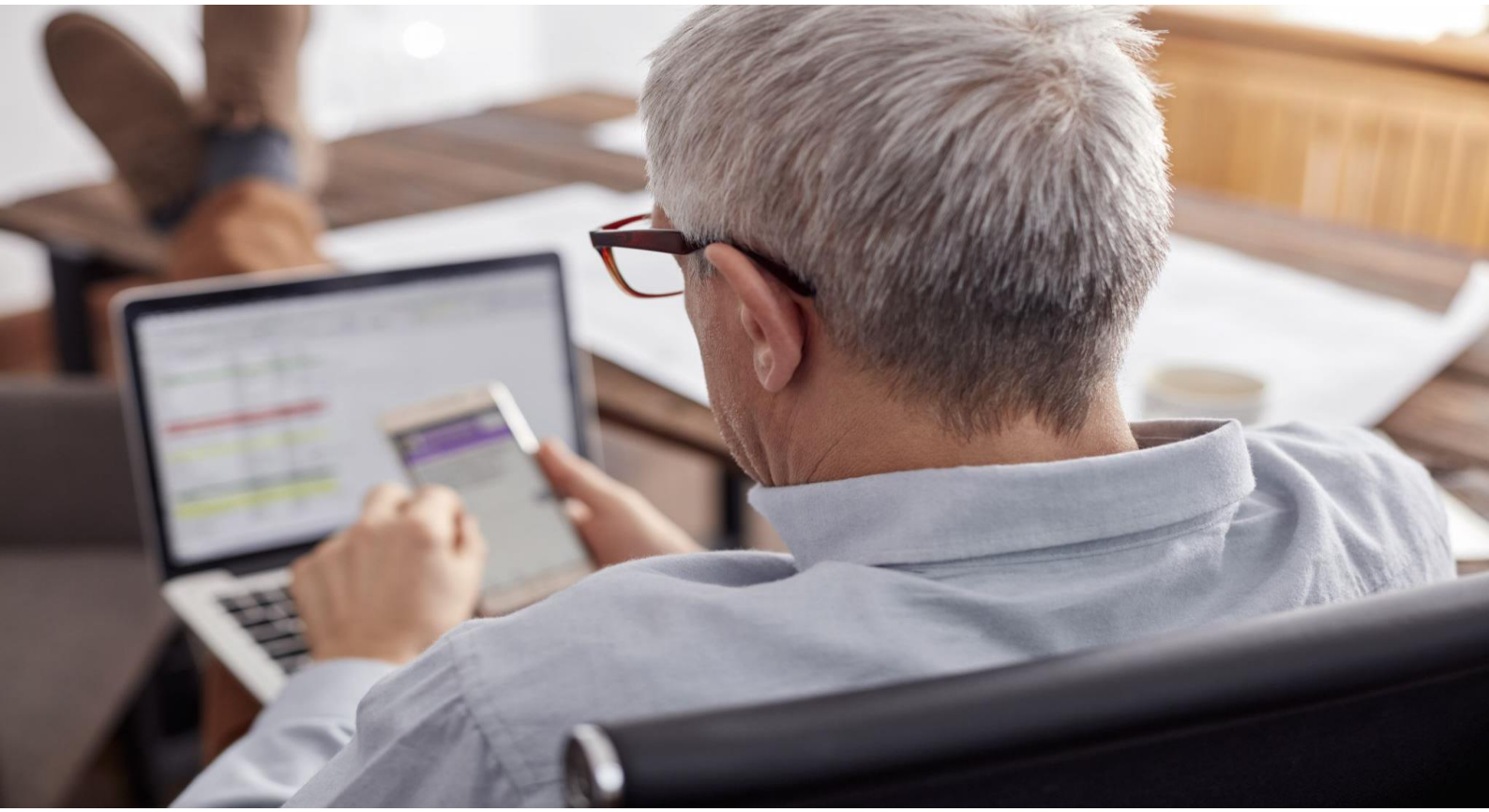
Звіт про базове дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки



Підготовлено для CRDF Global

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

Жовтень 2021

Зміст

Перелік діаграм 3
Перелік таблиць 4
I Ключові результати 5
II Висновки 8
III Мета дослідження і методологія 10
IV Результати дослідження 12
Поведінка в інтернеті 12
Обізнаність з поняттями «кібербезпека» та «правила кібергігієни» 21
Ризикована поведінка 23
Досвід зіткнення із кіберзагрозами 27
Обізнаність із правилами кібербезпеки 37
Безпека поведінки в інтернеті 42
Джерела інформації про правила безпечної поведінки в інтернеті 46
V Додаток 1. Міста 50+, де проводилося опитування 48
VI Додаток 2. Опитувальник 49
VII Додаток 3. Портрет респондента 61

Перелік діаграм

Діаграма 1. Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами? (% відповідей, всі респонденти) 12
Діаграма 2. Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами? Розподіл за цільовими групами (% відповідей, всі респонденти) 13
Діаграма 3. З яких пристроїв ви заходите в інтернет? (% відповідей, всі респонденти) 13
Діаграма 4. З якого пристрою ви заходите в інтернет найчастіше? (% відповідей, всі респонденти) 14
Діаграма 5. З яких пристроїв ви заходите в інтернет? Розподіл за цільовими групами (% відповідей, всі респонденти) 14
Діаграма 6. З якого пристрою ви заходите в інтернет найчастіше? Розподіл за цільовими групами (% відповідей, всі респонденти) 15
Діаграма 7. Уточніть, будь ласка, цей комп'ютер/ноутбук належить вам особисто? (% відповідей, респонденти, які частіше заходять в інтернет з комп'ютера/ноутбука) 16
Діаграма 8. Уточніть, будь ласка, цей комп'ютер/ноутбук належить вам особисто? Розподіл за цільовими групами (% відповідей, респонденти, які частіше заходять в інтернет з комп'ютера/ноутбука) 16
Діаграма 9. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, всі респонденти) 17
Діаграма 10. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, цільова група підлітки 11-17 років) 18
Діаграма 11. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, цільова група молодь 18-25 років) 18
Діаграма 12. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, цільова група дорослі 26-59 років) 19
Діаграма 13. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, цільова група люди старшого віку понад 60 років) 19
Діаграма 14. Коли ви завантажуєте матеріали, програми, ігри, як ви перевіряєте, що ресурс надійний? (% відповідей, респонденти, які завантажують матеріали, програми тощо) 20
Діаграма 15. Коли ви завантажуєте матеріали, програми, ігри, як ви перевіряєте, що ресурс надійний? За цільовими групами (% відповідей, респонденти, які завантажують матеріали, програми тощо) 21
Діаграма 16. Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека» та «правила кібергігієни»? (% відповідей, всі респонденти) 22
Діаграма 17. Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека» та «правила кібергігієни»? За цільовими групами (% відповідей, всі респонденти) 22
Діаграма 18. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, всі респонденти) 23
Діаграма 19. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, цільова група підлітки 11-17 років) 24
Діаграма 20. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, цільова група молодь 18-25 років) 25
Діаграма 21. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, цільова група дорослі 26-59 років) 25
Діаграма 22. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, цільова група люди старшого віку понад 60 років) 26
Діаграма 23. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, всі респонденти) 28
Діаграма 24. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, цільова група підлітки 11-17 років) 28
Діаграма 25. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, цільова група молодь 18-25 років) 29
Діаграма 26. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, цільова група дорослі 26-59 років) 30
Діаграма 27. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, цільова група люди старшого віку понад 60 років) 30
Діаграма 28. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто) 31

Діаграма 29. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто, цільова група підлітки 11-17 років) 32
Діаграма 30. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто, цільова група молодь 18-25 років) 32
Діаграма 31. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто, цільова група дорослі 26-59 років) 33
Діаграма 32. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто, цільова група люди старшого віку понад 60 років) 33
Діаграма 33. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами) 34
Діаграма 34. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами, цільова група підлітки 11-17 років) 35
Діаграма 35. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами, цільова група молодь 18-25 років) 35
Діаграма 36. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами, цільова група дорослі 26-59 років) 36
Діаграма 37. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами, цільова група люди старшого віку понад 60 років) 36
Діаграма 38. Наскільки ви готові вживати правила кібергігієни, щоб вберегтися від цих загроз? (% відповідей, респонденти, які почуваються не повністю захищеними щодо кіберзагроз) 37
Діаграма 39. Наскільки ви готові вживати правила кібергігієни, щоб вберегтися від цих загроз? За цільовими групами (% відповідей, респонденти, які почуваються не повністю захищеними щодо кіберзагроз) 38
Діаграма 40. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти) 38
Діаграма 41. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти, цільова група підлітки 11-17 років) 39
Діаграма 42. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти, цільова група молодь 18-25 років) 40
Діаграма 43. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти, цільова група дорослі 26-59 років) 40
Діаграма 44. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти, цільова група люди старшого віку понад 60 років) 41
Діаграма 45. Знання і виконання правил кібербезпеки, загалом 42
Діаграма 46. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? (% відповідей, всі респонденти) 42
Діаграма 47. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? За цільовими групами (% відповідей, всі респонденти) 43
Діаграма 48. Знання і виконання правил кібербезпеки у розбивці за рівнем самооцінки безпеки поведінки в інтернеті 44
Діаграма 49. Які джерела інформації ви використовуєте, щоб дізнатися про правила безпечної поведінки в інтернеті? Якому з цих джерел інформації ви довіряєте найбільше? (% відповідей, всі респонденти) 46
Діаграма 50. Які джерела інформації ви використовуєте, щоб дізнатися про правила безпечної поведінки в інтернеті? За цільовими групами (% відповідей, всі респонденти) 47
Діаграма 51. Якому з цих джерел інформації ви довіряєте найбільше? За цільовими групами (% відповідей, всі респонденти) 47

Перелік таблиць

Таблиця 1. Реальна поведінка щодо паролів серед тих, хто декларує використання відповідного правила 44
Таблиця 2. Реальна поведінка щодо використання двофакторної автентифікації серед тих, хто декларує використання відповідного правила 45
Таблиця 3. Реальна поведінка щодо використання резервного копіюванням серед тих, хто декларує використання відповідного правила 45

I Ключові результати

Активності в інтернеті

Для всіх вікових аудиторій найбільш поширена щоденна активність в Інтернеті – це користування месенджерами (Вайбер, Телеграм, Вотсап, Фейсбук), на другому місці для всіх вікових груп – пасивне користування соціальними мережами (відвідування, читання).

Активності другого порядку:

- Підлітків це ігри, завантаження контенту та дописи в соціальні мережі
- Для решти респондентів – електронна пошта, інтернет банкінг

Завантаження контенту спадає із віком: лише 4% підлітків не роблять цього ніколи, тоді як серед найстарших респондентів цей відсоток становить 58%. Утім, саме підлітки частіше завантажують контент із офіційних ресурсів (або таких, у надійності яких вони впевнені), решта респондентів частіше ніяк не перевіряє надійність ресурсів.

Підлітки також активніше інших груп використовують публічні вай-фай мережі.

Обізнаність з поняттями «кібербезпека» та «кібергігієна»

Поняття «кібербезпека» вважається більш знайомим для усіх вікових груп: частка відповідей «вперше чую» варіює від 7% до 12%, а відносна більшість схиляється до відповіді «Маю загальне поняття, без подробиць» (від 42% до 51%). Поняття «кібергігієна» меншою мірою знайоме респондентам: частка відповідей «вперше чую» більше майже у 4 рази: від 29% для підлітків до 32%-39% для решти вікових груп.

Ризикована поведінка в інтернеті

Серед варіантів небезпечної поведінки, яку демонструють респонденти, на першому місці для всіх вікових груп – відсутність звички робити резервні копії даних. На другому місці – відсутність звички вмикати двофакторну автентифікацію. Найбільш сумлінна в цих питаннях вікова група 18-25 років, а найбільш легковажна – 60+ років.

Думка про те, що «звичайна людина» не дуже цікава для інтернет-шахраїв також доволі широко поширена – її розділяє кожен другий респондент старше 18 років і приблизно троє із чотирьох підлітків.

В питаннях паролів респонденти також поводяться досить легковажно: значна частина респондентів (близько 40% у середньому) зізнається, що використовує один пароль на всі випадки, а також у тому, що цей пароль досить простий. Найбільш відповідальну поведінку демонструє група молоді 18-25 років, у цій віковій групі така поведінка трапляється рідше, ніж у інших.

Окремим видом ризикованої поведінки є дії у російському сегменті інтернету. Такі дії не є дуже поширеними, особливо у порівнянні з іншими видами ризикованої поведінки. Українці практикують (у порядку спадання частоти): відвідування російських сайтів (29%); відвідування заблокованих в Україні російських ресурсів та соціальних мереж (16%);

завантажування з російських сайтів файлів, заповнення анкет, реєстрація тощо (13%); користування російськими поштовими скриньками (10%).

