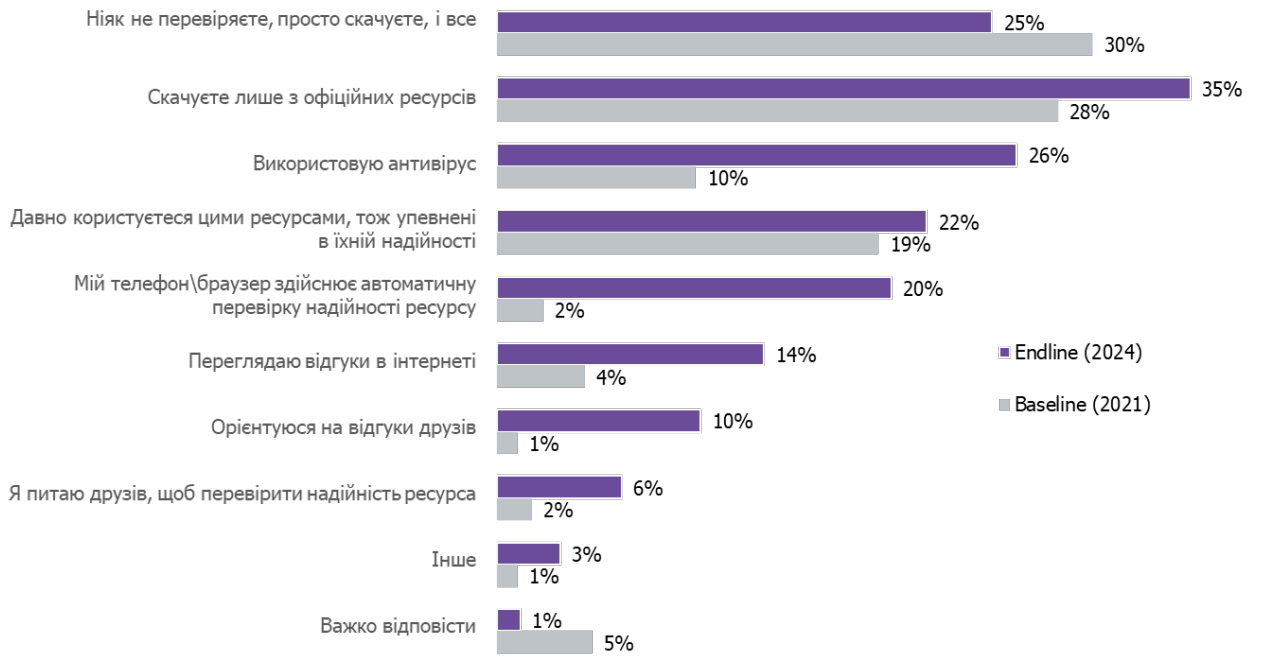
	Вік респондента											
	11-17 років			18-25 років			26-50 років			Більше 60 років		
	Endline (2024)	Midterm (2023)	Baseline (2021)	Endline (2024)	Midterm (2023)	Baseline (2021)	Endline (2024)	Midterm (2023)	Baseline (2021)	Endline (2024)	Midterm (2023)	Baseline (2021)
Я не роблю резервні копії документів, фотографій — для захисту даних	75,59%	76,91%	83,88%	68,59%	70,21%	72,31%	78,92%	75,51%	83,38%	92,67%	86,28%	90,69%
Я не використовую двофакторну автентифікацію, навіть якщо цього не вимагає політика безпеки сайту	61,52%	71,79%	78,62%	40,27%	59,75%	63,40%	66,90%	74,76%	72,07%	86,79%	90,52%	81,04%
Я не цікавий(-а) для інтернет-шахраїв	72,02%	65,89%	72,12%	58,87%	67,82%	54,92%	61,06%	61,83%	53,44%	45,22%	57,77%	52,07%
Якщо є анти-вірус, то мені нічого не загрожує	71,44%	54,11%	66,61%	46,46%	40,16%	51,77%	56,77%	47,56%	51,84%	44,19%	38,15%	56,48%
У мене один пароль на все, щоб завжди його пам'ятати	43,34%	50,03%	49,44%	38,60%	27,20%	48,08%	36,08%	32,04%	48,08%	44,05%	50,11%	48,08%
У мене простий пароль, тому що я боюся забути складний	47,78%	50,55%	48,08%	18,46%	16,31%	16,46%	33,66%	34,69%	36,52%	49,95%	52,45%	49,22%
Я не розумію, навіщо створювати різні паролі	36,71%	40,34%	45,15%	21,83%	22,17%	28,38%	27,07%	27,10%	26,53%	31,19%	36,46%	39,33%
Друзі або рідні знають мої паролі на випадок, якщо я забуду	39,18%	35,07%	39,04%	25,30%	14,27%	15,36%	23,79%	25,35%	27,48%	34,21%	39,75%	37,28%
Я іноді скачую відео, музику, книги, ігри або програми з так званих «піратських» сайтів	42,36%	-	-	37,91%	-	-	29,01%	-	-	13,00%	-	-
Я можу вставити чужу або незнайому флешку у свій комп'ютер	31,94%	30,51%	39,12%	25,10%	30,20%	35,01%	31,52%	26,66%	26,57%	12,27%	10,52%	14,78%
Я використовую відкритий WiFi в публічних місцях для здійснення платежів, купівлі квитків, товарів	45,92%	-	-	33,48%	-	-	25,47%	-	-	15,92%	-	-
Я відкриваю електронні листи і вкладення навіть з невідомих мені адрес електронної пошти або від незнайомців у месенджері	26,52%	28,05%	32,07%	29,80%	28,36%	33,54%	28,65%	23,45%	23,03%	11,02%	9,12%	12,51%
Я відвідую російські сайти	12,94%	14,83%	23,18%	19,49%	21,69%	40,37%	16,81%	18,66%	28,37%	15,85%	11,74%	23,70%
Я можу випадково «засвітити» дані банківської картки, паспорту, ю-ар коди квитків у соціальних мережах	13,26%	8,09%	10,38%	4,88%	6,68%	5,76%	6,38%	6,12%	5,36%	7,65%	6,05%	10,01%
Я відвідую заблоковані в Україні російські ресурси та соціальні мережі (такі як Яндекс, Вконтакті)	11,17%	11,96%	19,39%	7,13%	7,93%	29,04%	6,36%	7,27%	14,20%	5,46%	2,88%	12,83%
Я маю поштові електронні скриньки на російських поштових серверах	7,70%	5,71%	12,74%	5,36%	10,19%	16,33%	5,20%	7,40%	9,51%	2,30%	4,73%	7,60%
З російських ресурсів я іноді скачую файли, ігри або програми, заповнюю там анкети, реєструюсь чи вношу певні дані	14,58%	15,78%	23,15%	8,29%	7,16%	24,23%	3,18%	5,98%	10,92%	3,14%	4,29%	7,20%

Серед респондентів, які скачують матеріали з інтернету, 25% ніяк не перевіряють надійність ресурсу. Утім, частка таких відповідей знизилася (у 2021 році таких було 30%) (Діаграма 8). Натомість частка відповідей «скачую лише з офіційних ресурсів» зросла з 28% у baseline до 35% у endline замірі.

Також суттєво зросло використання антивірусу як запобіжника неприємним ситуаціям, а також вбудованих програм перевірки надійності ресурсів.

Про збільшення стурбованості користувачів свідчить також більша орієнтація на відгуки щодо надійності ресурсу — про це питають друзів, а також перевіряють відгуки в інтернеті.

Діаграма 8. Коли ви скачуєте матеріали, програми, ігри, як ви перевіряєте, що ресурс надійний? (% відповідей)



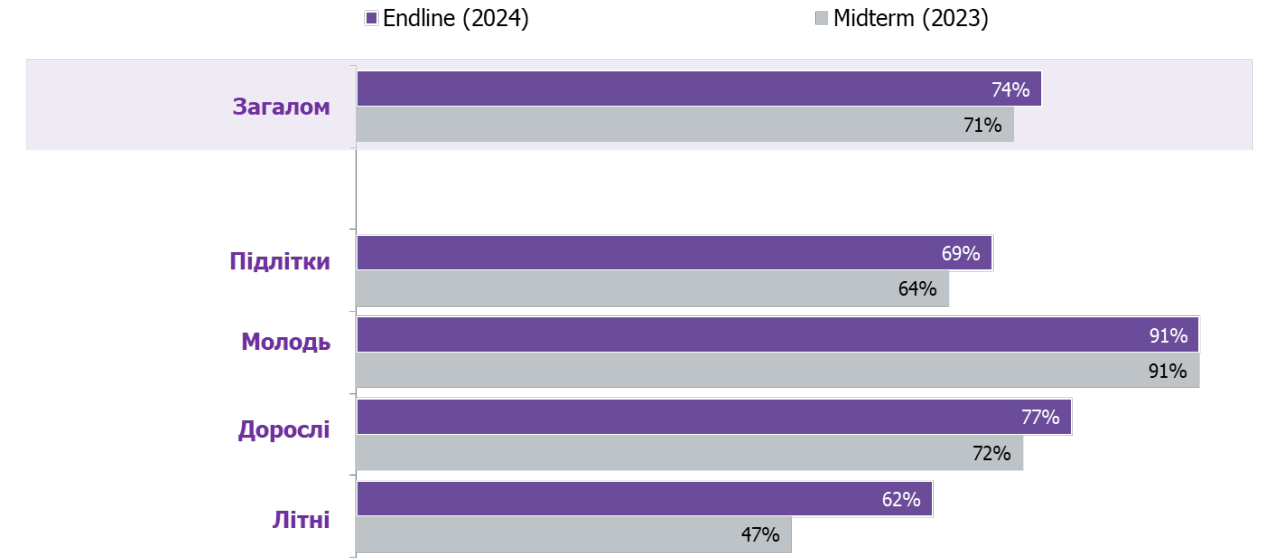
Здатність розпізнавати ризиковані ситуації

Здатність чітко розрізняти ризиковані ситуації є важливим чинником для підвищення безпеки в інтернеті. Без такої навички людина може або вважати інтернет повністю безпечним місцем і нехтувати правилами безпеки, або, навпаки, вважати, що небезпека очікує всюди і від неї неможливо захиститися.

Для розуміння, наскільки респонденти здатні розрізняти ризиковані ситуації, ми запропонували їм для оцінки десять прожективних ситуацій. Ці питання було сформульовано, як життєві ситуації, в які можуть потрапити респонденти або їх родичі або знайомі. Кожну ситуацію респондентам пропонувалося оцінити як безпечну або ризиковану з точки зору кібербезпеки. П'ять з десяти ситуацій, на думку експертів Представництва Фонду цивільних досліджень та розвитку США в Україні, є безпечними і п'ять — небезпечними.

Як індикатор здатності розрізняти ризиковані ситуації ми взяли частку респондентів, які здатні правильно розрізнити п'ять або більше ситуацій (тобто правильно позначити безпечні та небезпечні ситуації). Результати аналізу наведені на Діаграмі 9.

Діаграма 9. Здатність розпізнавати ризиковані ситуації (частка респондентів, які правильно розпізнали від п'яти ситуацій)



Загалом частка респондентів, які правильно розпізнали 5 і більше ризикованих і безпечних ситуацій, зросла з 71% у 2023 році до 74% у 2024 році.

Найгіршу здатність розрізняти ризиковані ситуації продемонстрували літні люди (62%). Утім, саме в цій групі спостерігається найбільша позитивна динаміка (плюс 15 в.п. порівняно з 2023 роком).

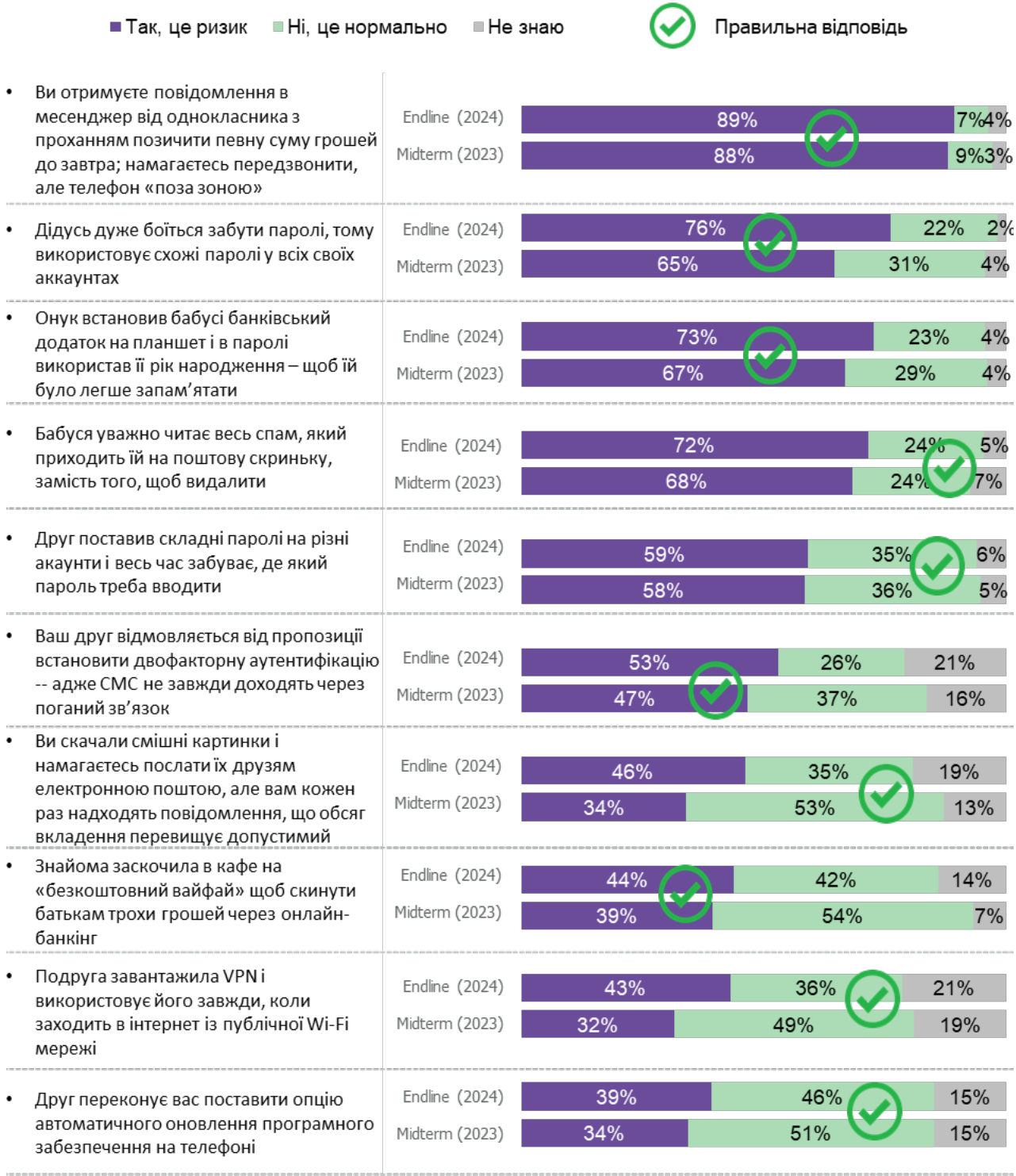
Найкраще усі групи респондентів розпізнають ситуацію вимагання грошей від «нібито» друга у соціальних мережах — її розпізнала як ризиковану найбільша частка респондентів: 89% серед підлітків і більше 90% серед усіх інших груп респондентів (Діаграми 10-13). Загалом здатність розрізняти ризиковані і безпечні ситуації порівняно до 2023 року зросла.

Підлітки значно частіше стали вважати ризиком ситуацію, коли паролі однакові для всіх акаунтів. Також підлітки частіше стали ідентифікувати ризики користування публічним WiFi, а також відмови від двофакторної автентифікації.

Загалом відмову від двофакторної автентифікації стали частіше вважати ризиком всі групи респондентів, утім, для людей літнього віку ця концепція залишається незрозумілою — значна частка респондентів не змогла оцінити ситуацію використання двофакторної автентифікації.

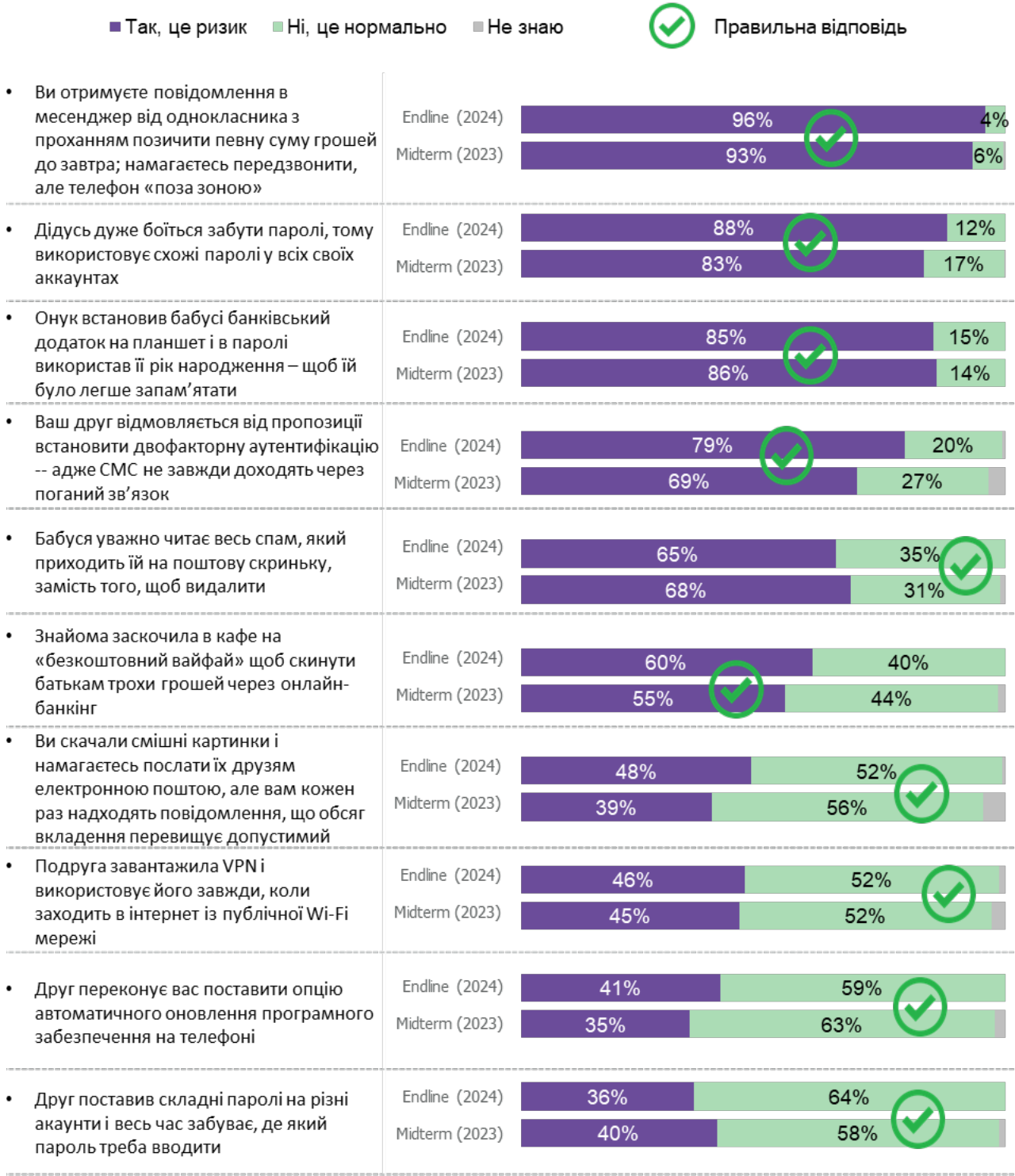
Значна частка респондентів помилково вважать загрозовими використання VPN та автоматичного оновлення застосунків.

Діаграма 10. Розпізнавання ризикованих ситуацій. Розподіл за цільовою групою 11-17 років (% відповідей)

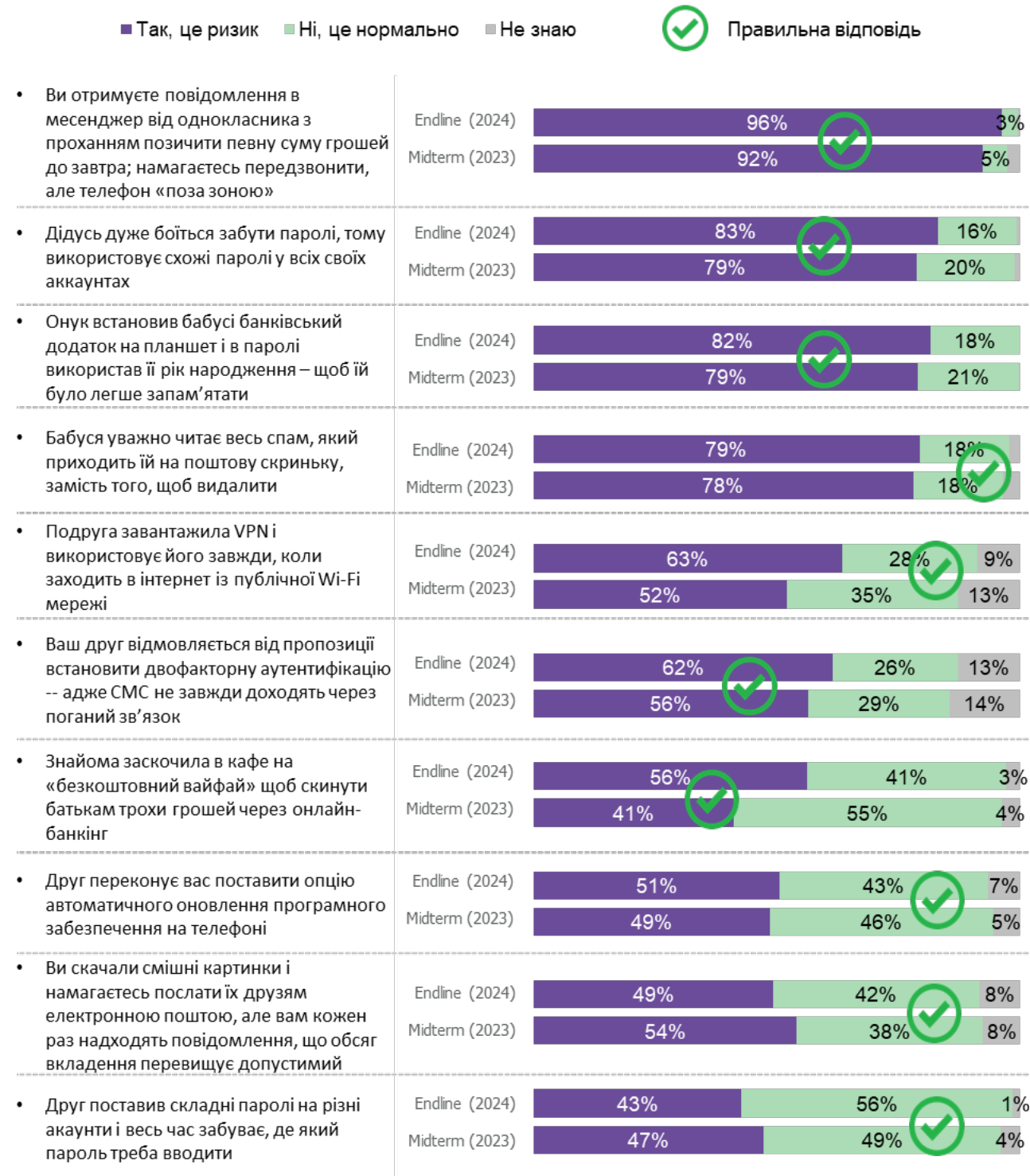


РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Діаграма 11. Розпізнавання ризикованих ситуацій. Розподіл за цільовою групою 18-25 років (% відповідей)

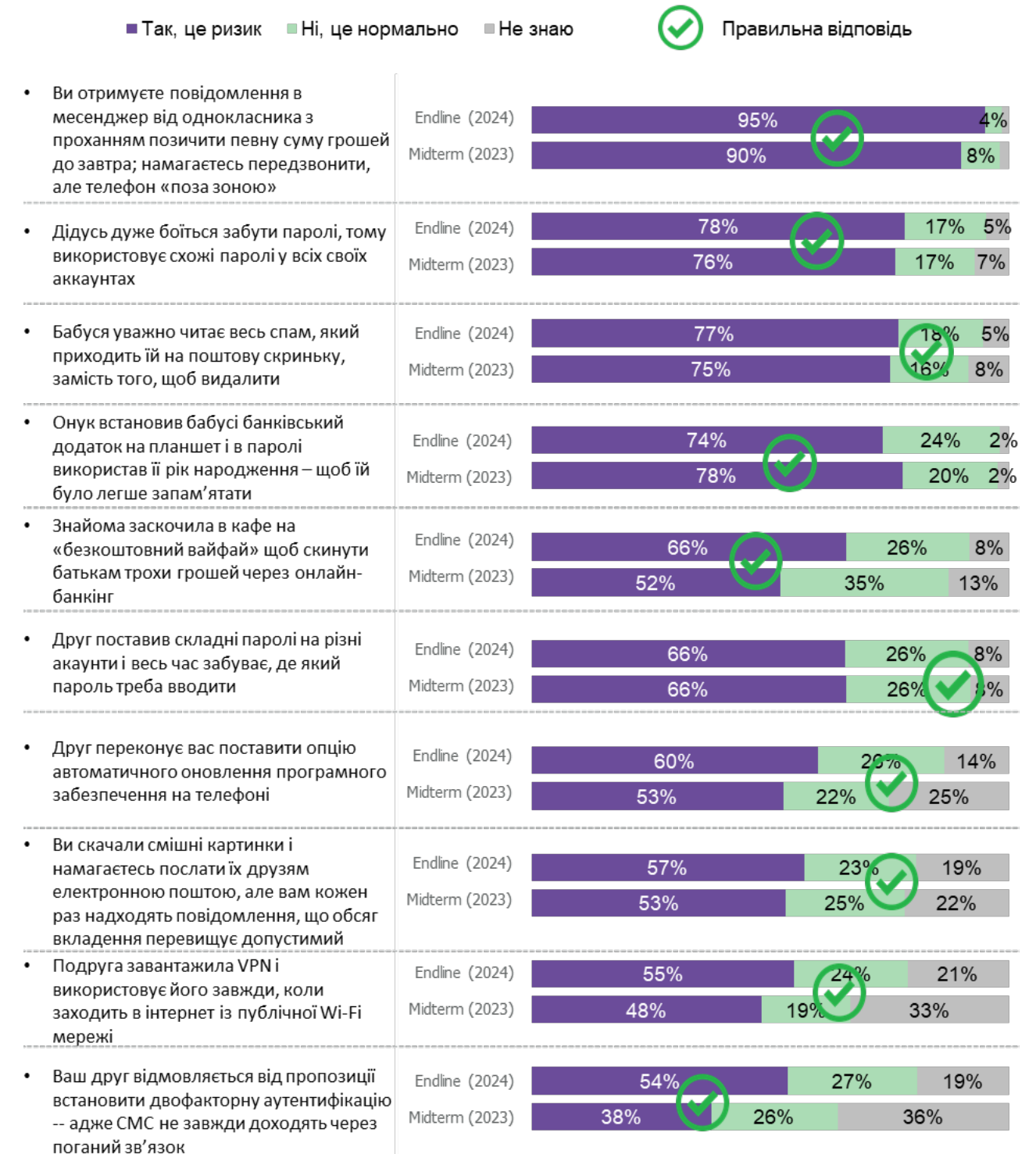


Діаграма 12. Розпізнавання ризикованих ситуацій. Розподіл за цільовою групою 26-59 років (% відповідей)



РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Діаграма 13. Розпізнавання ризикованих ситуацій. Розподіл за цільовою групою старше 60 років (% відповідей)