З точки зору дій у російському сегменті найбільш уразливою групою є молодь 18-25 років: такі користувачі найчастіше відвідують російські сайти (40%) і заблоковані в Україні ресурси (29%), завантажують з російських ресурсів файли, програми, проходять реєстрацію (25%), мають поштові скриньки на російських серверах (17%). На другому місці за розповсюдженістю такої поведінки – підлітки 11-17 років. Найстарша вікова група вдається до подібних дій найменше, утім, є підозра, що респонденти цього віку (понад 60 років) можуть не усвідомлювати, у якому сегменті інтернету вони перебувають.

Досвід кіберзагроз

Загалом по вибірці хоча б з одним із видів кібершахрайства стикалися 41% користувачів. Найбільша частка припадає на групу віком 25-59 років, тут особистий досвід має майже кожен другий (47%). Серед молоді 18-25 років ця частка становить 37%, а серед літніх людей старше 60 років – 43%. Підліткам пощастило найбільше – лише 7% стикалися із випадками кібершахрайства особисто. Більш обережну поведінку молоді (18-25 років) у питаннях паролів, звички робити резервні копії та використовувати двофакторну автентифікацію можна пояснити тим, що саме представники цієї групи частіше стикаються із зламом паролів: наприклад 60% респондентів цієї групи стикалися із зламом аккаунта у соціальних мережах у найближчому колі знайомих, при цьому половина з них – стикалася особисто. Для решти вікових груп цей показник у півтора-два рази нижче.

Для людей віком від 26 років на першому місці серед кіберзагроз - вимагання банківських даних, паролів та доступу до облікових записів банківських мобільних додатків, банківських рахунків (у т.ч. через телефон, месенджери). Така ситуація особисто або у колі найближчих знайомих траплялася з 44% людей середнього віку (26-59 років) та 37% людей найстаршого віку (понад 60 років), частка тих, хто стикався особисто майже однакова і становить 23-24%. Відносно більша частка літніх людей (28% респондентів у віці 60+) особисто стикалася із ситуацією, коли кібер шахраї вимагають гроші, використовуючи методи соціальної інженерії (маніпуляції, погрози, шантаж), а також особисті та родинні дані (через телефон та месенджери), а у колі знайомих така ситуація виникала у 42% респондентів.

Почуття захищеності у інтернеті

Частка людей, які почуваються беззахисними або не завжди почуваюся захищеними, варіює від 49% до 75% у залежності від вікової групи та ситуації. Найбільше користувачів непокоїть ситуація зламу паролів та облікових записів у соціальних мережах: 75% респондентів віком 26-59 років не почуваються повністю захищеними проти цієї кіберзагрози. Щодо усіх типів загроз підлітки і молодь до 25 років почуваються більш захищеними порівняно до найстарших респондентів.

Одночасно підлітки вважають свою поведінку в інтернеті більш безпечною за інші вікові групи: 37% вважають поведінку повністю безпечною (у вікових групах 18-25, 26-59 та 60+ років цей показник становить 29%, 25% та 23% відповідно).

Серед користувачів старше 25 років кожен третій вважає, що поводиться в інтернеті небезпечно.

Правила кібербезпеки

Щодо основних правил кібербезпеки, найбільша частка респондентів (97%) знає про те, що не можна відправляти фото та скани банківських карток та особистих документів (цей показник стабільний і не варіює з віком). Дотримуються цього правила від 83% до 90% респондентів, у залежності від віку. Також респонденти добре знають, що не можна залишати пристрій без нагляду (81-87% знають і дотримуються цього правила). Менша частка респондентів свідома того, що не можна відкривати сумнівні листи: 57-58% респондентів до 25 років дотримуються цього правила; серед груп віком 26-59 та понад 60 років ця частка трохи вища – 65% та 64% відповідно. Регулярне оновлення пристроїв у середньому практикують трохи більше половини респондентів. Використання складних і різних паролів у середньому практикують трохи менше половини (частка респондентів, які дотримуються цього правила, трохи більша у групі 18-25 років і складає 64%; для решти вікових груп цього правила дотримуються лише 45-48%).

Створення резервних копій важливих даних та обов'язкове використання двофакторної аутентифікації декларують 30% та 28% респондентів відповідно, цих двох правил дотримуються рідше за інші. Молодь 18-25 років декларує дотримання цих правил частіше за вікову групу 25-59 років (для інших вікових груп правило не пропонувалося). .

Загалом, підлітки 11-17 років є найбільш обізнаною групою щодо правил кібербезпеки: 83% знають усі правила. Утім, лише 50% підлітків виконують усі правила хоча б інколи, а постійно виконують усі правила лише 22%. Утім, показники виконання правил у групі підлітків найбільші серед решти цільових груп: серед молоді 18-25 років хоча б інколи виконують правила 21%, серед дорослих 25-59 років – 12%, а серед найстарших респондентів понад 60 років – 22%.

Найстарша група респондентів є найменш обізнаною: лише 37% знають про усі правила кібербезпеки для цієї групи. Але також ці респонденти є найбільш свідомими: якщо старша людина знає правило, вона з більшою ймовірністю буде його дотримуватися.

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. Ця кореляція прослідковується для всіх вікових груп. Користувачі, які оцінюють свою поведінку як небезпечну, або не знають правил, або знають, але нехтують ними.

Утім, декларування виконання правил кібербезпеки не означає справжнього виконання цих правил. Ми проаналізували відповіді респондентів, які заявили, що виконують певне правило, і подивилися, наскільки їм притаманна ризикована поведінка, пов'язана із невиконанням цього правила. Виявилося, що серед тих, хто задекларував виконання правила щодо паролів, лише приблизно ¾ дійсно поводяться таким чином; лише половина з тих, хто декларує виконання правила щодо двофакторної автентифікації, дійсно її вживають роблять, а кожен п'ятий – не вживає взагалі; серед тих, хто знає і, за їхніми словами, завжди дотримується правила щодо створення резервних копій, менше половини дійсно декларують таку поведінку, а кожен третій каже, що не робить цього.

Джерела інформації

Щодо джерел інформації про правила безпечної поведінки в інтернеті, перше і друге місце для всіх вікових груп посідають «сарафанне радіо» (друзі, родичі, знайомі, які знаються на цій темі) та . люди, яких респонденти вважають фахівцями (наприклад, системний адміністратор на роботі, в школі, в університеті). При цьому сарафанне радіо лідирує із великим відривом для наймолодшої (11-17 років) та найстаршої (60+ років) груп. Відповідно саме цим джерелам і довіряють найбільше.

Щодо решти джерел, вони варіюють з віком. Так, найстарша група майже не використовує інші джерела, окрім друзів і знайомих фахівців. Підлітки частіше звертаються до соціальних мереж; молодь (18-25 років) і доросла група (26-59 років) частіше використовує інтернет (крім соціальних мереж) та спеціалізовані джерела, сайти, форуми , а.Традиційні ЗМІ, зовнішня реклама, блогери – не вважається релевантними джерелами інформації про правила безпечної поведінки в інтернеті для всіх вікових груп.

II Висновки

Більша частина користувачів проводить у інтернеті частину дня щоденно, користуючись персональним пристроєм. Тож і відповідальність за власну безпеку користувачі несуть персонально.

Користування месенджерами і соціальними мережами є найбільш поширеними видами активностей у інтернеті, тож основні загрози спіткають користувачів саме тут. Утім, для поширення знань про кібербезпеку і основні правила кібергігієни також можна рекомендувати використовувати саме ці джерела.

Перший пріоритет для інформаційної кампанії – просування правил кібергігієни. Адже 62% користувачів або не чули про таке поняття, або чули, але не знають, що це. Лише кожен десятий впевнений у своїх знаннях настільки, що може пояснити іншим.

Така ситуація вдається загрозливою, адже серед джерел інформації про кібербезпеку переважають саме «друзі, знайомі та родичі», які можуть пояснити своїми словами, що і як роботи, аби вберегтися від загроз. А саме з цим джерелом спостерігається очевидний провал. Саме через це серед користувачів поширюються міфи, які підсилюють ризиковану поведінку.

Одним із найпоширеніших міфів є твердження «я не цікавий для інтернет шахраїв» - до цієї думки схиляються більше половини респондентів (найбільш вразлива група – підлітки 11-17 років, 72% яких погоджуються з цією думкою). Другий рівною мірою поширений міф – «якщо є антивірус, мені нічого не загрожує» (найбільш вразливі групи – підлітки 11-17 років та найстарші люди віком понад 60 років).

Озброєні цими ідеями, користувачі почуваються в інтернеті більш-менш впевнено (підлітки – найбільш впевнена група), щонайменше не вважають свою поведінку небезпечною приблизно

двоє із трьох. Але щодо зовнішніх загроз, які не залежать від власної поведінки, користувачі часто почуваються беззахисними.

Зокрема, найчастіше відсутність захисту користувачі відчувають у ситуаціях, коли зловмисники крадуть облікові записи у соціальних мережах (76%), кібершахраї вимагають у старших людей гроші, використовуючи методи соціальної інженерії (маніпуляції, погрози, шантаж), а також особисті та родинні дані (через телефон та месенджери) (74%). Показово, що саме ці кіберзагрози є одними із найпоширеніших: про злам аккаунтів у соціальних мережах принаймні чули 80% користувачів (а серед молоді 28-26 років кожен третій відчув це на собі), серед літніх людей про вимагання грошей знають 90% (28% - із власного досвіду).

Люди, які почуваються недостатньо захищеними, переважно (троє із чотирьох) декларують готовність додержуватися правил. Проблема у тому, що найбільш актуальні (і найменш інтуїтивно зрозумілі) правила знає мала кількість користувачів. Так, правило щодо недопустимості відправляти фото банківських карток та документів незнайомцям знають майже усі, і майже усі дотримуються. А от правила щодо використання двофакторної автентифікації або створення резервних копій важливих документів знають і хоча б інколи дотримуються лише 53% та 62% відповідно (утім, як показав аналіз, декларування наслідування правилу і реальне використання цього правила у побуті може відрізнятися удвічі).

Найменшу обізнаність користувачі демонструють щодо правила повідомляти відповідні органи за підозри зараження гаджета або компрометації даних: майже половина користувачів віком 18-59 років вперше про це чує. Літнім людям пропонується повідомляти Кіберполіції а також дітей та близьких – за рахунок останніх знання цього правила трохи вище. Утім, як ми пам’ятаємо, серед дітей та близьких рівень обізнаності щодо правил кібергігієни загалом становить близько 10%.

Зважаючи на те, що українці усе частіше стикаються із кіберзагрозами на власному досвіді (41%) питання освітньої інформаційної кампанії набуває усе більшої актуальності. Адже саме знання і використання правил кібергігієни є чинником безпечної поведінки в інтернеті, і користувачі це усвідомлюють.

Така кампанія може бути спрямована як на поширення інформації про те, де можна отримати підтримку у критичній ситуації (Кіберполіція, інші відповідні органи), так і на поширення спеціальних знань у доступному форматі. Також важливим є пояснення, чому треба вдавалися до тих чи інших дій, які не завжди зрозумілі пересічному користувачу, але вимагають від нього певних зусиль (двофакторна автентифікація, складні паролі, резервні копії тощо). Правила, які інтуїтивно зрозумілі на побутовому рівні (повідомте про кіберінцидент батькам або дорослим дітям, не панікуйте, тощо, рівень знання яких і так досить великий), можна не пояснювати докладно, але забезпечити рівень підтримки.

Кампанія може мати подовжений ефект за рахунок так званого «сарафанного радіо» — до людей, які набули знань завдяки кампанії, зможуть звертатися за порадою їхні родичі і знайомі.

III Мета дослідження і методологія

Визнаючи ризики, пов'язані із все більшою цифровізацією світу, CRDF Global у 2019 році розпочала програму покращення кібербезпеки в Україні, Молдові та Західних Балканах. Програма присвячена запобіганню кібератакам шляхом створення міцної кіберінфраструктури та зміцнення кібербезпеки. Ця програма підтримується Офісом Державного департаменту США Координатора допомоги США Європі та Євразії.

Проект кампанії "Інформація про кібербезпеку" є частиною програми кібербезпеки CRDF Global, і основна мета проекту - покращити обізнаність щодо загроз кібербезпеки серед широкої громадськості України.

З огляду на відсутність даних про рівень обізнаності громадськості про щодо загроз кібербезпеки, було прийнято рішення провести базове дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки і правила кібергігієни.

Опитування має на мені оцінити:

- рівень поінформованості цільових аудиторій про кіберзагрози кібербезпеки;
- рівень обізнаності про основні правила кібергігієни та їх використання у повсякденному житті;
- особистий досвід користувачів за останні місяці щодо кібер-хакерів, кіберзлочинів, кібератак, кіберзагроз;
- джерела інформації про кібербезпеку, кібератаки, кібергігієну;

Цільова аудиторія 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.

Метод проведення дослідження – кількісне опитування за структурованим опитувальником.

Географія дослідження: вся Україна, включно із селами, за винятком АР Крим та окремих районів Донецької та Луганської області, які тимчасово не контролюються українською владою. Опитування проводилося в усіх областях України, зокрема, 296 респондентів опитано в містах із чисельністю населення понад 500 тисяч; 287 респондентів – у містах із чисельністю населення понад 50 тисяч (перелік міст наведено у Додатку 1); 245 респондентів – у менших містах і селищах міського типу, і 372 респондентів опитано у селах.