Досвід зіткнення із кіберзагрозами

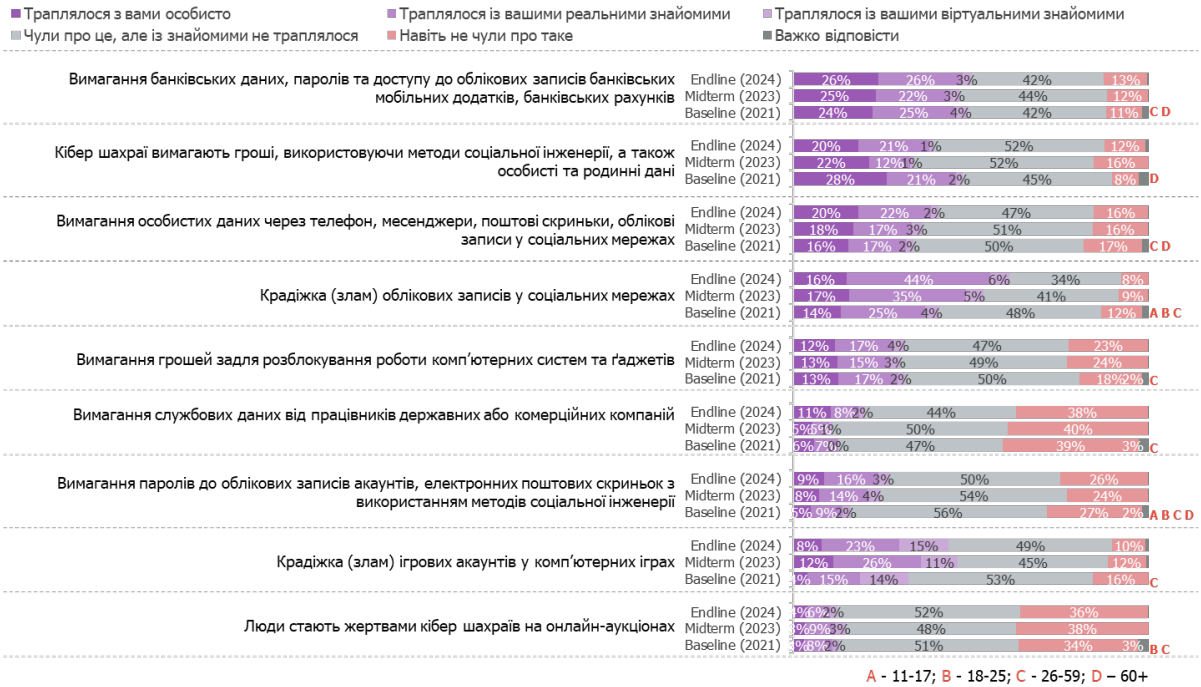
Ми запропонували респондентам оцінити свій досвід зіткнення із кіберзагрозами для моніторингу ситуації та проведення порівняльного аналізу з даними попередніх замірів у 2021 і 2023 рр.

Кожній цільовій групі було запропоновано окремий перелік кіберзагроз, які, на думку експертів, притаманні саме цій віковій групі; щодо кожної кіберзагрози респонденти могли позначити, чи траплялася така ситуація з ними особисто або з їхніми реальними чи віртуальними знайомими.

За показником «траплялося зі мною особисто» першість посідає ситуація, коли кібершахраї вимагають дані банківських карток, паролі та доступ до облікових записів мобільних додатків, — з цим стикався кожен четвертий респондент. Друге місце поділили ситуації вимагання грошей з використанням методів соціальної інженерії (маніпуляції, погрози, шантаж), а також особистих та родинних даних (через телефон та месенджери).

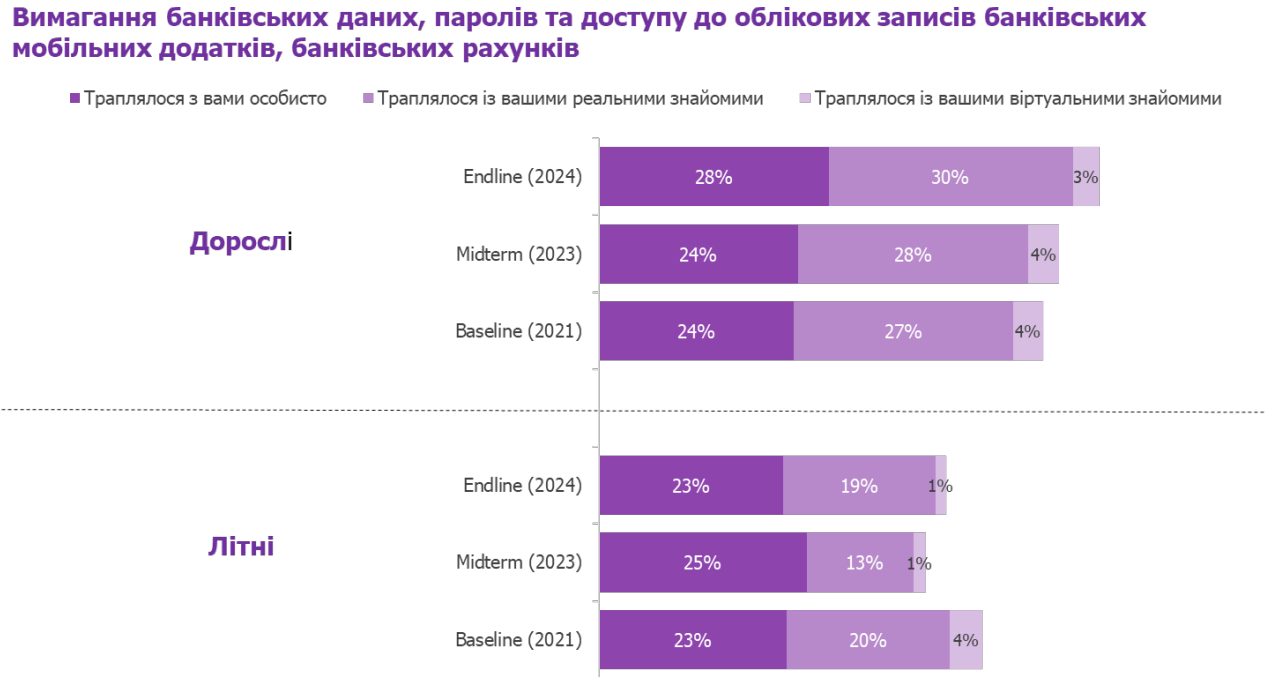
З показником «траплялося з вашими реальними знайомими» перше місце незаперечно належить ситуації зламу облікових записів в соціальних мережах. Більше того, це єдина ситуація, щодо якої спостерігається невпинне і значне зростання частки респондентів, які мають знайомих, що стали жертвами такого зламу (25%, 35% і 44% відповідно у baseline, midterm і endline-замірах).

Діаграма 14. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей)



З вимаганням банківських даних майже рівною мірою особисто стикалися люди віком 26-59 та 60+ років (28% і 23% відповідно). Серед літніх людей менша частка тих, хто чув про такі випадки від знайомих, але це може бути пов'язане з меншим колом спілкування порівняно до молодшої аудиторії.

Діаграма 15. Чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей)



Досвід вимагання особистих даних вище серед «дорослої» аудиторії порівняно до літніх респондентів. Утім, серед респондентів 26-59 років частка тих, хто стикався з такою ситуацією, зросла у 2024 році порівняно до 2021-2023 рр.

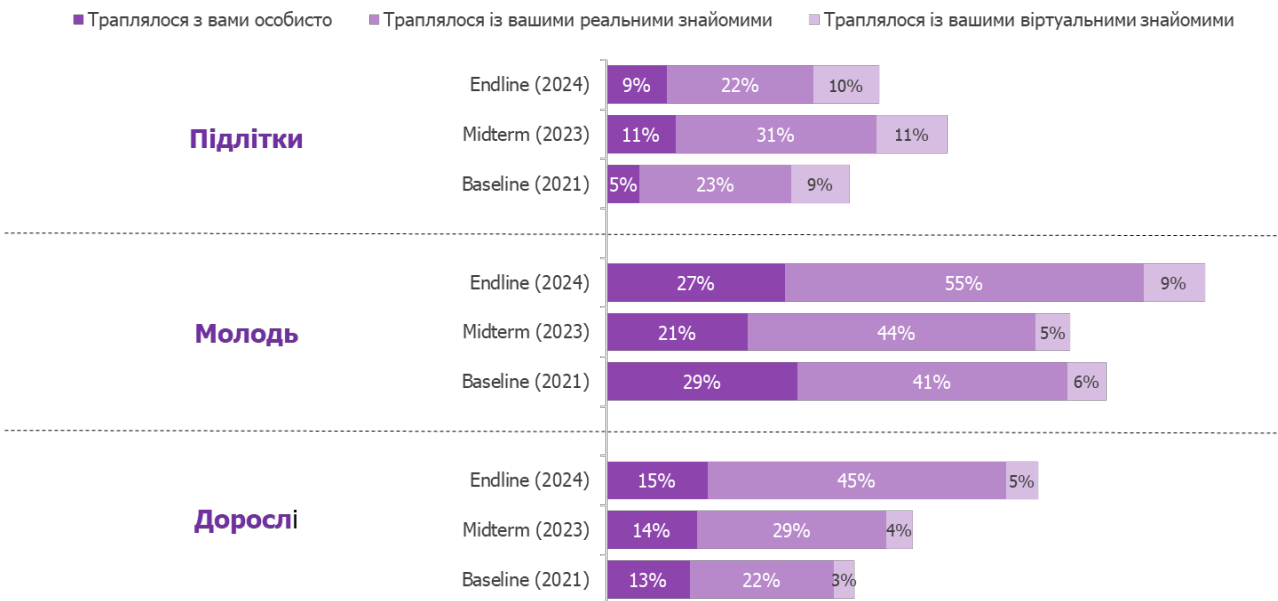
Діаграма 16. Чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей)



Крадіжка (злам) облікових записів в соціальних мережах найчастіше фіксує молода аудиторія 18-25 років: 27% стикалися з такою ситуацією особисто, а 55% чули про це від знайомих. Серед підлітків ця ситуація розповсюджена в 2-3 рази менше.

Діаграма 17. Чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей)

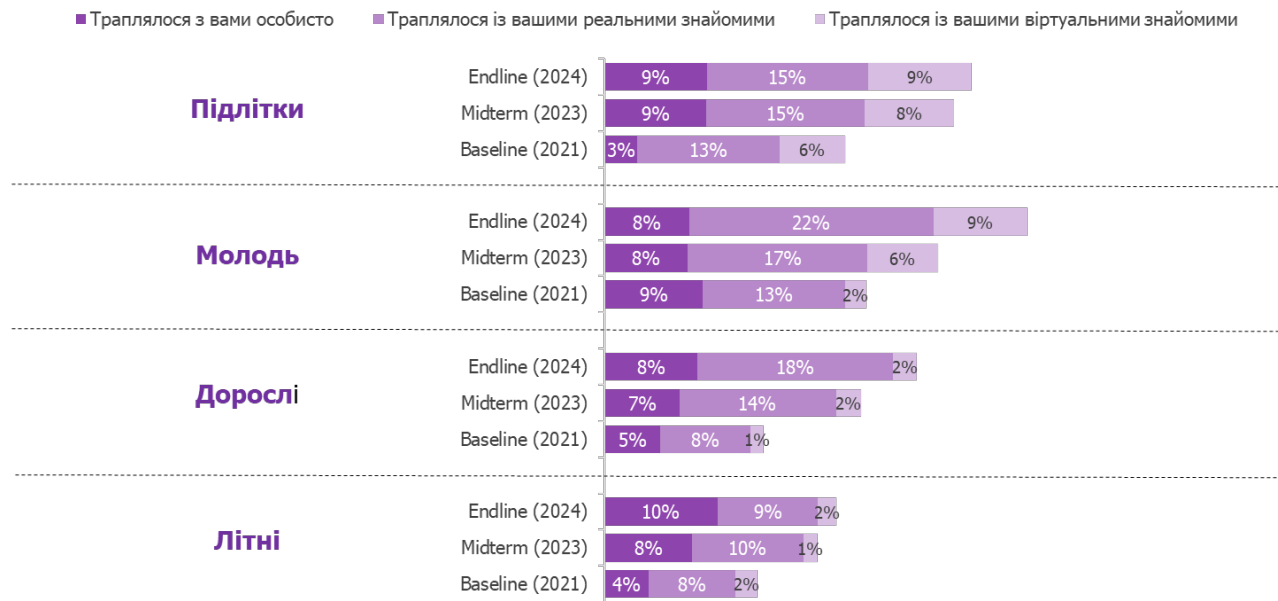
Крадіжка (злам) облікових записів у соціальних мережах



З вимаганням паролів до облікових записів стикалися респонденти усіх вікових груп, на щастя, особистий досвід не перевищує 10% в кожній віковій групі.

Діаграма 18. Чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей)

Вимагання паролів до облікових записів акаунтів, електронних поштових скриньок з використанням методів соціальної інженерії



Онлайн-аукціони залишаються екзотикою в Україні. Про те, що вони стали жертвами кібершахраїв, заявили 3-4% респондентів.