Загальна кількість респондентів: 1200.

Кількість респондентів за цільовими групами:

- Підлітки 11-17 років: 300 респондентів;

- Молодь 18-25 років: 300 респондентів;
- Дорослі 26-59 років: 450 респондентів;
- Люди старшого віку від 60 років: 150 респондентів.

Попередньо було заплановано провести рівну кількість інтерв'ю з усіма цільовими групами (по 300 інтерв'ю). Утім, в ході опитування дослідники стикнулися із дуже низьким проникненням інтернету у найстаршій цільовій групи (люди віком понад 60 років). За даними Омнібусу компанії Info Sapiens, рівень проникнення інтернету становить 99% серед аудиторії віком 11-25 років, 90% серед аудиторії 26-59 років та лише 38% серед аудиторії понад 60 років.

З огляду на низьке проникнення інтернету серед найстаршої вікової групи було прийнято рішення скоротити цільову кількість інтерв'ю до 150 за рахунок збільшення цільової кількості інтерв'ю у групи 26-59 років до 450 інтерв'ю.

Метод опитування:

- для цільової групи «Підлітки» — особисте опитування на дому 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.

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

Максимальна статистична помилка вибірки становить:

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

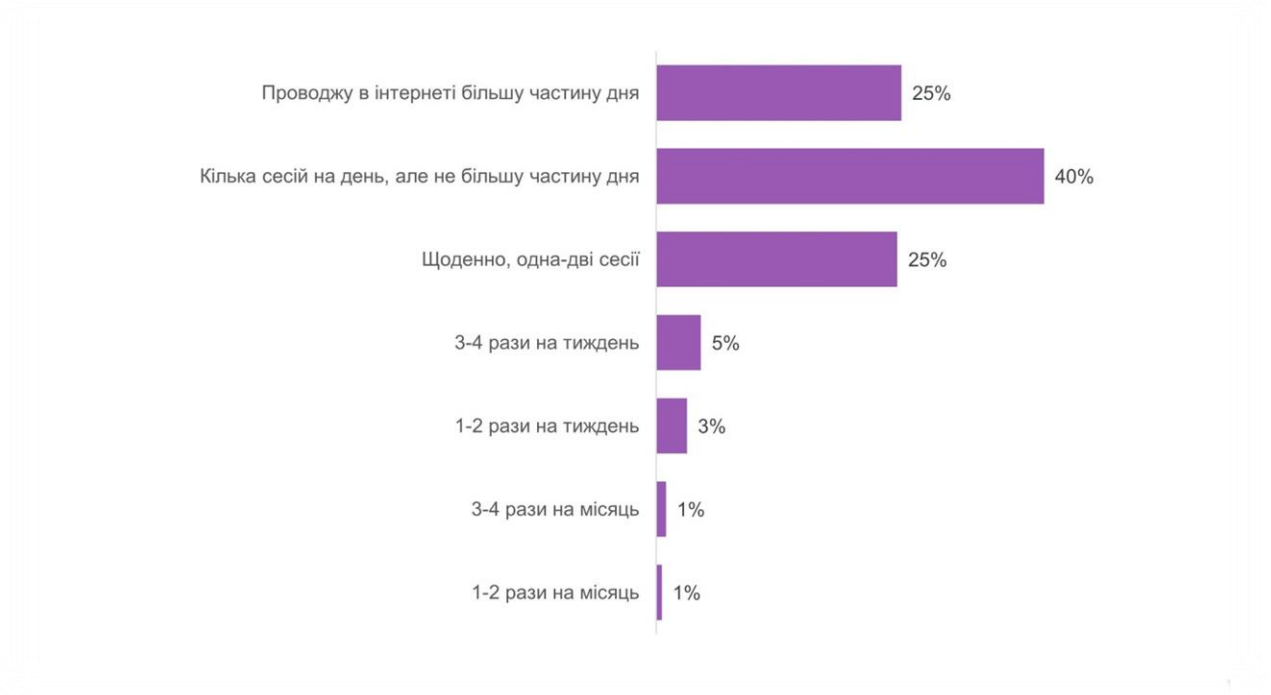
Опитування проводилося за структурованим опитувальником (див. Додаток 2). В опитувальнику, зокрема, використовуватися п'ятибальні та десятибальні шкали. З точки зору аналізу позитивною оцінкою вважається оцінка 4 або 5 за п'ятибальною шкалою, та 9 або 10 за десятибальною шкалою.

IV Результати дослідження

Поведінка в інтернеті

До участі в опитуванні запрошувалися люди, які користуються інтернетом щонайменше раз на місяць, утім більша частина опитаних (90%) користуються інтернетом щоденно. Чверть з респондентів проводять в інтернеті більшу частину дня (див. Діаграма 1).

Діаграма 1. Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами? (% відповідей, всі респонденти)



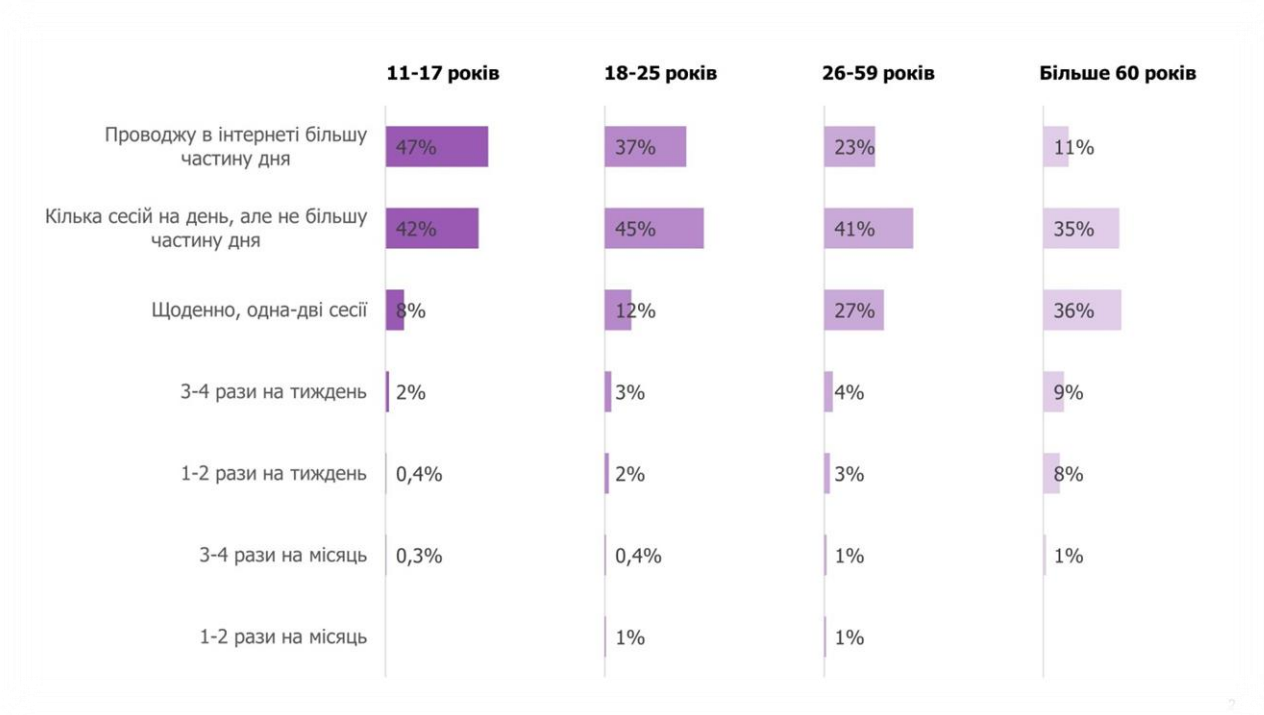
Частка людей, які проводять інтернеті більшу частину дня, спадає з віком респондентів. Так, серед наймолодшої групи підлітків 11-17 років таких респондентів майже половина (47%), серед молоді 18-25 років більшу частину дня в інтернеті проводять 37%, серед дорослих 25-59 років – майже кожен четвертий (23%), а серед літніх людей – лише 13%.

Утім, частота щоденного користування спадає з віком значно повільніше: частка людей, які заходять в інтернет щоденно суттєво нижча за загальний показник лише для літніх людей (82% респондентів віком від 60 років), а для решти вікових груп вона перевищує 90% (98%, 94% та 91% для підлітків, молоді та дорослої аудиторії відповідно).

Таким чином, люди із доступом в інтернет схильні користуватися інтернетом щоденно, але літні люди переважно обмежуються 1-2 сесіями зв'язку, тоді як молодь проводить в інтернеті більшу частину дня (див.

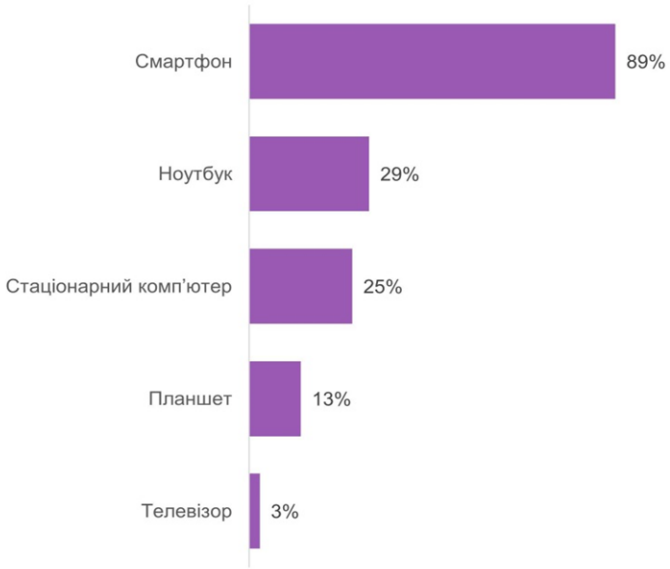
Діаграма ***2***).

Діаграма 2. Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами? Розподіл за цільовими групами (% відповідей, всі респонденти)

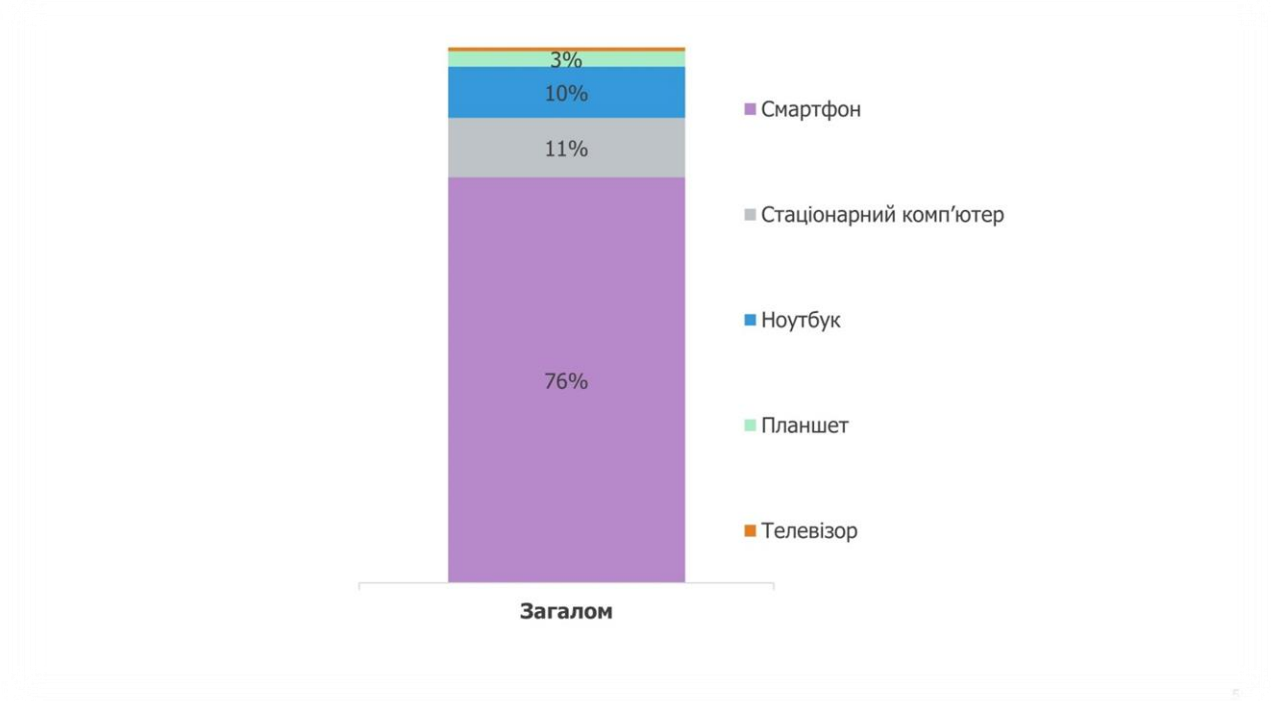


Серед пристроїв, з яких здійснюється вхід в інтернет, беззаперечним лідером є смартфон: загалом по аудиторії 89% респондентів користуються цим пристроєм і 76% вважають його основним пристроєм для виходу в інтернет (див. Діаграма 3, Діаграма 4).