Діаграма 19. Чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей)

Люди стають жертвами кібер шахраїв на онлайн-аукціонах



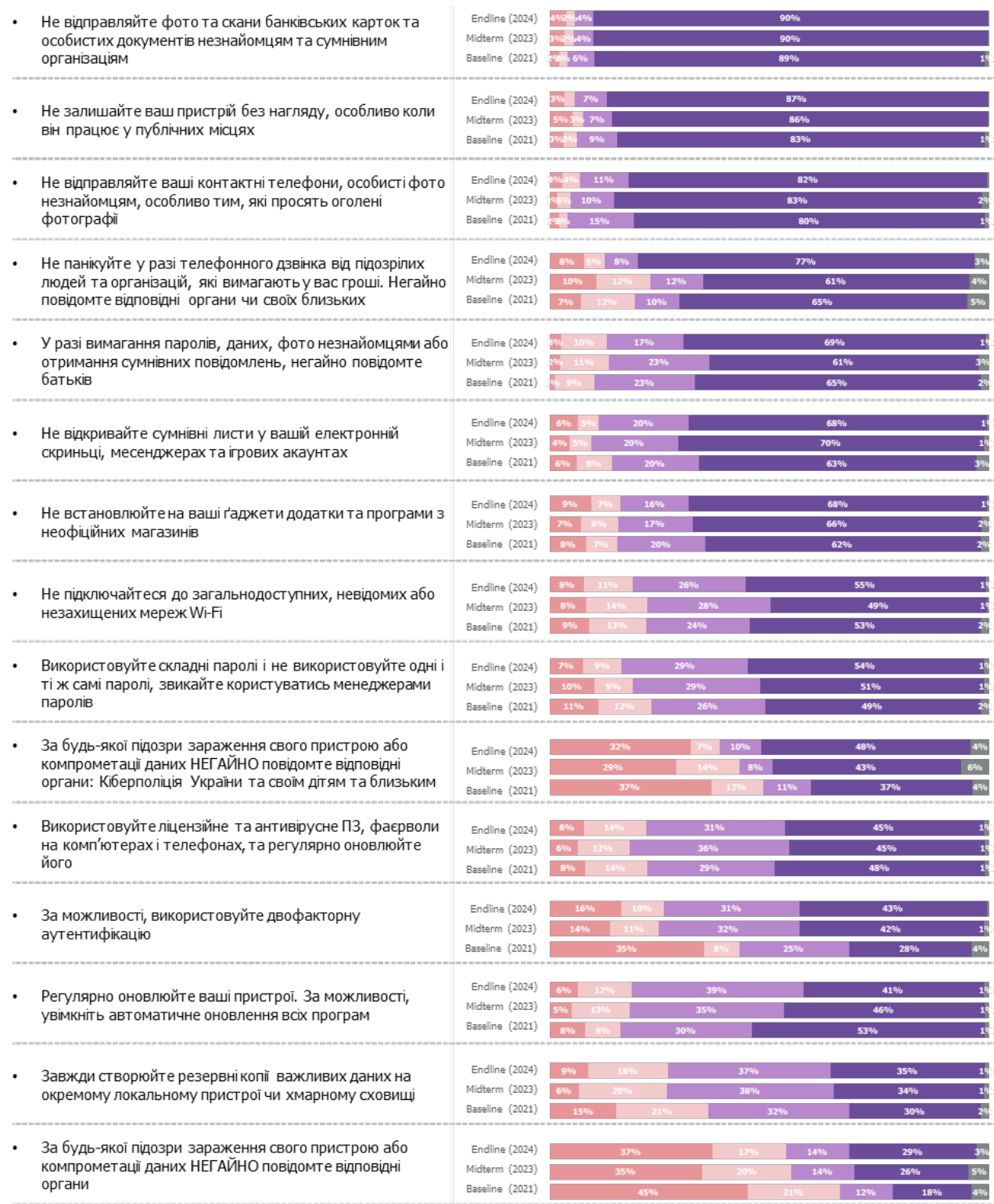
Обізнаність із правилами кібербезпеки

У рамках даного дослідження також піднімалися питання базових правил кібергігієни. Ми надали аудиторії можливість оцінити ставлення до базових правил кібергігієни для моніторингу ситуації та відстежування тенденцій. Серед ТОП-3 базових, найбільш вживаних правил кібергігієни з 2021 року залишаються такі:

- Не можна відправляти фото та скани особистих банківських карток та документів незнайомцям та сумнівним організаціям (90%);
- Не можна залишати пристрій без нагляду, коли він працює, у публічних місцях (87%);
- Не варто відправляти контактні телефони, особисті фото незнайомцям, особливо тим, які просять оголені фотографії (82%).

З більшістю правил аудиторії обізнані (див. Діаграма 20).

Діаграма 20. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей)



Вперше чую

Знаю, але не дотримуюся

Знаю і дотримуюся інколи

Знаю і завжди дотримуюся

Важко відповісти

Аби порівняти, наскільки кожна вікова група знає і виконує правила кібербезпеки та наскільки дані показники змінились із плином часу, ми порахувати кілька інтегральних показників. Три показники відображають частку респондентів, які:

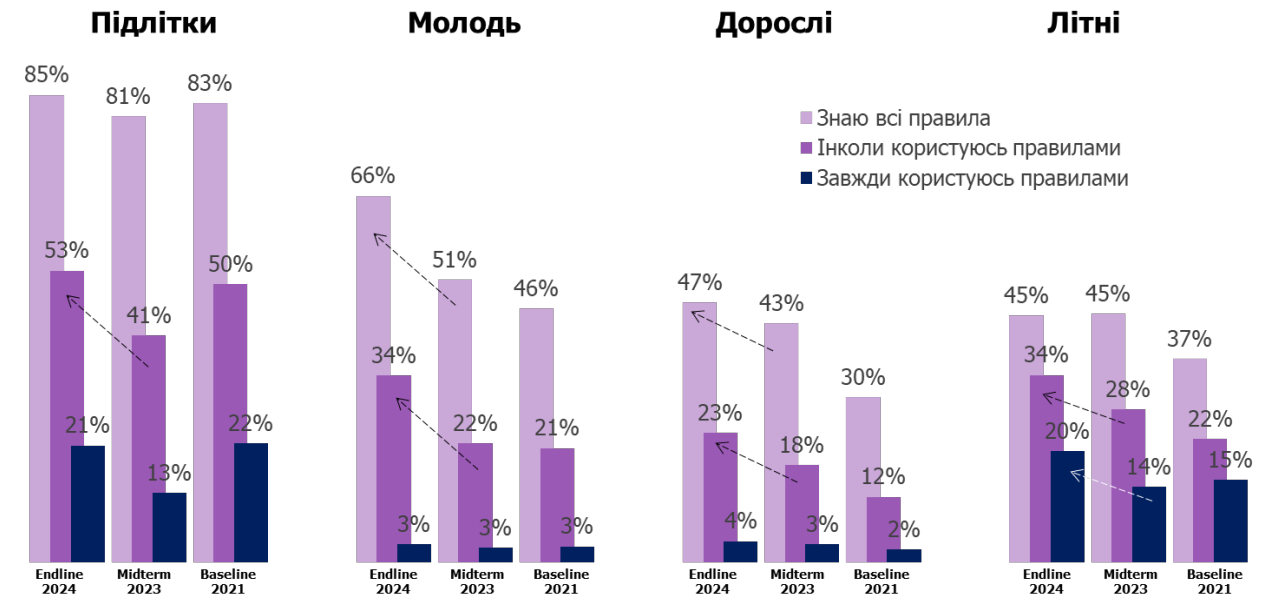
- Знають усі правила кібербезпеки;
- Застосовують усі правила кібербезпеки хоча б іноді;
- Завжди застосовують усі правила кібербезпеки.

За результатами аналізу цих інтегральних показників, підлітки 11-17 років залишаються найбільш обізнаною групою: 85% знають усі правила кібербезпеки, 41% виконують усі правила хоча б інколи, постійно виконують усі правила 21% (Діаграма 21). Таким чином, показник обізнаності залишається на рівні попередніх замірів, а от показники застосування правил кібербезпеки серед підлітків зросли порівняно до midterm-заміру. Таким чином, показники виконання правил у групі підлітків залишаються найвищими серед решти цільових груп: серед молоді 18-25 років хоча б інколи виконують правила 34%, у групі 25-59 років — 23%, серед найстарших респондентів понад 60 років — майже третина (34%). Зауважимо, що показники виконання правил зросли в усіх вікових групах.

Знання правил кібербезпеки помітно зросло у групі молоді (з 51% у 2023 році до 66% у 2024 році).

Найстарша і наймолодша групи респондентів є найбільш свідомими: частка тих, хто завжди виконує всі правила, становить 20-21%. Утім, якщо порахувати частку виконання правил до обізнаності, то серед літніх людей майже половина з тих, хто знає всі правила кібербезпеки, завжди їх виконує.

Діаграма 21. Знання і виконання правил кібербезпеки. Розподіл за цільовими групами (% відповідей)



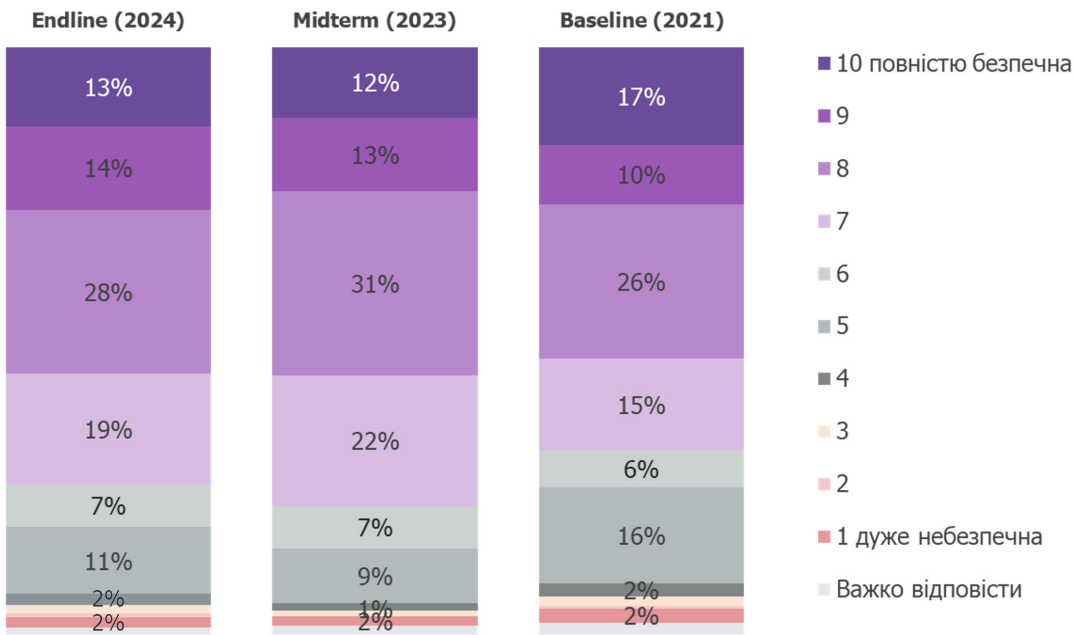
Безпека поведінки в інтернеті

Для самооцінки власної безпечної поведінки в інтернеті респондентам було запропоновано шкалу від 1 до 10, де 1 означає «дуже небезпечна», а 10 — «повністю безпечна». На основі цієї шкали було виділено такі типи поведінки:

- Дуже небезпечна (1-6)
- Помірно безпечна (7-8)
- Повністю безпечна (9-10)

Частка респондентів, які вважають свою поведінку в інтернеті повністю безпечною, майже не змінилася і становить 25-27% протягом 2021-2024 рр. Натомість відчуття помірно безпечної поведінки зросло з 41% у 2021 році до 53-47% у 2023-2024 роках. Частка тих, хто вважає свою поведінку дуже небезпечною, становить 24% (29% в baseline та 20% у midterm) (Діаграма 22).

Діаграма 22. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? (% відповідей)

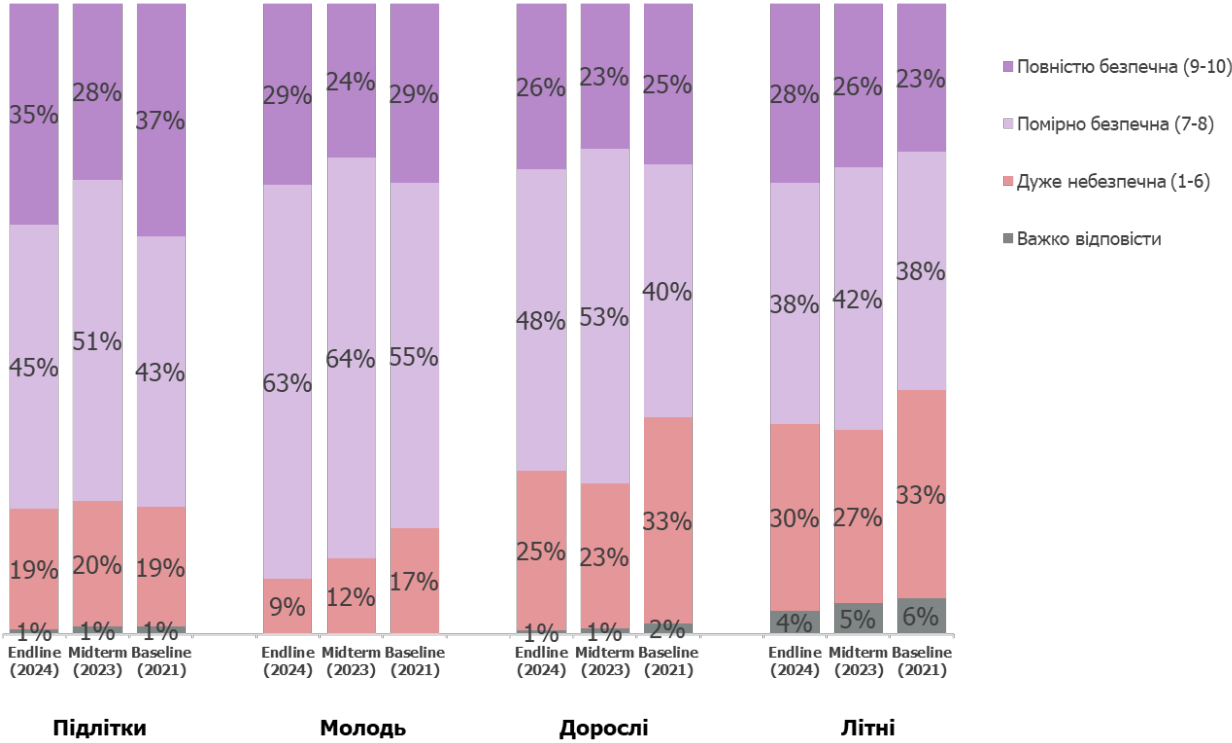


Оцінки власної безпеки значною мірою варіюють із віком (Діаграма 23). Серед підлітків (11-17 років) та молоді (18-25 років) менше тих, хто вважає, що поводить себе небезпечно (19% та 9% відповідно, при цьому серед молоді показник стрімко спадає). Водночас, серед людей старше 25 років більше тих, хто вважає перебування в інтернеті небезпечним (25-30% серед дорослих і літніх людей відповідно).

Серед підлітків найбільша частка тих, хто вважає, що поводить себе повністю безпечно (35%), тоді як серед інших вікових груп ця частка хоч і не суттєво, однак менша.

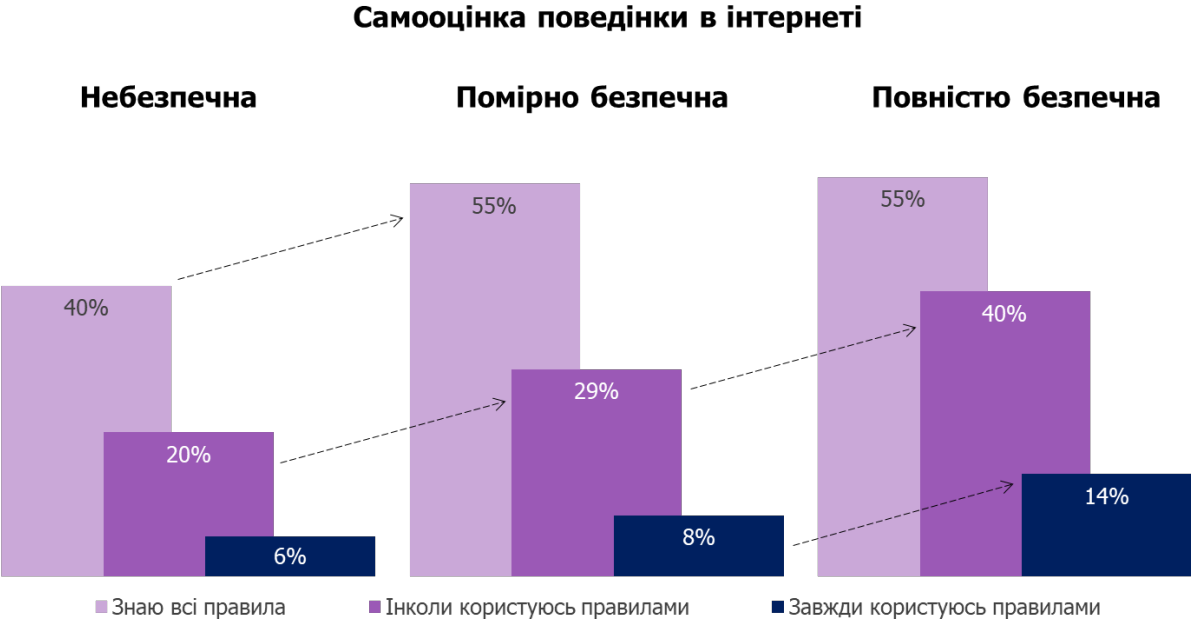
Загалом серед молоді до 25 років частка тих, хто вважає свою поведінку безпечною, є більшою, ніж частка тих, хто вважає, що поводить себе небезпечно.

Діаграма 23. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? Розподіл за цільовими групами (% відповідей)



Самооцінка поведінки в інтернеті залежить від знання та виконання правил кібербезпеки: чим вище людина оцінює безпеку своєї поведінки, тим краще вона знає і частіше виконує правила кібербезпеки (Діаграма 24).

Діаграма 24. Користування правилами кібербезпеки (% відповідей відповідно до самооцінки поведінки в інтернеті)



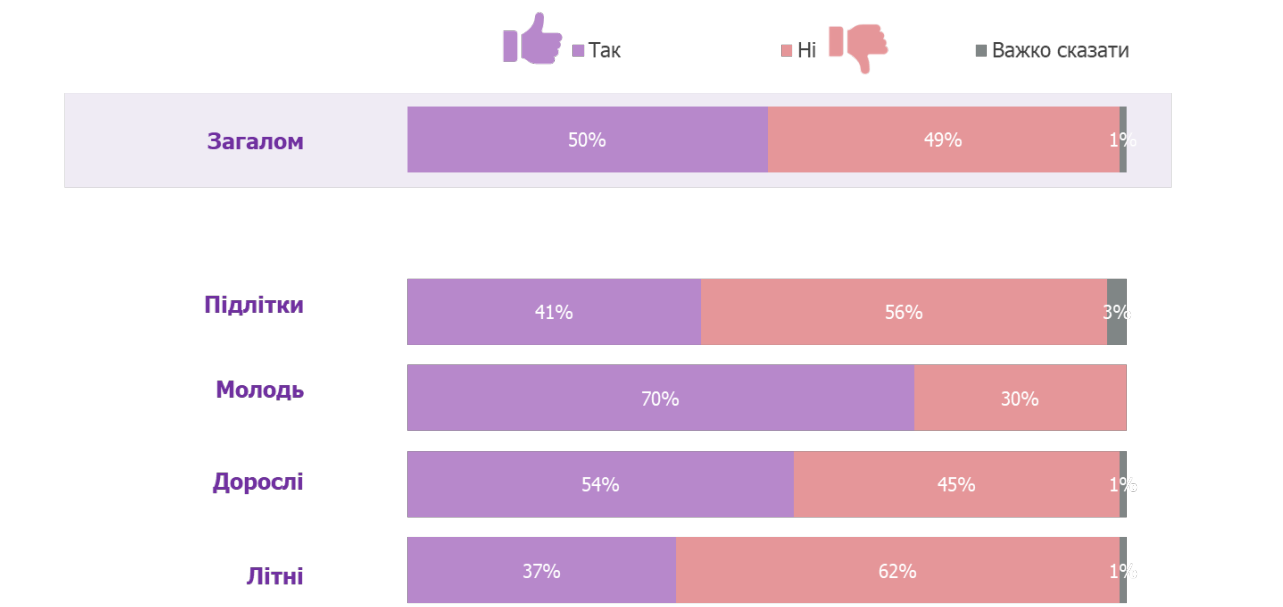
Інформаційні матеріали та оцінка динаміки поведінки

В endline-замірі було додано питання «Чи бачили ви за останній рік матеріали, публікації, відео про правила безпечної поведінки в інтернеті?». Розподіл відповідей представлено на Діаграмі 25: з такими матеріалами в середньому стикався кожен другий респондент. Найчастіше з матеріалами про кібербезпеку стикалися респонденти віком 18-25 років (що пояснює їхню кращу обізнаність з поняттями «кібербезпека» і «правила кібергігієни»).

Найгірше охоплення матеріалами про правила безпечної поведінки в інтернеті зафіксовано в групах підлітків і людей літнього віку (41% та 37% відповідно бачили подібні матеріали)

Щодо джерел розповсюдження подібних матеріалів, то найчастіше згадують такі: Інтернет, соціальні мережі, Кіберполіція (респонденти старшої вікової групи), робота (молодь і дорослі), школа (підлітки).

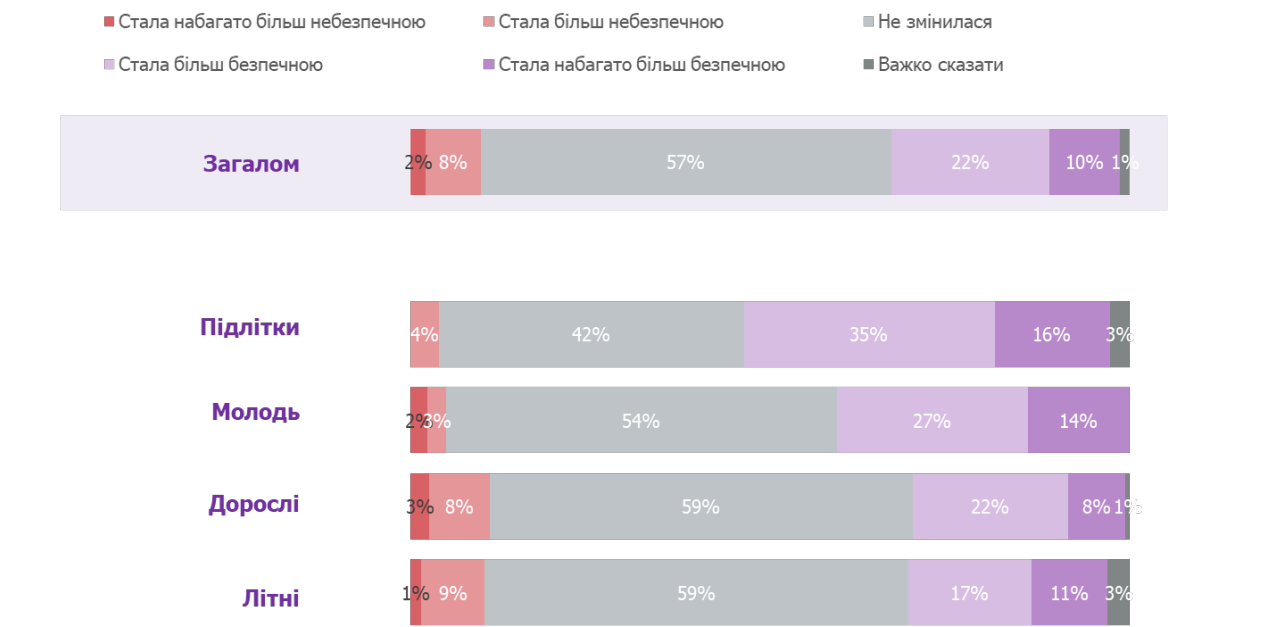
Діаграма 25. Чи бачили ви за останній рік матеріали, публікації, відео про правила безпечної поведінки в інтернеті? (% відповідей)



Також в endline-замірі було додано питання «Яким чином змінилася ваша поведінка в інтернеті за останній рік?». В середньому кожен десятий респондент зазначив, що його/її поведінка стала більш небезпечною (Діаграма 26). Таких респондентів приблизно удвічі більше серед старших вікових груп (25-59 років і 60+ років), ніж серед молоді і підлітків.

Відповідно, молодь і підлітки більше схильні оцінювати зміни своєї поведінки на краще. Так, серед підлітків майже половина впевнені, що їхня поведінка стала більш безпечною. Серед молоді частка таких відповідей становить 41%, серед дорослих — 30%, а серед літніх людей — 28%. Утім, для всіх вікових груп балансовий показник (частка позитивних змін мінус частка негативних змін) є позитивним, тобто зміни на краще переважають.

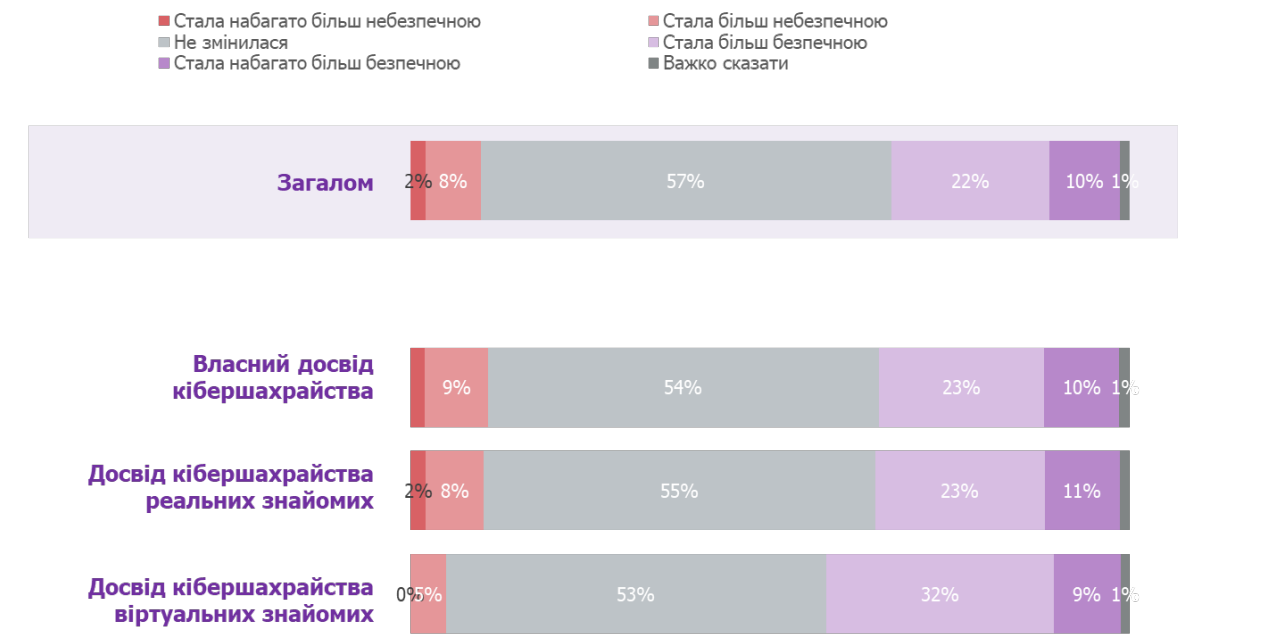
Діаграма 26. Яким чином змінилася ваша поведінка в інтернеті за останній рік? (% відповідей)



При оцінці чинників, які можуть впливати на зміну поведінки, ми також оцінили досвід стикання із кібершахрайством (Діаграма 27) і доступ до матеріалів з кібербезпеки (Діаграма 28).

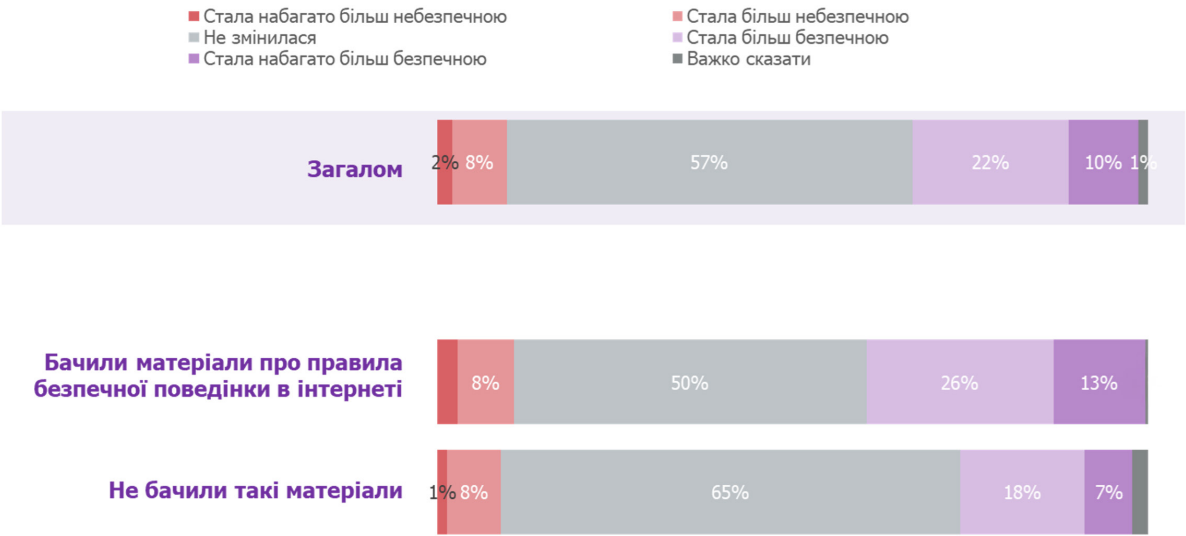
Найчастіше про позитивні зміни у поведінці кажуть респонденти, які беруть до уваги досвід кібершахрайства своїх віртуальних знайомих. Вірогідно, це люди, які чутливі до тематики кібербезпеки, і саме тому зважають на досвід кібершахрайства віртуальних знайомих.