Діаграма 3. З яких пристроїв ви заходите в інтернет? (% відповідей, всі респонденти)



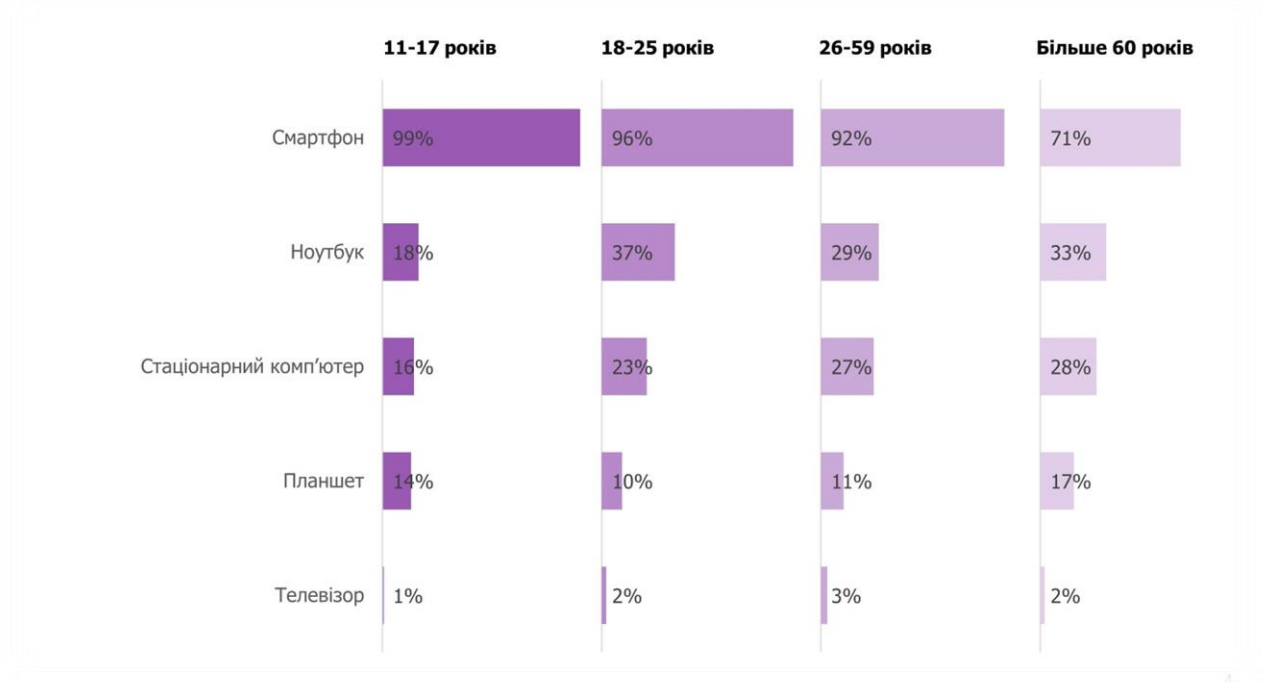
Діаграма 4. З якого пристрою ви заходите в інтернет найчастіше? (% відповідей, всі респонденти)



Частка користування смартфонами найвища серед підлітків (99%) і значно спадає для найстаршої аудиторії (71%). Для молоді і дорослих респондентів частка користувачів смартфонів складає 96% та 92% відповідно (див. Діаграма 5, Для респондентів усіх цільових груп смартфон є основним пристроєм для здійснення інтернет-зв'язку, хоча серед найстаршої аудиторії помітна частка респондентів найчастіше користуються ноутбуками (20%) та стаціонарними комп'ютерами (18%) (див. Діаграма 6).

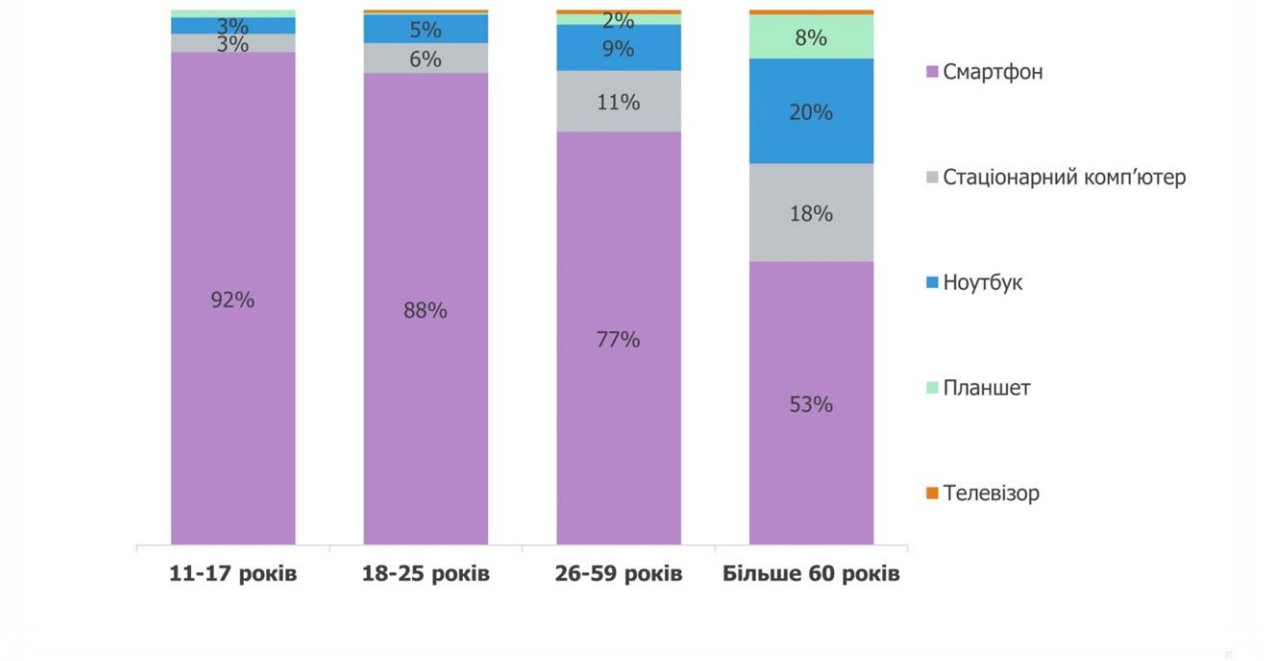
*Діаграма **6**)*

Діаграма 5. З яких пристроїв ви заходите в інтернет? Розподіл за цільовими групами (% відповідей, всі респонденти)



Для респондентів усіх цільових груп смартфон є основним пристроєм для здійснення інтернет-зв'язку, хоча серед найстаршої аудиторії помітна частка респондентів найчастіше користуються ноутбуками (20%) та стаціонарними комп'ютерами (18%) (див. Діаграма 6).

Діаграма 6. З якого пристрою ви заходите в інтернет найчастіше? Розподіл за цільовими групами (% відповідей, всі респонденти)



Якщо смартфон є беззаперечно особистим пристроєм, то ноутбуки та стаціонарні комп'ютери можуть перебувати у колективному користуванні. Ми запитали респондентів, які частіше за все заходять в інтернет з комп'ютера або ноутбука, чи належить їм цей пристрій особисто.

Більша частина аудиторії (55%) не ділить комп'ютер або ноутбук з родиною або колегами, утім кожен четвертий користується родинною технікою разом з іншими членами родини, а кожен п'ятий користується корпоративною технікою (див.

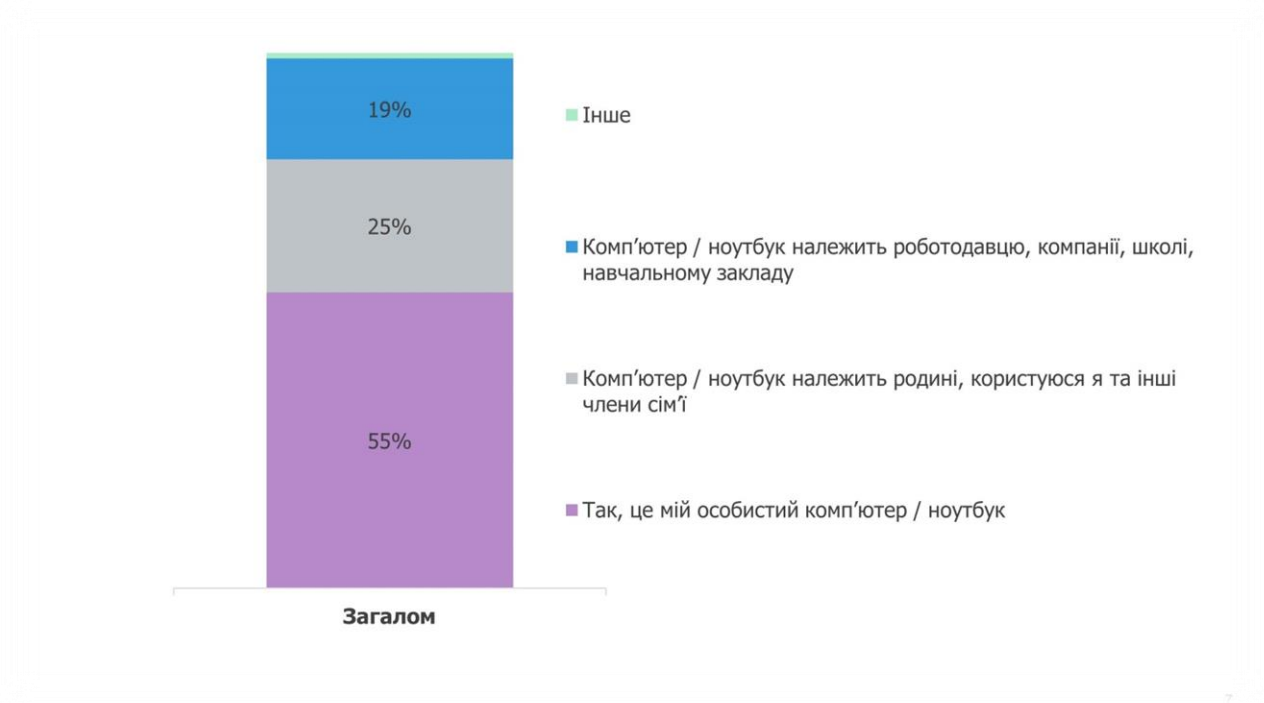
Діаграма **7**).

Частка респондентів, які користуються корпоративними пристроями, найбільша у групі респондентів 26-59 років (29%). Підлітки найчастіше не мають власного комп'ютера і вимушені ділити техніку із родиною (48% з тих, хто заходять в інтернет з комп'ютера або ноутбука, а таких лише 6% у загальній вибірці).

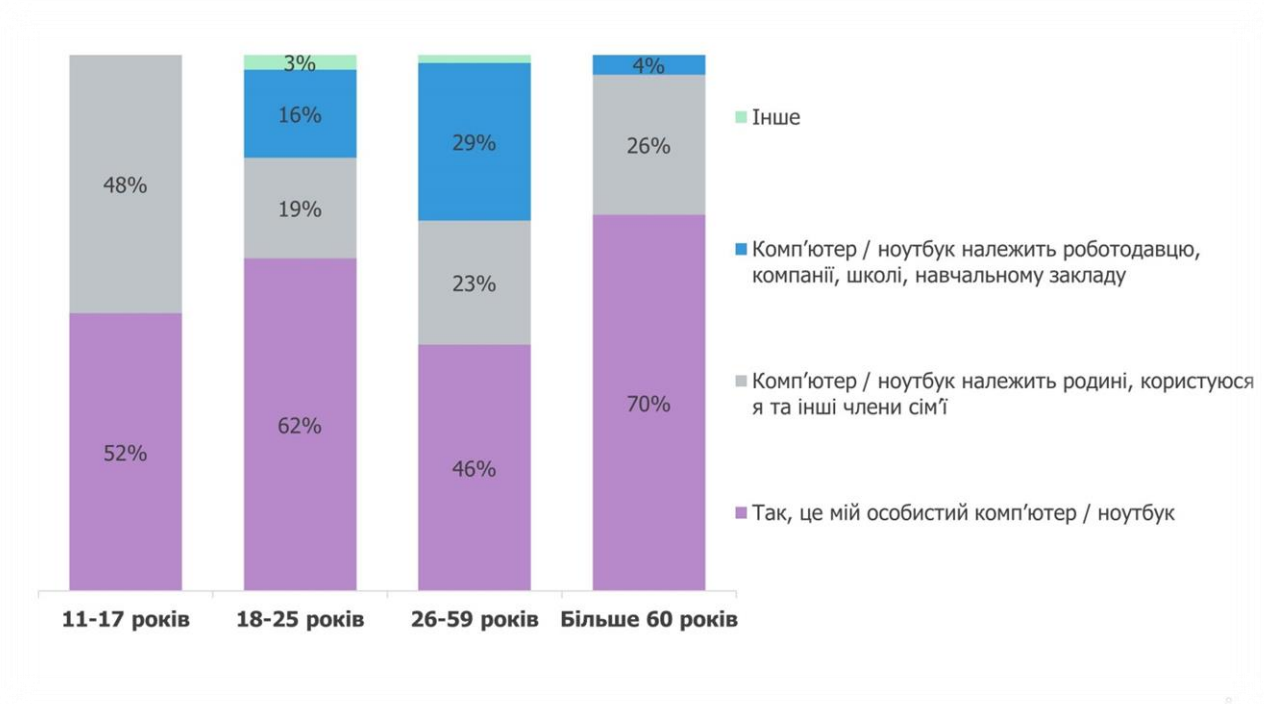
Літні люди, які найчастіше заходять в інтернет з комп'ютера або ноутбука (їх 38% у завальній вибірці), так само найчастіше мають власну техніку – 70% сказали, що користуються особистим пристроєм і лише 26% ділять техніку із іншими членами сім'ї (див. Діаграма 8).

Таким чином, здебільшого вихід в інтернет відбувається із особистого пристрою, якій перебуває в індивідуальному використанні.

Діаграма 7. Уточніть, будь ласка, цей комп'ютер/ноутбук належить вам особисто? (% відповідей, респонденти, які частіше заходять в інтернет з комп'ютера/ноутбука)



Діаграма 8. Уточніть, будь ласка, цей комп'ютер/ноутбук належить вам особисто? Розподіл за цільовими групами (% відповідей, респонденти, які частіше заходять в інтернет з комп'ютера/ноутбука)



Серед дій, які користувачі виконують в інтернеті, беззаперечне лідерство належить месенджерам (загалом 71% респондентів користуються ними щодня, і ще 14% - кілька разів на тиждень). На другому місці – користування соціальними мережами (61% щодня, 15% - кілька разів на тиждень). Замикає трійку лідерів електронна пошта – кожен четвертий респондент користується електронною скринькою щодня, ще 13% - кілька разів на тиждень (див. Діаграма 9).

Діаграма 9. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, всі респонденти)

Утім, якщо спілкування у месенджерах і гортання стрічки соціальних мереж є лідерами за частотою користування в усіх вікових групах, то частоти решти інтернет-активностей варіюють із віком.

Так, для підлітків на третьому місці за частотою знаходяться онлайн ігри: майже кожен третій (32%) грає щодня, і іще 27% - кілька разів на тиждень. Не грають в онлайн ігри загалом лише 15% респондентів наймолодшої групи.

Підлітки також є найактивнішою групую щодо розміщення контенту у соціальних мережах: майже половина роблять дописи або розміщують фотографії як мінімум кілька разів на тиждень, при чому 22% роблять це щодня.

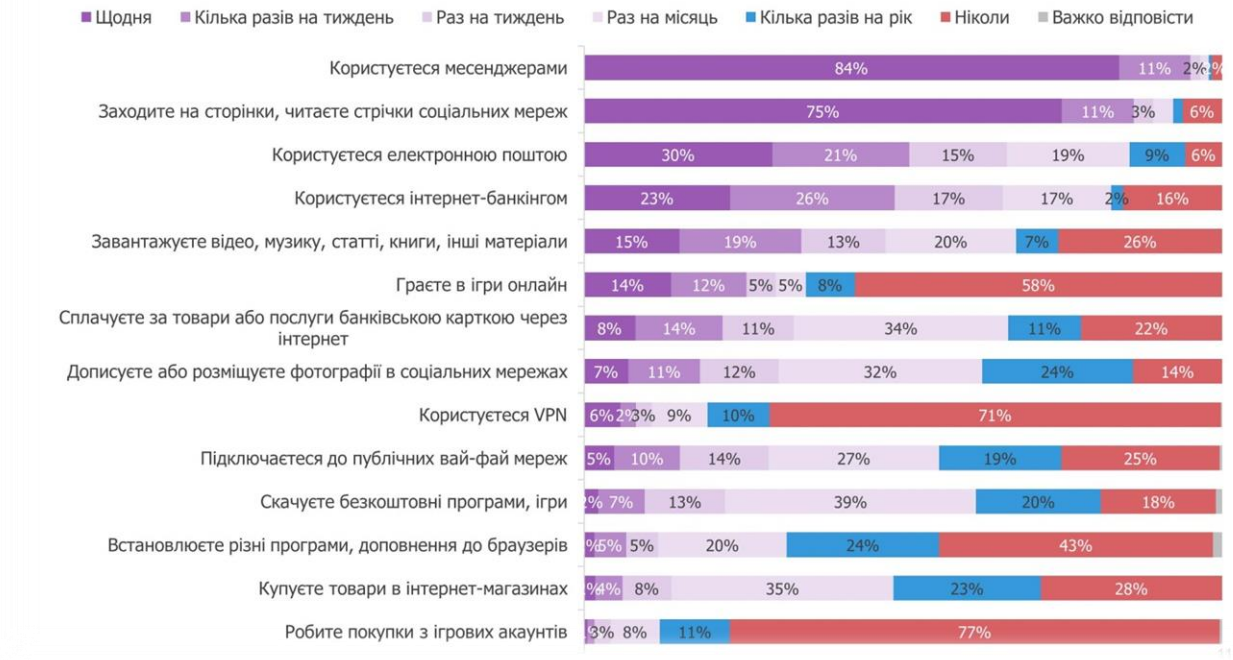
Також половина наймолодших респондентів принаймні кілька разів на тиждень завантажує матеріали (музику, відео тощо) з інтернету, і лише 4% не роблять це ніколи (див.

Діаграма ***10***).

Діаграма 10. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, цільова група підлітки 11-17 років)

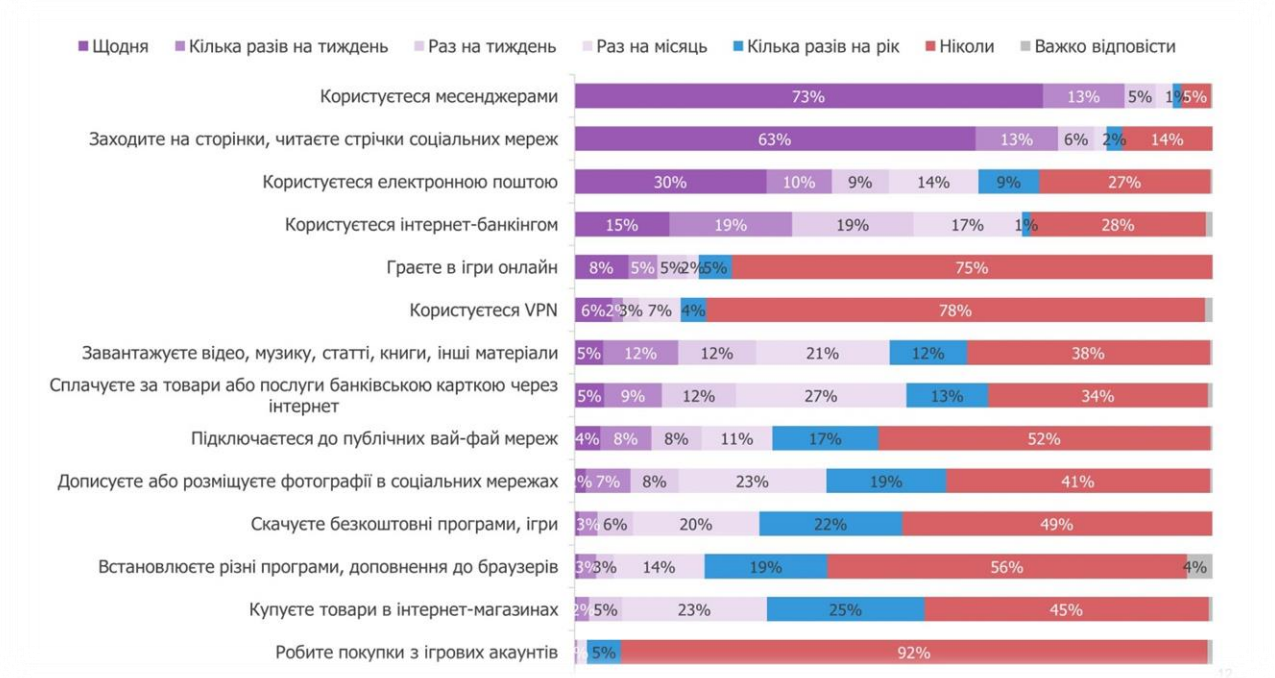
Для молоді 18-25 років третє та четверте місце за частотою посідають користування електронною поштою та інтернет банкінгом – приблизно половина опитаних звертаються до цих активностей щонайменше кілька разів на тиждень (див. Діаграма 11).

Діаграма 11. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, цільова група молодь 18-25 років)



Дорослі респонденти 25-59 років також часто користуються електронною поштою та інтернет-банкінгом, утім частота користування дещо менша, ніж у молоді (див. Діаграма 12)

Діаграма 12. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, цільова група дорослі 26-59 років)

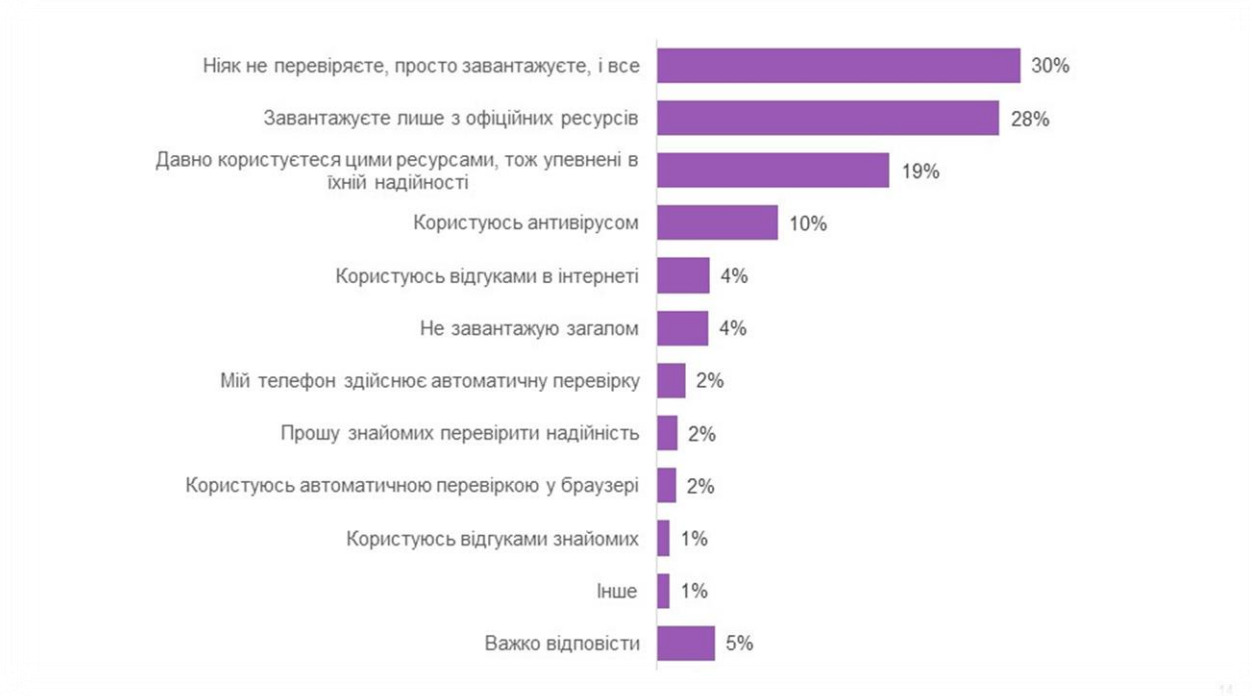


Найстарші респонденти рідше вдаються до усіх видів інтернет-активностей (див. Діаграма 13)

Діаграма 13. Чи виконуєте ви наступні дії в інтернеті і як часто? (% відповідей, цільова група люди старшого віку понад 60 років)

Таким чином, серед тих, хто завантажує матеріали, програми, ігри з інтернету, переважає молодь. Ми запитали таких респондентів, чи перевіряють вони надійність ресурсу. Загалом по вибірці майже рівні частки респондентів відповіли що або ніяк не перевіряють надійність, або впевнені у надійності, бо завантажують з офіційних ресурсів (30% та 28% відповідно). Ще 19% впевнені у надійності ресурсів через довгий досвід користування і 10% вважають, що антивірус попередить про небезпеку (див. Діаграма 14).