Діаграма 27. Яким чином змінилася ваша поведінка в інтернеті за останній рік? (% відповідей відповідно до досвіду кібершахрайства)



Серед тих, хто бачив матеріали про правила безпечної поведінки в інтернеті, 39% оцінюють зміни у власній поведінки як такі, що сприяють більшій безпеці. Для порівняння, серед тих, хто не бачив подібних матеріалів, частка позитивних змін становить 25%.

Діаграма 28. Яким чином змінилася ваша поведінка в інтернеті за останній рік? (% відповідей відповідно до досвіду перегляду матеріалів про кібербезпеку)



Утім, перегляд матеріалів з кібербезпеки не гарантує виконання усіх правил кібербезпеки — частка респондентів, які виконують усі правила, майже не залежить від перегляду матеріалів. А от рівень обізнаності та рівень виконання окремих правил — суттєво зростає (Діаграма 29).

Діаграма 29. Користування правилами кібербезпеки (% відповідей відповідно до досвіду перегляду матеріалів про кібербезпеку)

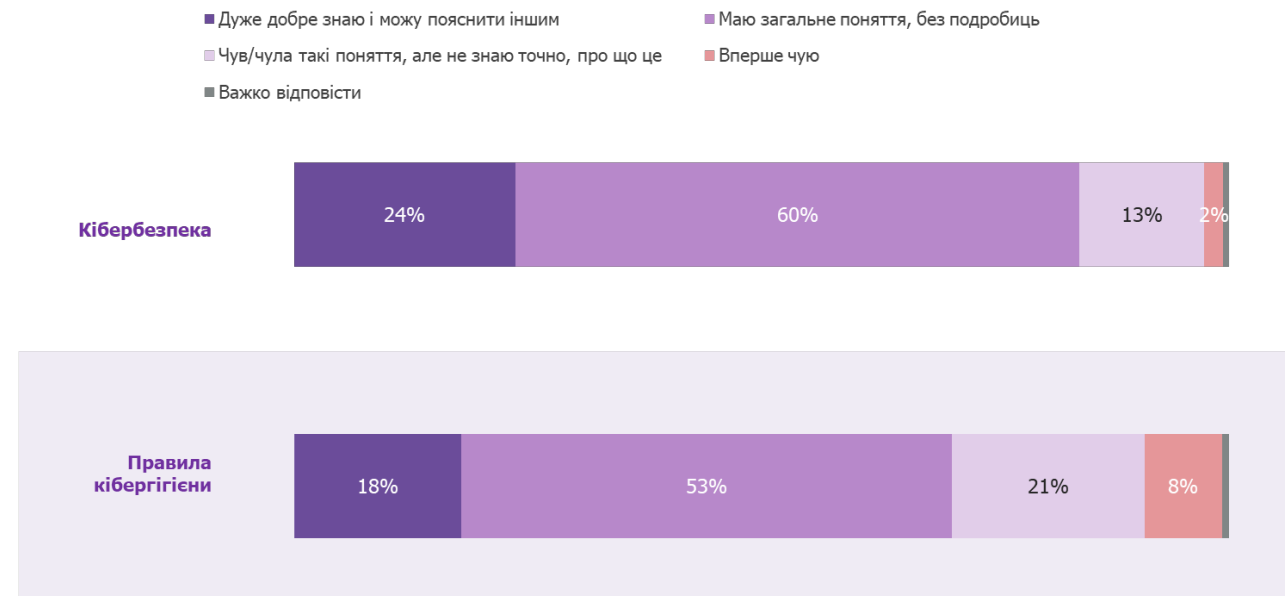


Оцінка інформаційних матеріалів

Для оцінки інформаційних матеріалів проєкту «Інформаційна кампанія про кібербезпеку» програми кібербезпеки Представництва Фонду цивільних досліджень та розвитку США в Україні було проведено опитування респондентів онлайн.

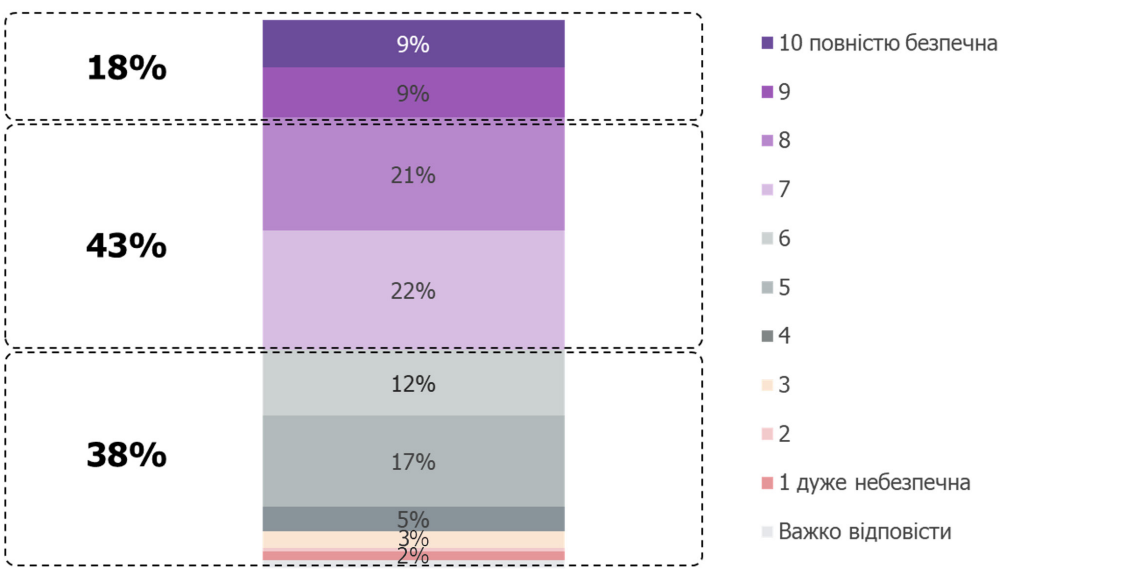
Вибірка репрезентативна дорослому населенню України за віком, статтю, регіоном та розміром населеного пункту, утім, серед учасників онлайн-опитування трохи вищий рівень обізнаності про кібербезпеку і правила кібергігієни (Діаграма 30), а також суттєво гірша самооцінка власної поведінки в інтернеті (Діаграма 31).

Діаграма 30. Обізнаність про кібербезпеку і правила кібергігієни (% відповідей)



Гірші показники самооцінки можуть пояснюватися кращим рівнем обізнаності: учасники онлайн-панелі як більш активні інтернет-користувачі можуть краще усвідомлювати ризики і наслідки ризикованої поведінки.

Діаграма 31. Самооцінка поведінки в інтернеті (% відповідей)

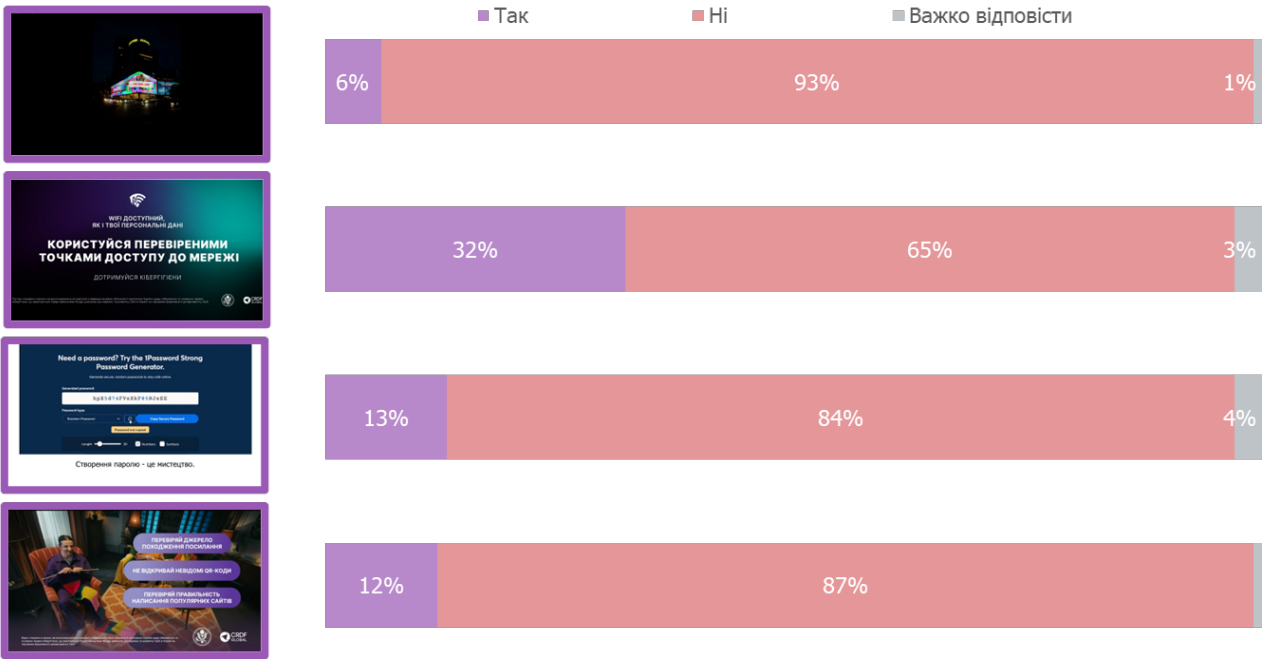


Респондентам онлайн-опитування було запропоновано кілька матеріалів проєкту «Інформаційна кампанія про кібербезпеку» програми кібербезпеки Представництва Фонду цивільних досліджень та розвитку США в Україні:

- 1. Зовнішня реклама на екрані ТРЦ «Гулівер» (Київ);
- 2. Зовнішня реклама в містах України;
- 3. Всеукраїнський урок з кібергігієни;
- 4. Соціальна реклама на Телемарафоні.

Найбільше охоплення — у зовнішньої реклами в містах України: її бачили 32% опитаних (Діаграма 32). Найменше — у рекламного ролика в ТРЦ «Гулівер»: його пригадали лише 6%. Інші матеріали (всеукраїнський урок та соціальну рекламу) бачили 12-13%.

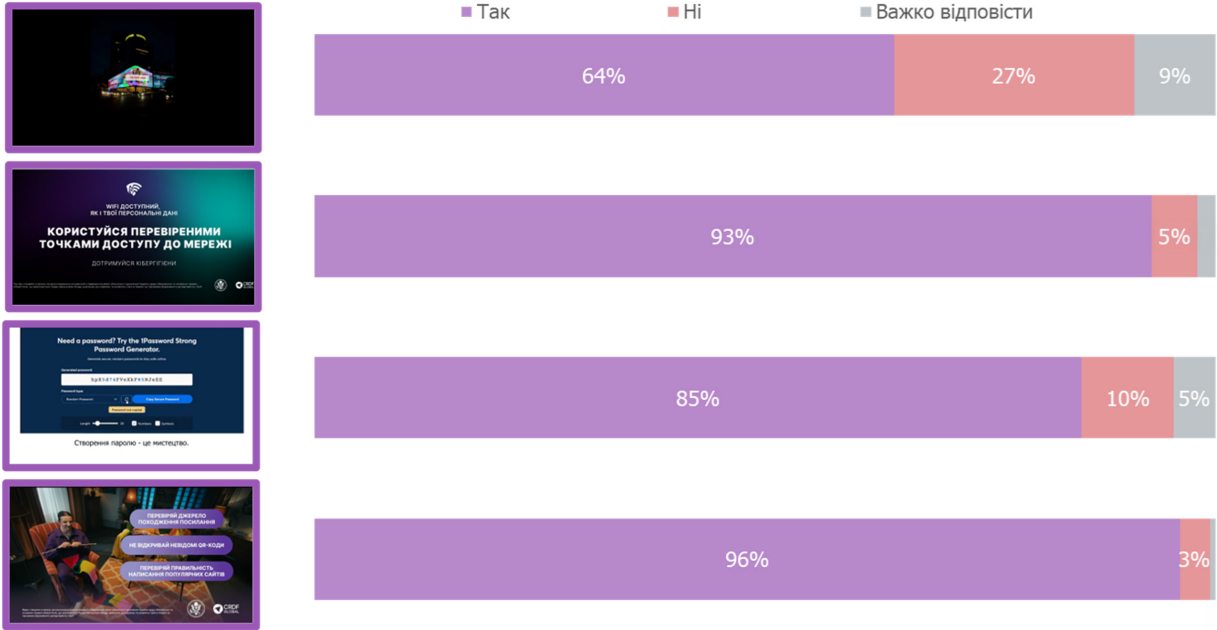
Діаграма 32. Порівняння матеріалів — досвід попереднього перегляду (% відповідей)
Чи бачили раніше?



За показником зрозумілості основної думки першість також посідає зовнішня реклама в містах України, а також соціальний ролик на Телемарафоні — понад 93% і 96% опитаних відповідно сказали, що основна думка їм цілком зрозуміла (Діаграма 33).