Діаграма 14. Коли ви завантажуєте матеріали, програми, ігри, як ви перевіряєте, що ресурс надійний? (% відповідей, респонденти, які завантажують матеріали, програми тощо)



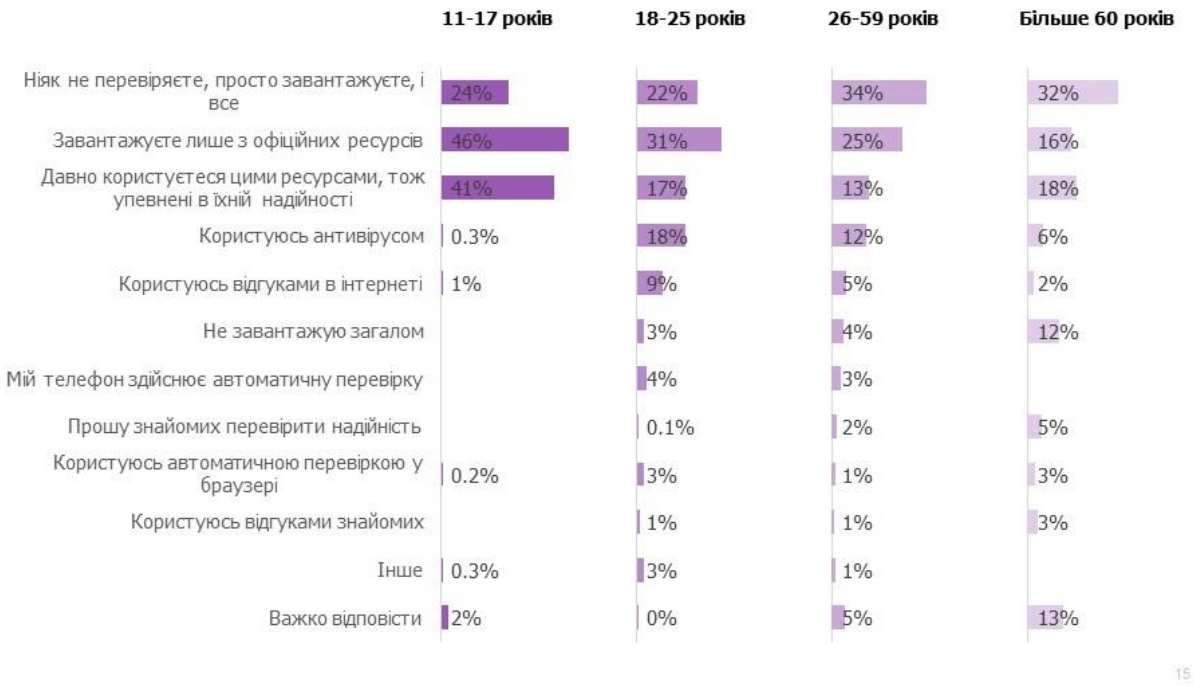
Утім, частки цих найчастіших відповідей значно варіюють за віковими групами. Так, підлітки майже не користуються антивірусами, утім найчастіше користуються офіційними ресурсами (46%). Молодь 18-25 років також досить часто звертається до офіційних ресурсів (31%), утім 22% ніяк не перевіряє надійність ресурсу, також значна частка покладається на антивірус (18%).

Серед людей середнього (26-59 років) та старшого (понад 60 років) віку частка тих, хто ніяк не перевіряє надійність ресурсу, зростає до 34% та 32% відповідно.

Серед літніх респондентів частка тих, хто користується офіційними ресурсами, найнижча, і складає лише 16% (див.

Діаграма ***15***).

Діаграма 15. Коли ви завантажуєте матеріали, програми, ігри, як ви перевіряєте, що ресурс надійний? За цільовими групами (% відповідей, респонденти, які завантажують матеріали, програми тощо)



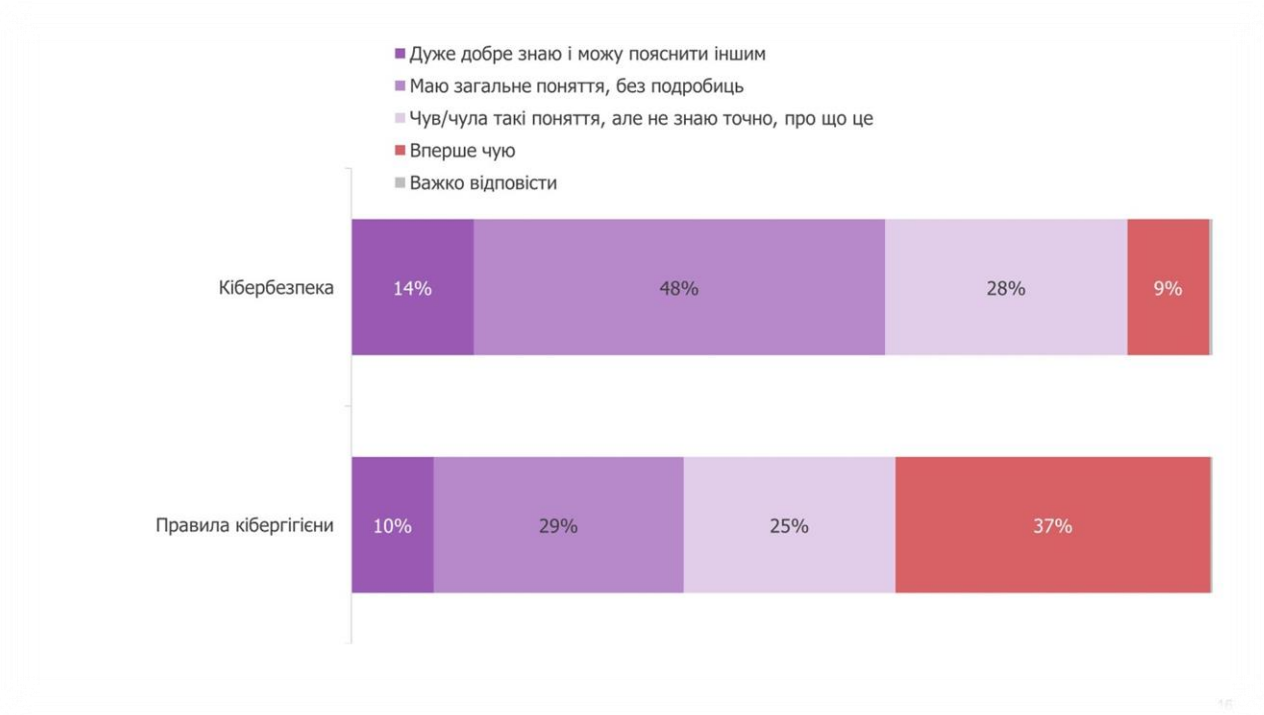
Обізнаність з поняттями «кібербезпека» та «правила кібергігієни»

Ми поцікавилися у респондентів, наскільки їм знайомі поняття «кібербезпека» та «правила кібергігієни». Утім, перевірка, що саме мають на увазі респонденти, які обрали відповідь «дуже добре знаю і можу пояснити іншим», не проводилася. Дуже добре знають, що таке кібербезпека 14% респондентів, а що таке правила кібергігієни – 10%.

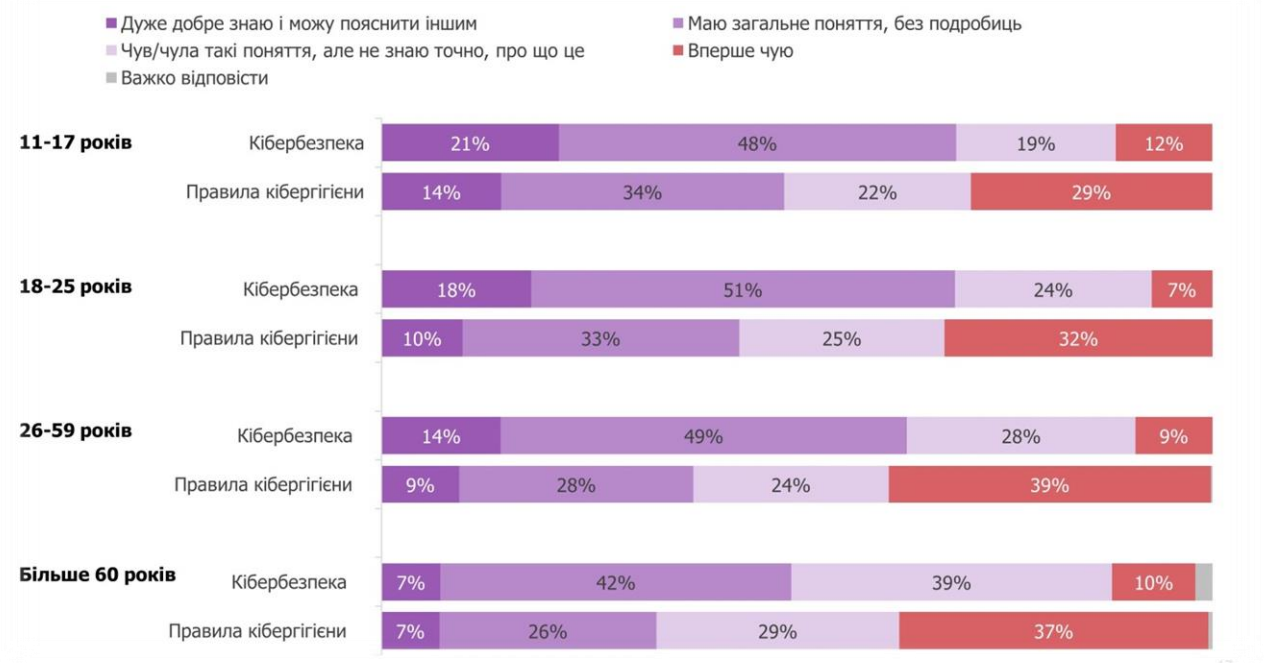
Загалом по вибірці 9% вперше чують про поняття «кібербезпека» і 37% вперше чують про існування «правил кібергігієни». Близько половини опитаних мають загальне поняття про «кібербезпеку», але не знають подробиць. Таку ж відповідь щодо «правил кібергігієни» обрали лише 29% опитаних (див. Діаграма 16).

Показово, що зазначені показники знання не дуже сильно варіюють із віком (див. Діаграма 17): майже для усіх вікових груп частки відповідей «вперше чую» співставні, також усі вікові групи більше обізнані щодо поняття «кібербезпека» аніж «правила кібергігієни». Молодь почувається більше обізнаною щодо обох понять (відповідь «дуже добре знаю» обрали 21% та 14% підлітків відповідно). Для літньої аудиторії аналогічні показники становлять по 7%, що втричі-удвічі менше.

Діаграма 16. Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека» та «правила кібергігієни»? (% відповідей, всі респонденти)



Діаграма 17. Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека» та «правила кібергігієни»? За цільовими групами (% відповідей, всі респонденти)



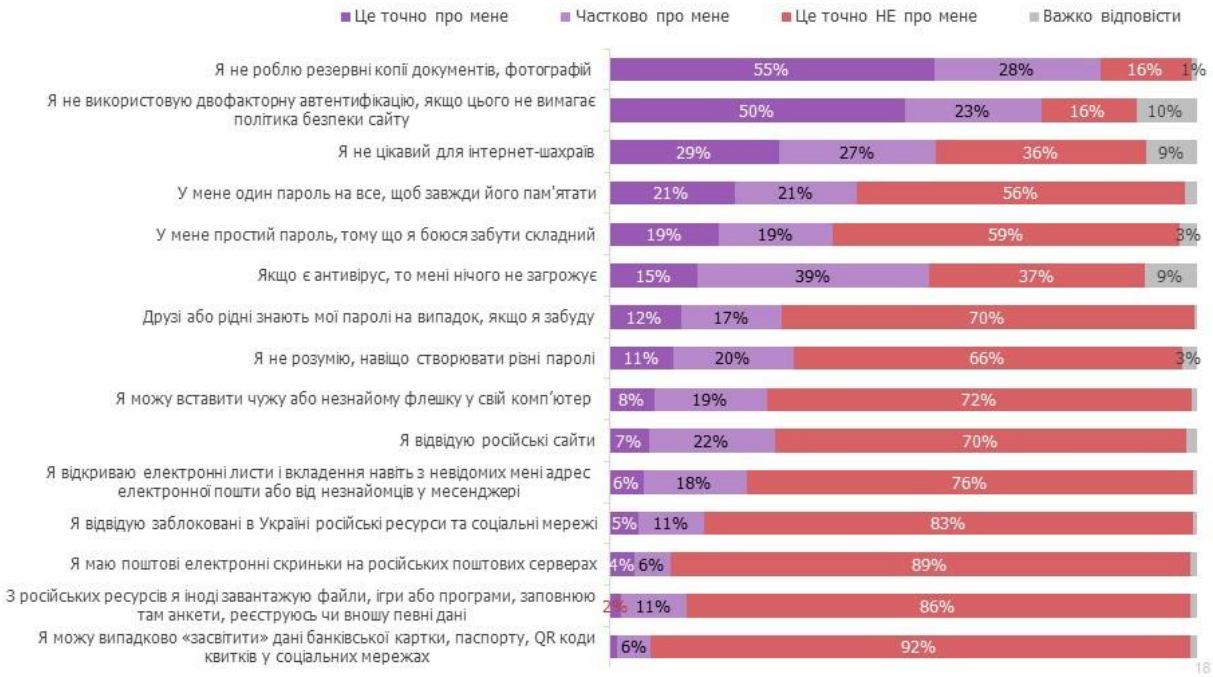
Ризикована поведінка

Ми запропонували респондентам оцінити кілька варіантів ризикованої поведінки в інтернеті, наскільки ці поведінкові шаблони схожі на їхню власну поведінку. Лідерами ризикованої поведінки є три шаблони:

- Відсутність резервних копій документів та даних (55% їх не роблять)
- Невикористання двофакторної автентифікації (50% не роблять цього)
- Впевненість, що користувач є нецікавим для інтернет-шахраїв (54% впевнені у цьому хоча б частково, 29% впевнені точно).

Також досить поширеною є думка про те, що наявність антивірусу гарантує захист від загроз (15% впевнені в цьому, ще 39% частково впевнені) (див. Діаграма 18. *Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, всі респонденти)*.

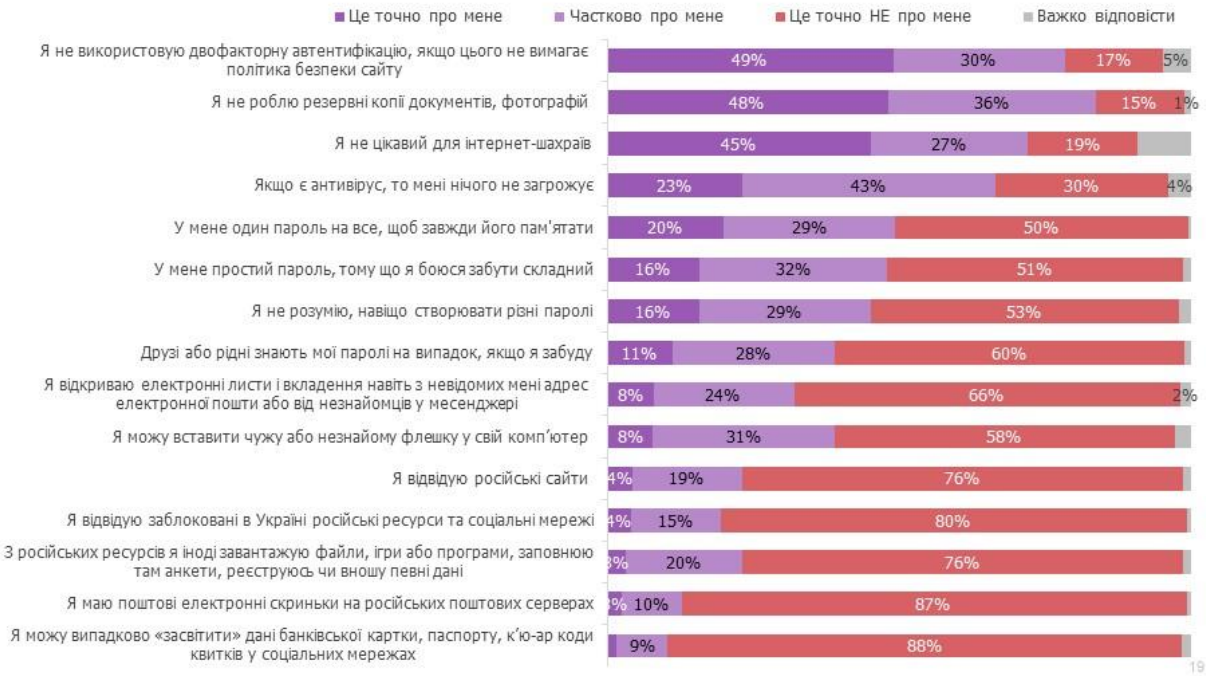
Діаграма 18. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, всі респонденти)



Невикористання резервних копій і двофакторної автентифікації є основними шаблонами ризикової поведінки для всіх вікових груп. Для підлітків більше, ніж для решти аудиторій, характерна впевненість у тому, що вони не цікаві інтернет-шахраям (45% впевнені у цьому, ще 27% частково впевнені). Також підлітки більшою мірою, ніж інтернет аудиторія загалом, впевнені у тому, що антивірус забезпечує повний захист (23% точно впевнені, ще 43 впевнені частково).

Рівень використання одного єдиного паролю для всіх випадків серед підлітків навіть вищий, ніж по вибірці в цілому: 20% заявили, що це шаблон поведінки повністю співпадає з їхнім (по вибірці в цілому 21%), ще 29% сказали, що шаблон частково співпадає з їхнім (по вибірці в цілому 21%). (див. Діаграма 19).

Діаграма 19. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, цільова група підлітки 11-17 років)



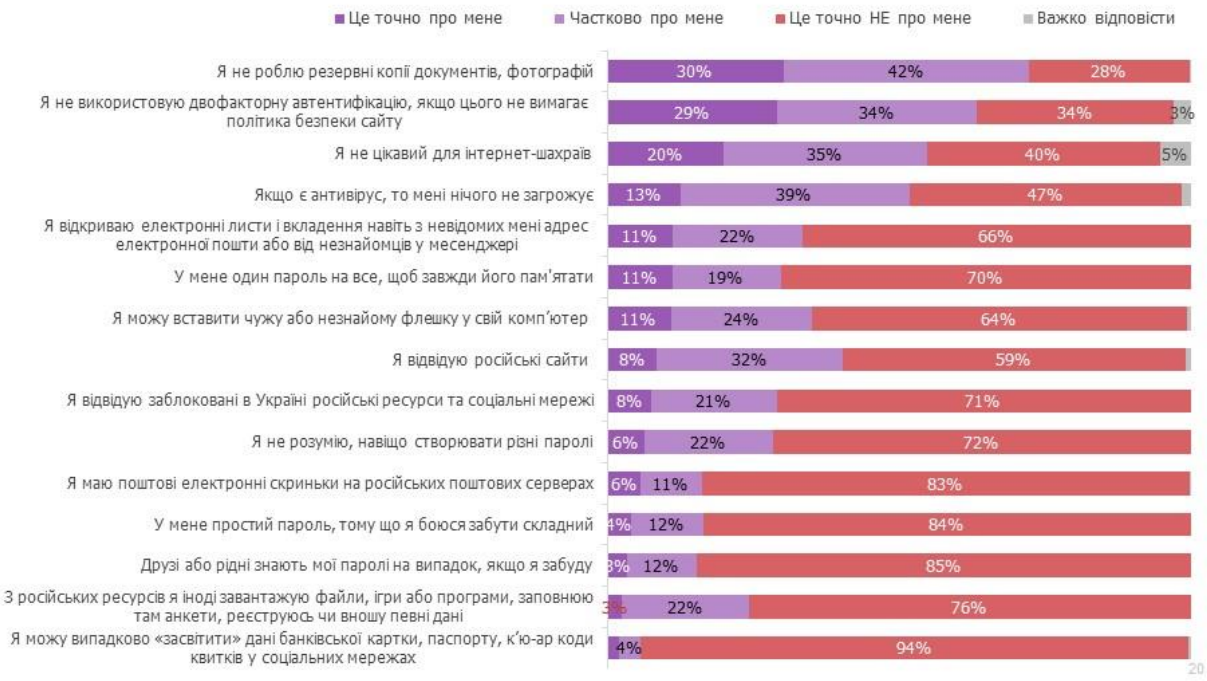
Молодь 18-25 років – найбільш обережна цільова група з поміж інших: вони з більшою регулярністю використовують двофакторну автентифікацію та роблять запасні копії документів та даних (а частка тих, хто це не робить, майже удвічі менша, ніж по вибірці в цілому).

Також молодь меншою мірою погоджується з тим, що є нецікавими для інтернет-шахраїв (20% повністю погоджуються порівняно до 29% по вибірці в цілому.

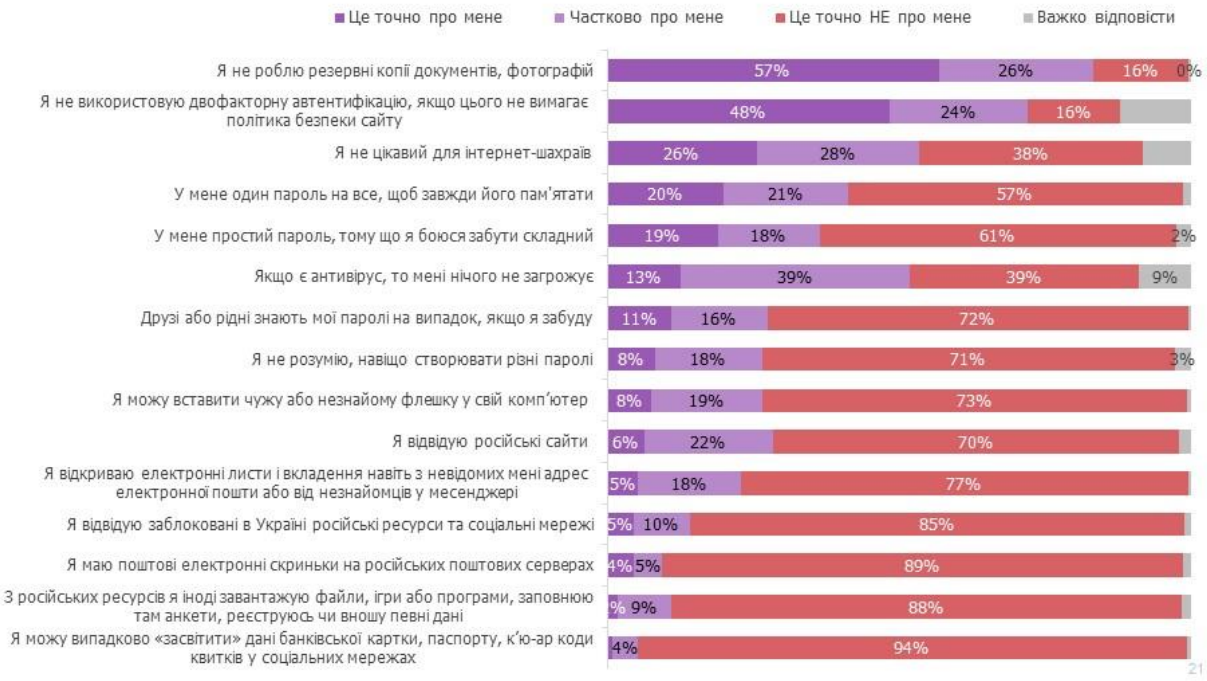
Утім, 40% цієї групи відвідують російські сайти – це найбільший показник з-посеред інших вікових груп (серед підлітків – 23%, серед дорослих – 28%, серед найстарших респондентів – 24%) (див. Діаграма 20).

Доросла аудиторія віком 26-59 років також впевнена у нецікавості для інтернет-шахраїв (26% впевнені, ще 28% впевнені частково та вірить у силу антивірусу (13% повністю покладається на антивірус, 39% покладається частково) Невикористання резервних копій і двофакторної автентифікації є основними шаблонами ризикової поведінки для цієї групи (див. Діаграма 21).

Діаграма 20. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, цільова група молодь 18-25 років)



Діаграма 21. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, цільова група дорослі 26-59 років)



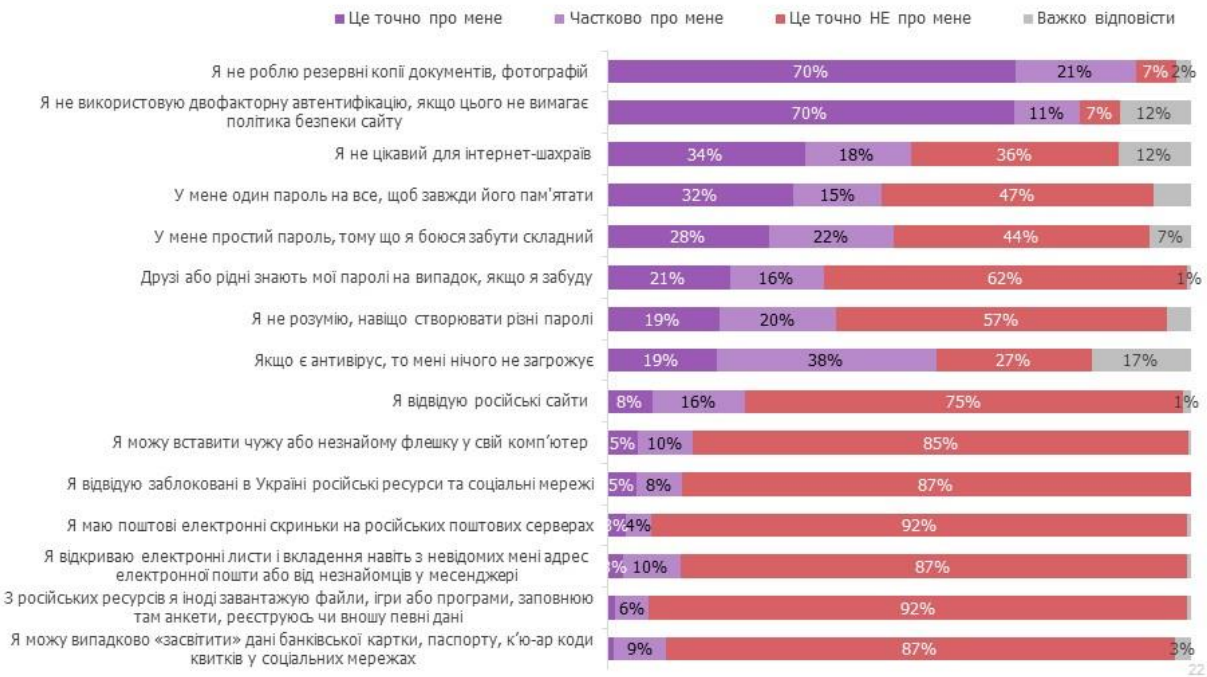
Невикористання резервних копій і двофакторної автентифікації серед найстаршої аудиторії (понад 60 років) розповсюджене найбільше за інші вікові групи: 70% респондентів не роблять

цього. Також люди найстаршого віку частіше за загальну аудиторію використовують один простий пароль (32% мають один пароль, 28% мають простий пароль, щоб не забути).