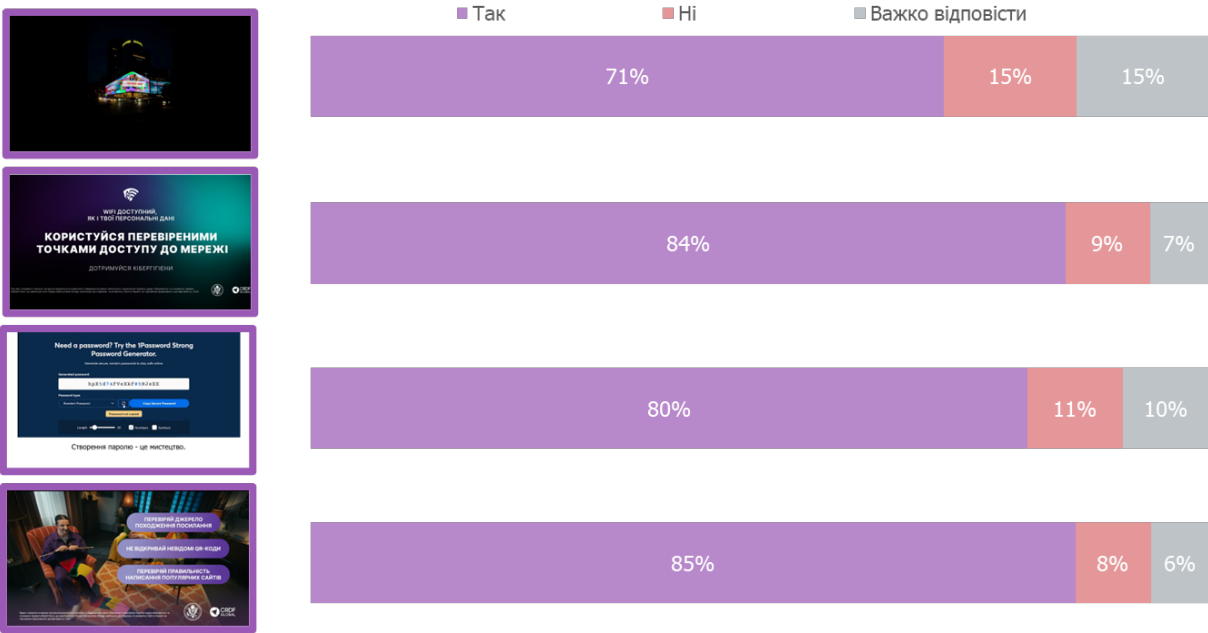
Основну думку рекламного ролика в ТРЦ «Гулівер» зрозуміли лише 64% опитаних.

Діаграма 33. Порівняння матеріалів — зрозумілість основної думки (% відповідей)
Чи зрозуміла основна думка матеріалу?



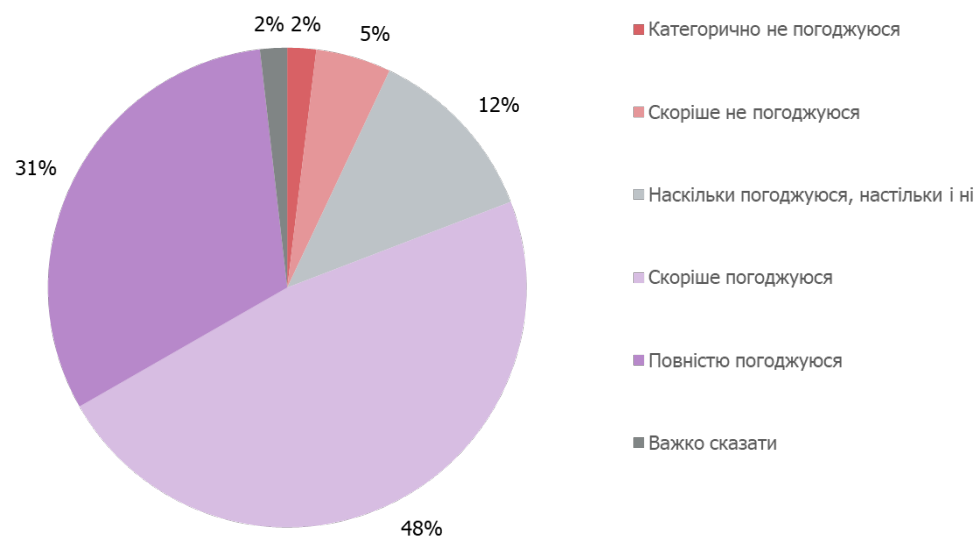
Готовність змінити поведінку на більш безпечну корелює із зрозумілістю основної думки: найкращі показники (84-85%) у зовнішньої реклами в містах України і соціального ролика на Телемарафоні, найгірший — у рекламного ролика в ТРЦ «Гулівер» (71%) (Діаграма 34).

Діаграма 34. Порівняння матеріалів — готовність змінити поведінку (% відповідей)
Чи готові Ви змінити поведінку в інтернеті на більш безпечну?



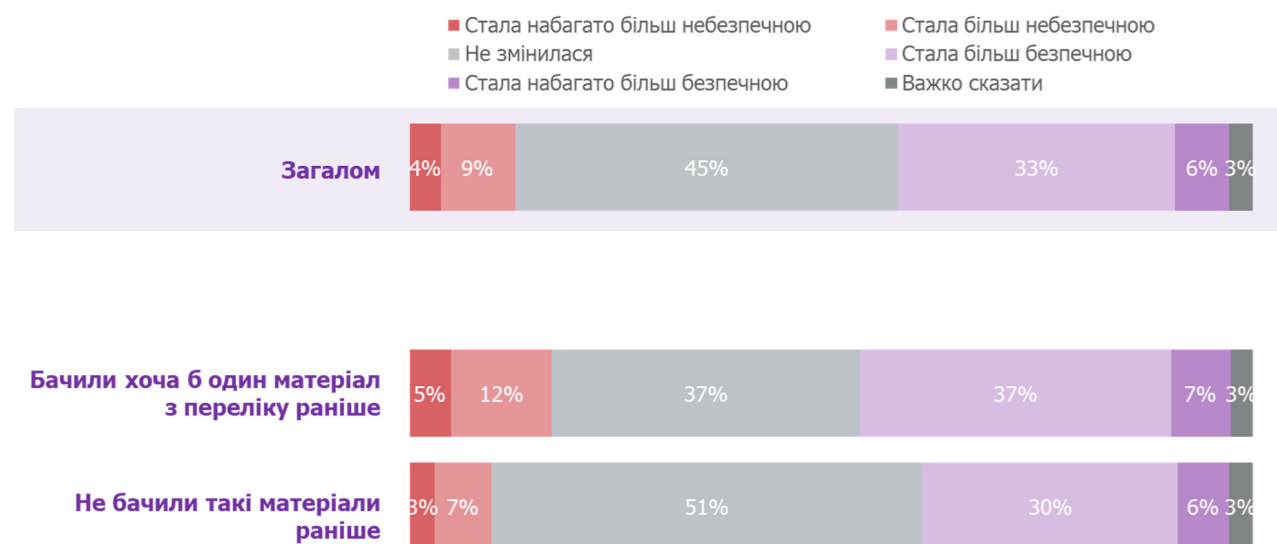
Загалом майже 80% опитаних погоджуються з твердженням, що після перегляду подібних інформаційних матеріалів їхня поведінка в інтернеті стає більш безпечною. Частка респондентів, які не погоджуються з цією думкою, становить лише 7%.

Діаграма 35. Наскільки ви погоджуєтесь із твердженням: «Після перегляду подібних інформаційних матеріалів моя поведінка в інтернеті стає більш безпечною»? (% відповідей)



Загалом 39% респондентів онлайн-опитування впевнені, що за останній рік їхня поведінка стала більш безпечною (Діаграма 36). Серед тих, хто бачив хоч один з матеріалів інформаційної кампанії Представництва Фонду цивільних досліджень та розвитку США в Україні раніше (а таких 39% респондентів), частка тих, хто змінив поведінку на краще, становить 44%. Проте також більшою є частка тих, хто засвідчив, що поведінка погіршилася з точки зору безпеки (17% серед тих, хто бачили матеріали, порівняно до 10% тих, хто не бачили ці матеріали раніше). Утім, це також може бути пов'язане із усвідомленням загроз і ризиків власної поведінки.

Діаграма 36. Яким чином змінилася ваша поведінка в інтернеті за останній рік? (% відповідей відповідно до досвіду перегляду матеріалів про кібербезпеку)



ВИКЛИКИ І ПЕРСПЕКТИВИ



Протягом проведення baseline, midterm та endline досліджень ми стикнулися з низкою викликів. Midterm та endline дослідження були проведені уже після початку повномасштабного вторгнення РФ в Україну, що означає, що і інтерв'юери, і респонденти, і аналітики повною мірою стикнулися з усіма викликами воєнного часу, а також паралельно із проведенням дослідження мали дбати про безпекові питання.

Утім, одним з найбільших викликів стала швидка втрата фокусу і втомлюваність респондентів:

- Так, анкета baseline опитування (2021 рік) налічувала 20 питань (окрім демографії) і середня тривалість опитування складала 16 хвилин.
- Анкета midterm опитування (2023 рік) налічувала 9 питань (окрім демографії), але середня тривалість опитування також складала 16 хвилин.
- Анкета endline опитування (2024 рік) налічувала 14 питань (окрім демографії), тривалість опитування також складала 26 хвилин.

Таким чином, реалії воєнного часу, зокрема втрату фокусу і швидку втомлюваність респондентів слід брати до уваги при розробці подальшого плану досліджень. Також цей факт слід брати до уваги при розробці інформаційних кампаній, зокрема з точки зору складності повідомлень, кількості і частоти інтервенцій тощо. При підготовці інформаційних інтервенцій також слід врахувати, що в воєнний час питання фізичної безпеки є набагато більш актуальними, ніж питання кібербезпеки.

Щодо подальшого плану досліджень, то ми рекомендуємо більше уваги приділити бар'єрам використання правил кібергігієни. Адже зростання обізнаності щодо правил поведінки в інтернеті є обов'язковим, але не достатнім чинником для практичного запровадження цих правил у щоденні рутини. Для вивчення цих бар'єрів рекомендовано провести докладний розвідувальний етап якісними методами (глибинні інтерв'ю, фокус-групові дискусії, спостереження), що дозволить сформулювати гіпотези, чому люди свідомо нехтують правилами кібергігієни. Такі гіпотези можуть бути підтверджені або спростовані шляхом кількісних опитувань.

Також метод фокус-групових обговорень корисно застосовувати при розробці інформаційних матеріалів, зокрема для того, щоб оцінити як зрозумілість основної думки, так і пошукати важелі, які можуть вплинути на фактичну, а не декларовану зміну поведінки в інтернеті на більш безпечну.

ДОДАТКИ



Додаток 1. Опитувальник

Відбір респондента

S1. Скажіть, будь ласка, скільки вам виповнилося повних років?

Запишіть _____ і закодуйте

0	Менше 10 років	КІНЕЦЬ
1	11-17 років	Продовжити, КВОТА N = 300 (CAPI)
2	18-25 років	Продовжити, КВОТА N = 300 (CAPI)
3	26-59 років	Продовжити, КВОТА N = 300 (CAPI)
4	Більше 60 років	Продовжити, КВОТА N = 300 (CAPI)
5	Відмова	КІНЕЦЬ

S2. Позначте стать респондента

Одна відповідь, не зачитувати

1	Чоловік	Контроль квот всередині вікової страти
2	Жінка	Контроль квот всередині вікової страти

S3. Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами?

Одна відповідь, зачитати

1	Проводжу в інтернеті більшу частину дня	
2	Кілька сесій на день, але не більшу частину дня	
3	Щоденно, одна-дві сесії	
4	3-4 рази на тиждень	
5	1-2 рази на тиждень	
6	3-4 рази на місяць	
7	1-2 рази на місяць	
8	Рідше, ніж один раз на місяць	КІНЕЦЬ
9	Взагалі не користуюсь Інтернетом	КІНЕЦЬ
99	Важко відповісти (ВВ) (не зачитувати!)	КІНЕЦЬ

ОСНОВНИЙ ОПИТУВАЛЬНИК

A1.1. Чи виконуєте ви наступні дії в інтернеті і як часто?

Зачитати альтернативи. Одна відповідь у рядку.

Шкала:

1. Щодня
2. Кілька разів на тиждень
3. Раз на тиждень
4. Раз на місяць
5. Кілька разів на рік
6. Ніколи
99. ВВ (не зачитувати)

Програміст: РОТАЦІЯ РЯДКІВ	
1	Заходите на сторінки, читаете стрічки соціальних мереж (такі як Тік Ток, Фейсбук, Інстаграм)
2	Допикуєте або розміщуєте фотографії в соціальних мережах
3	Купуєте товари в інтернет-магазинах (в тому числі у соціальних мережах, таких як Фейсбук, Інстаграм)
4	Сплачуєте за товари або послуги банківською картою через інтернет
5	Користуєтеся інтернет-банкінгом (переказуєте кошти, переглядаєте залишок на рахунку, управляєте рахунками)
6	Завантажуєте відео, музику, статті, книги, інші матеріали
7	Підключаєтеся до публічних вай-фай мереж (в кафе, публічних місцях)
8	Користуєтеся електронною поштою
9	Користуєтеся месенджерами (Вайбер, Телеграм, Ватсап, Фейсбук)
10	Користуєтеся ВіПіЕн (наприклад, для доступу на сайти, які заблоковано)
11	Граєте в ігри онлайн
12	Робите покупки з ігрових акаунтів
13	Скачуєте безкоштовні програми, ігри
14	Встановлюєте різні програми, доповнення до браузерів

A1.2. Коли ви скачуєте матеріали, програми, ігри, як ви перевіряєте, що ресурс надійний?

Не зачитувати! Можна кілька відповідей

1. Ніяк не перевіряєте, просто скачуєте, і все
2. Скачуєте лише з офіційних ресурсів
3. Давно користуєтеся цими ресурсами, тож упевнені в їхній надійності
4. Використовую антивірус
5. Переглядаю відгуки в інтернеті
6. Не скачую нічого
7. Мій телефон/браузер здійснює автоматичну перевірку надійності ресурсу
8. Я питаю друзів, щоб перевірити надійність ресурсу
9. Орієнтуюся на відгуки друзів
98. Інше: записати _____
99. ВВ (не зачитувати!)

A1. Основна тема нашої розмови — це кібербезпека та правила кібергігієни. Скажіть, будь ласка, наскільки вам знайомі ці поняття? Оберіть варіант відповіді: «дуже добре знаю і можу пояснити іншим», «маю загальне поняття, без подробиць», «чув/чула такі поняття, але не знаю точно, про що це» або «вперше чую».

Одна відповідь у стовпчику.

	Кібербезпека	Правила кібергігієни
Дуже добре знаю і можу пояснити іншим	1	1
Маю загальне поняття, без подробиць	2	2
Чув/чула такі поняття, але не знаю точно, про що це	3	3
Вперше чую	4	4
ВВ (не зачитувати!)	99	99

A2. Деякі типи поведінки в інтернеті можуть бути ризикованими і призводити до негативних наслідків. Я зачитаю різні ситуації, у які потрапляють інші люди, а ви скажіть, чи вважаєте ви таку ситуацію ризикованою, чи це нормально:

Програміст, випадковий порядок тверджень!	Так, це ризик	Ні, це нормально	Не знаю
Онук встановив бабусі банківський додаток на планшет і в паролі використав її рік народження — щоб їй було легше запам'ятати	1	2	99
Ваш друг відмовляється від пропозиції встановити двофакторну аутентифікацію -- адже СМС не завжди доходять через поганий зв'язок	1	2	99
Знайома заскочила в кафе на «безкоштовний вайфай» щоб скинути батькам трохи грошей через онлайн-банкінг	1	2	99
Ви отримуєте повідомлення в месенджер від однокласника з проханням позичити певну суму грошей до завтра; намагаєтесь передзвонити, але телефон «поза зоною»	1	2	99
Дідусь дуже боїться забути паролі, тому використовує схожі паролі у всіх своїх акаунтах	1	2	99
Друг переконує вас поставити опцію автоматичного оновлення програмного забезпечення на телефоні	1	2	99
Подруга завантажила VPN і використовує його завжди, коли заходить в інтернет із публічної Wi-Fi мережі	1	2	99
Бабуся уважно читає весь спам, який приходить їй на поштову скриньку, замість того, щоб видалити	1	2	99
Друг поставив складні паролі на різні акаунти і весь час забуває, де який пароль треба вводити	1	2	99
Ви скачали смішні картинки і намагаєтесь послати їх друзям електронною поштою, але вам кожен раз надходять повідомлення, що обсяг вкладення перевищує допустимий	1	2	99

A3. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас. Ви можете сказати «це точно про мене», «це частково про мене» або «це точно не про мене».

Одна відповідь.

Шкала

1. Це точно про мене
2. Частково про мене
3. Це точно НЕ про мене
99. ВВ (не зачитувати)

Програміст: РОТАЦІЯ РЯДКІВ	
1	У мене простий пароль, тому що я боюся забути складний
2	У мене один пароль на все, щоб завжди його пам'ятати
3	Друзі або рідні знають мої паролі на випадок, якщо я забуду
4	Я не розумію, навіщо створювати різні паролі
5	Я не цікавий(-а) для інтернет-шахраїв
6	Якщо є антивірус, то мені нічого не загрожує
7	Я відкриваю електронні листи і вкладення навіть з невідомих мені адрес електронної пошти або від незнайомців у месенджері
8	Я можу вставити чужу або незнайому флешку у свій комп'ютер
9	Я можу випадково «засвітити» дані банківської картки, паспорту, к'ю-ар коди квитків у соціальних мережах
10	Я використовую двофакторну автентифікацію, навіть якщо цього не вимагає політика безпеки сайту (наприклад, банківські додатки) * для групи 11-17 років додати інструкцію. <i>Інтерв'юер! У разі необхідності поясніть: двофакторна автентифікація — це додатковий рівень захисту для вашого облікового запису, а саме після стандартного пароля потрібно також ввести ще цей додатковий код доступу, який автоматично надсилається SMS-повідомленням або ви бачите додатковий код доступу на екрані.</i>
11	Я регулярно роблю резервні копії документів, фотографій — для захисту даних
12	Я відвідую російські сайти (які закінчуються на «крапка RU»)
13	Я маю поштові електронні скриньки на російських поштових серверах
14	Я відвідую заблоковані в Україні російські ресурси та соціальні мережі (такі як Яндекс, ВКонтакте)
15	З російських ресурсів (крапка RU) я іноді скачую файли, ігри або програми, заповнюю там анкети, реєструюсь чи вношу певні дані
16	Я іноді скачую відео, музику, книги, ігри або програми з так званих «піратських» сайтів
17	Я використовую відкритий вай-фай в публічних місцях для здійснення платежів, купівлі квитків, товарів

A4. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією?

Зачитати альтернативи. Кілька відповідей.

Варіанти відповідей

1.

Траплялося з вами особисто
2.

Траплялося із вашими реальними знайомими
3.

Траплялося із вашими віртуальними знайомими
4.

Чули про це, але із знайомими не траплялося
5.

Навіть не чули про таке
99.

ВВ (не зачитувати)

Програміст: РОТАЦІЯ РЯДКІВ		S1 = ...			
Увага, програміст:		1	2	3	4
Виводити альтернативи відповідно до вікових груп					
1	Крадіжка (злам) облікових записів у соціальних мережах	x	x	x	
2	Крадіжка (злам) ігрових акаунтів у комп'ютерних іграх	x			
3	[Формулювання для S1 =1] Довірче вимагання паролів до облікових записів, акаунтів, електронних поштових скриньок, ігрових бонусів, банківських даних батьків з використанням методів соціальної інженерії (маніпуляцій, погроз, шантажу) та секстингу (повідомлення сексуального характеру)	x	x	x	x
	[Формулювання для S1 =2,3,4] Вимагання паролів до облікових записів акаунтів, електронних поштових скриньок з використанням методів соціальної інженерії (маніпуляцій, погроз, шантажу)				
4	Люди стають жертвами кібершахраїв на онлайн-аукціонах		x	x	
5	Вимагання особистих даних через телефон, месенджери, поштові скриньки, облікові записи у соціальних мережах			x	x
6	Вимагання банківських даних, паролів та доступу до облікових записів банківських мобільних додатків, банківських рахунків (у т.ч. через телефон, месенджери)			x	x
7	Вимагання грошей задля розблокування роботи комп'ютерних систем та гаджетів (електронних пристроїв)			x	
8	Вимагання службових даних від працівників державних або комерційних компаній			x	
9	Кібершахраї вимагають гроші, використовуючи методи соціальної інженерії (маніпуляції, погрози, шантаж), а також особисті та родинні дані (через телефон та месенджери)				x

A5. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом. Ви можете обрати відповідь «Вперше чую», «Знаю, але не дотримуюся», «Знаю і дотримуюся інколи» або «Знаю і завжди дотримуюся».

Зачитати альтернативи. Одна відповідь у рядку.

Шкала

1.

Вперше чую
2.

Знаю, але не дотримуюся
3.

Знаю і дотримуюся інколи
4.

Знаю і завжди дотримуюся
99.

ВВ (не зачитувати)

Програміст: РОТАЦІЯ РЯДКІВ		S1 =			
Увага, програміст:		1	2	3	4
Виводити альтернативи відповідно до вікових груп					
1	[Формулювання для S1 =1] Використовуйте складні паролі і не використовуйте одні і ті ж самі паролі для реєстрації на онлайн-ресурсах, у соціальних мережах та ігрових мобільних додатках, зникайте користуватись менеджерами паролів [Формулювання для S1 =2,3,4] Використовуйте складні паролі і не використовуйте одні і ті ж самі паролі для реєстрації на онлайн-ресурсах, в банківських системах тощо, зникайте користуватись менеджерами паролів.	x	x	x	x
2	[Формулювання для S1 =1] Не відправляйте фото та скани банківських карток та особистих документів своїх та батьків незнайомцям та сумнівним організаціям [Формулювання для S1 =2,3,4] Не відправляйте фото та скани ваших банківських карток та особистих документів незнайомцям та сумнівним організаціям	x	x	x	x
3	[Формулювання для S1 =1] Не відкривайте сумнівні листи у вашій електронній скриньці, месенджерах та ігрових акаунтах [Формулювання для S1 =2,3,4] Не відкривайте сумнівні листи у вашій електронній скриньці, месенджерах	x	x	x	x
4	Не відправляйте ваші контактні телефони, особисті фото незнайомцям, особливо тим, які просять оголені фотографії	x			
5	Не встановлюйте на ваші гаджети додатки та програми з неофіційних магазинів	x	x	x	x
6	Не підключайтеся до загальнодоступних, невідомих або незахищених мереж Wi-Fi	x	x	x	x
7	У разі вимагання паролів, даних, фото незнайомцями або отримання сумнівних повідомлень, негайно повідомте батьків	x			
8	Регулярно оновлюйте ваші пристрої. За можливості, увімкніть автоматичне оновлення всіх програм		x	x	
9	Використовуйте ліцензійне та антивірусне програмне забезпечення, фаєрволи на комп'ютерах і телефонах, та регулярно оновлюйте його, коли отримуєте повідомлення про оновлення системи		x	x	
10	Завжди створюйте резервні копії важливих даних на окремому локальному пристрої чи хмарному сховищі		x	x	
11	За можливості, використовуйте двофакторну аутентифікацію		x	x	
12	Не залишайте ваш пристрій без нагляду, особливо коли він працює, у публічних місцях		x	x	x
13	За будь-якої підозри зараження свого пристрою або компрометації даних НЕГАЙНО повідомте відповідні органи: Урядова команда реагування на комп'ютерні надзвичайні події України, Національний координаційний центр з кібербезпеки РНБОУ, Кіберполіція України		x	x	
14	Не панікуйте у разі телефонного дзвінка чи повідомлення у месенджери від підозрілих людей та організацій, які вимагають у вас гроші, аби врятувати вашу родину, тварину чи близьку людину. Негайно повідомте відповідні органи чи своїх близьких у разі такого дзвінка				x
15	За будь-якої підозри зараження свого пристрою або компрометації даних НЕГАЙНО повідомте відповідні органи: Кіберполіція України тел. 0 800 505 170 та своїм дітям та близьким				x

A6. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? Дайте оцінку за шкалою від 1 до 10, де 1 означає «дуже небезпечна», а 10 — «повністю безпечна».

1	2	3	4	5	6	7	8	9	10	BB=99
---	---	---	---	---	---	---	---	---	----	-------

A7. Чи бачили ви за останній рік матеріали, публікації, відео про правила безпечної поведінки в інтернеті?

1. Так

2. Ні

99. BB (не зачитувати)

A8. [для A7=1] Хто саме поширював ці матеріали? А хто ще?

Запишіть усе, що скаже респондент. Перепитайте.

- Записати _____

Записати _____

Записати _____

Записати _____

99. BB (не зачитувати)

A9. Яким чином змінилася ваша поведінка в інтернеті за останній рік?

Зачитайте, одна відповідь

1. Стала набагато більш небезпечною

2. Стала більш небезпечною

3. Не змінилася

4. Стала більш безпечною

5. Стала набагато більш безпечною

99. BB (не зачитувати)

ДЕМОГРАФІЯ

D1. Назвіть, будь ласка, свій основний рід занять.

Зачитайте, одна відповідь

1. Працюю за наймом

2. Зареєстрований приватний підприємець

3. Самозайнятий

4. Студент / учень

5. Веду домашнє господарство

6. Пенсіонер

7. Тимчасово не працюю, але шукаю роботу

98. Інше (запишіть)

D2. [Якщо D1= 1] Де саме ви навчаєтесь?

Одна відповідь

1. У школі

2. В професійно-технічному навчальному закладі

3. В коледжі

4. В вищому навчальному закладі

98. Інше (запишіть)

D3. Який ваш рівень освіти?

Зачитайте, одна відповідь

1. Немає початкової освіти

2. Початкова середня освіта (уточніть за необхідності: закінчили 4 класи загальноосвітньої школи)

3. Базова загальна середня (уточніть за необхідності: закінчили 9 класів загальноосвітньої школи)

4. Повна загальна середня (уточніть за необхідності: закінчили 12 класів загальноосвітньої школи)

5. Спеціальна середня освіта (уточніть за необхідності: закінчили професійно-технічний навчальний заклад, коледж)

5. Неповна вища/початкова вища (уточніть за необхідності: закінчили 1-3 курс вищого навчального закладу)

6. Вища освіта, бакалаврат

7. Вища освіта, магістратура (спеціаліст)

99. BB (не зачитувати!)

D4. Що б ви могли сказати про фінансове становище вашої сім'ї?

Зачитайте, одна відповідь

1. Змушені економити на харчуванні

2. Вистачає на харчування. Для придбання одягу, взуття необхідно заощадити або позичити

3. Вистачає на харчування та необхідний одяг, взуття. Для таких покупок, як гарний костюм, мобільний телефон, пілосос, необхідно заощадити або позичити

4. Вистачає на харчування, одяг, взуття, інші покупки. Але для придбання речей, які дорого коштують (таких як телевізор, холодильник), необхідно заощадити або позичити

5. Вистачає на харчування, одяг, взуття, дорогі покупки. Для таких покупок, як машина, квартира, необхідно заощадити або позичити

5. Будь-які необхідні покупки можу зробити в будь-який час

99. BB (не зачитувати!)

Це всі питання.

Подякуйте респондентові за участь в опитуванні!

Додаток 2. Портрет респондента

[illegible]

[illegible]

[illegible]

		Загалом			Вік респондента					
					26-59 років			Більше 60 років		
		Endline (2024)	Midterm (2023)	Baseline (2021)	Endline (2024)	Midterm (2023)	Baseline (2021)	Endline (2024)	Midterm (2023)	Baseline (2021)
Основний рід занять	Працюю за наймом	34,13%	26,30%	37,04%	48,57%	45,34%	51,68%	10,73%	16,54%	16,07%
	Зареєстрований приватний підприємець	8,40%	4,84%	6,81%	10,96%	9,19%	8,97%	3,41%	0,69%	3,50%
	Самозайнятий	5,23%	3,94%	4,82%	7,83%	6,68%	6,17%	1,01%	0,25%	2,54%
	Студент/учень	10,57%	27,89%	14,68%	0,17%	0,88%	0,23%	0,00%	0,00%	0,00%
	Веду домашнє господарство	6,07%	5,81%	9,25%	8,69%	14,55%	13,03%	3,22%	1,31%	1,97%
	Пенсіонер	24,19%	18,20%	18,73%	6,38%	5,57%	8,06%	79,20%	78,96%	74,96%
	Тимчасово не працюю, але шукаю роботу	7,25%	7,27%	7,82%	11,20%	10,76%	10,71%	1,59%	0,52%	0,96%
	Інше	4,16%	5,74%	0,30%	6,21%	7,04%	0,41%	0,83%	1,73%	0,00%
	Важко сказати	0,00%	0,00%	0,56%	0,00%	0,00%	0,73%	0,00%	0,00%	0,00%
	Загалом	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
Місце навчання	У школі	58,62%	64,27%	67,96%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
	В професійно-технічному навчальному закладі	5,11%	4,22%	4,27%	0,00%	30,98%	0,00%	0,00%	0,00%	0,00%
	В коледжі	5,33%	9,18%	7,69%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
	В вищому навчальному закладі	29,08%	21,84%	20,08%	100,00%	69,02%	100,00%	0,00%	0,00%	0,00%
	Інше	1,85%	0,50%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
	Загалом	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	0,00%	0,00%	0,00%

[illegible]

[illegible]