Також 19% цієї групи не розуміють, нащо створювати складні паролі (по вибірці в цілому цей показник 11%).

Також літні люди частіше діляться своїми паролями з друзями або рідними (21% повністю підтримує цей поведінковий шаблон, 16% - підтримує частково, в той час як по вибірці в цілому ці показники становлять 12% і 17% відповідно) (див. Діаграма 22).

Діаграма 22. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, цільова група люди старшого віку понад 60 років)



Окремим видом ризикованої поведінки може бути користування російськими поштовими скриньками, відвідування заблокованих в Україні російських ресурсів та соціальних мереж, а також відвідування російських сайтів та здійснення певних дій на них, як от завантаження з них файлів, заповнення анкет, реєстрація тощо.

Загалом по аудиторії найбільш поширене відвідування російських сайтів, 30% сказали, що роблять це. Найбільша частка респондентів з такою поведінкою серед молоді 18-25 років (40%), а найменша – серед найстаршої аудиторії понад 60 років (24%). Утім, є гіпотеза, що найстарші респонденти не завжди звертають увагу на доменне ім'я сайту і можуть не знати, на сайті якої країни знаходяться.

Молодь 18-25 років також частіше за інші групи відвідує заблоковані в Україні ресурси – таку поведінку визнали 29% цієї цільової групи (це майже удвічі більше, ніж по вибірці в цілому, 16%).

Молодь (18-25 років) і підлітки (11-17 років) також частіше за інші групи завантажує з російських ресурсів файли, програми, проходять реєстрацію. Частка респондентів з такою

поведінкою серед цих груп становить 24% та 23% відповідно. Серед цільової групи 25-59 років така поведінка зустрічається удвічі рідше (11%), а серед найстарший респондентів – утричі рідше (8%).

Російські поштові скриньки найчастіше використовують респонденти віком 18-25 років, 17% зареєстровані на російських поштових серверах. На другому місці за розповсюдженістю такої поведінки – підлітки 11-17 років, 13% з них мають російські поштові скриньки. Більш старші аудиторії використовують російські поштові сервери рідше: серед групи віком 26-59 років таких 9%, а серед групи віком більше 60 років – 7%.

Досвід зіткнення із кіберзагрозами

Ми запропонували респондентам оцінити свій досвід зіткнення із кіберзагрозами. Кожній цільовій групи було запропоновано свій перелік кіберзагроз, які, на думку експертів, притаманні саме цій віковій групі; по кожній кіберзагрозі респонденти могли позначити, чи траплялася така ситуація з ними особисто, з їхніми реальними або віртуальними знайомими.

Загалом по вибірці хоча б з одним із видів кібершахрайства стикалися 41% користувачів. Найбільша частка припадає на групу віком 25-59 років, тут особистий досвід має майже кожен другий (47%). Серед молоді 18-25 років ця частка становить 37%, а серед літніх людей старше 60 років – 43%. Підліткам пощастило найбільше – лише 7% стикалися із випадками кібершахрайства особисто.

Перше місце у вибірці в цілому посіла ситуація, коли кібершахраї вимагають гроші, використовуючи методи соціальної інженерії (маніпуляції, погрози, шантаж), а також особисті та родинні дані (через телефон та месенджери). Цю ситуацію оцінювали лише літні люди (віком понад 60 років), і майже кожен третій (28%) стикався з такою ситуацією особисто. 21% чув про подібні ситуації від знайомих (див. Діаграма 23).

Діаграма 23. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, всі респонденти)

Підлітки найчастіше стикаються із крадіжкою облікових записів (див. Діаграма 24).

Діаграма 24. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, цільова група підлітки 11-17 років)

Утім, найчастіше від усіх інших аудиторій, із крадіжкою облікових записів у соціальних мережах стикається молодь віком 18-25 років: майже кожен третій (29%) стикався з таким особисто, 41% знають про подібні випадки від знайомих. А кожен десятий мав і особистий досвід, і знає про досвід друзів. Загалом, особисто або у дружньому колі із випадками зламу аккаунтів стикалися 60% респондентів. Із випадками вимагання паролів молодь стикається утричі рідше (див. Діаграма 25).

Діаграма 25. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, цільова група молодь 18-25 років)

Для дорослої аудиторії віком 26-59 років найбільш розповсюдженою загрозою є Вимагання банківських даних, паролів та доступу до облікових записів банківських мобільних додатків, банківських рахунків (у т.ч. через телефон, месенджери): кожен четвертий стикався з цим особисто, 27% знають про такі випадки від знайомих. Також поширеними, але менш розповсюдженими є випадки вимагання особистих даних, злам облікових записів у соціальних мережах та вимагання грошей задля розблокування роботи комп'ютерних систем (частка аудиторії, яка стикалася з цими ситуаціями особисто, становить 15%, 13% та 13% відповідно) (див.

Діаграма ***26***).

Діаграма 26. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, цільова група дорослі 26-59 років)

Літні люди, стикаються із кіберзагрозами частіше за інші аудиторії: з вимаганням грошей, банківських та особистих даних стикалися 28%, 23% та 19% відповідно (див. Діаграма 27).

Діаграма 27. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, цільова група люди старшого віку понад 60 років)

Значна частина ситуацій, які траплялися із респондентами особисто, траплялася протягом останніх 3 місяців (див Діаграма 28).

Діаграма 28. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто)

41% підлітків з тих, хто стикався із довірчим вимаганням паролів, мали цей досвід протягом останніх трьох місяців. Атаки на ігрові аккаунти та аккаунти у соціальних мережах також відбувалися нещодавно: 29% та 23% з тих, хто стикався із такою ситуацією, стикалися з нею протягом останніх 3 місяців (див.

Діаграма ***29***).

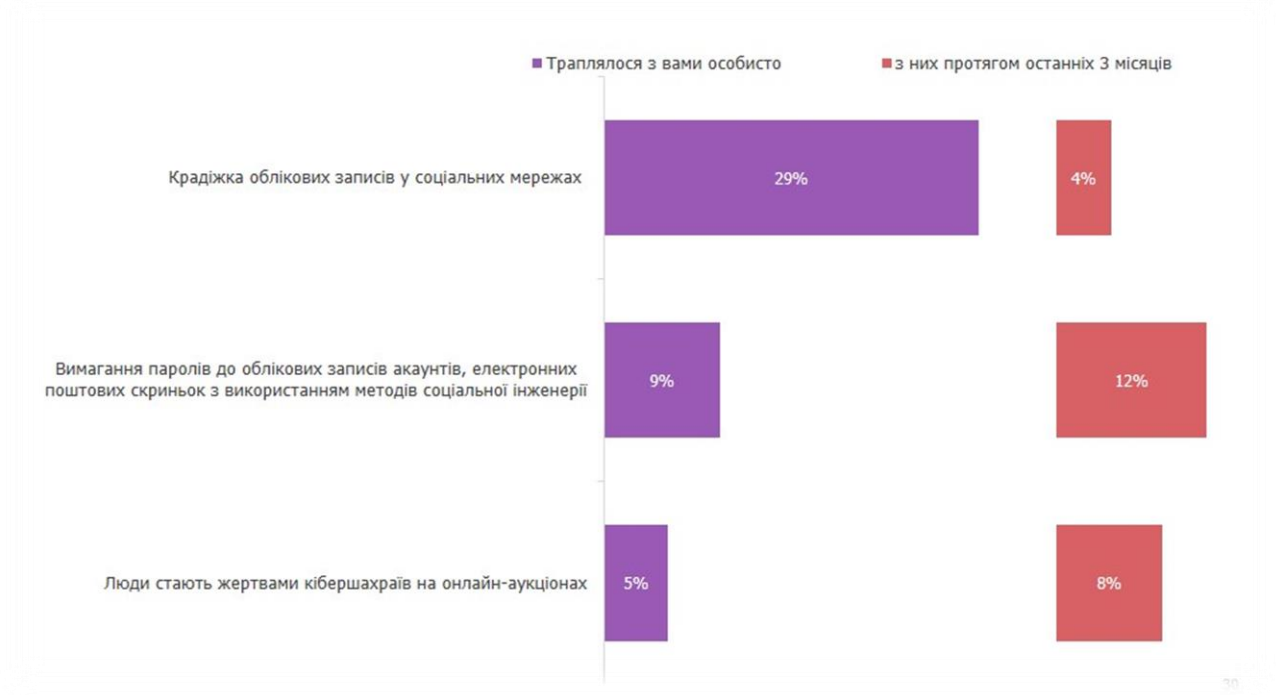
Атаки на молодь 18-25 років відбуваються не так часто: лише 4% з тих, хто стикався із крадіжкою облікових записів (а це найбільш поширене кібершахрайтсво у цій віковій групі), стикалися з такою ситуацією протягом останніх 3 місяців (див. Діаграма 30).

Респонденти дорослої (26-59 років) групи стикаються із загрозами трохи частіше за молодь: 24% з тих, хто стикнувся з вимаганням банківських даних, пережили цей негативний досвід протягом останніх 3 місяців. Жертвами кібершахраїв на онлайн аукціонах були лише 2%, утім з 27% це сталося протягом останніх місяців (див. Діаграма 31).

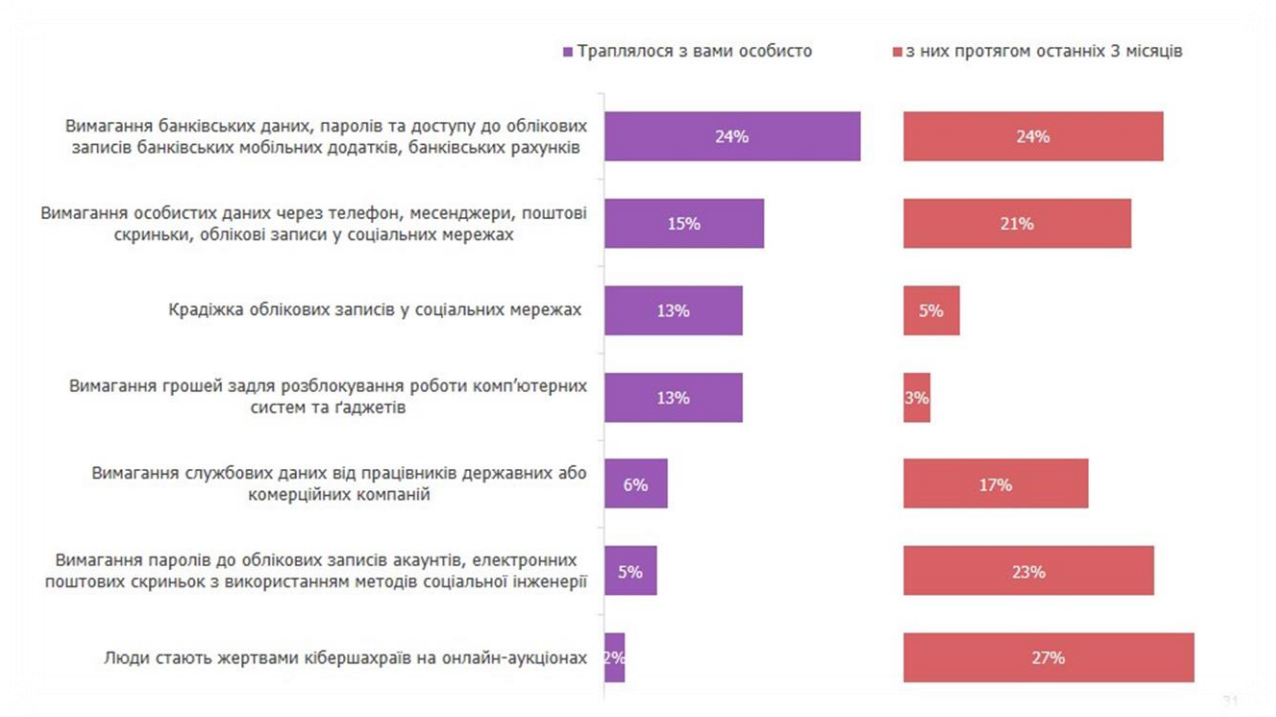
Серед найстаршої групи кожен п’ятий випадок вимагання грошей або банківських даних трапився протягом останніх 3 місяців (див. Діаграма 32).

Діаграма 29. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто, цільова група підлітки 11-17 років)

Діаграма 30. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто, цільова група молодь 18-25 років)



Діаграма 31. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто, цільова група дорослі 26-59 років)



Діаграма 32. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз? (% відповідей, респонденти, які стикалися з загрозами особисто, цільова група люди старшого віку понад 60 років)

Попри усі випадки загроз, респонденти рідко почуваються повністю беззахисними у таких ситуаціях: частка таких відповідей варіює від 11 до 17% у залежності від загрози. Найчастіше повністю беззахисними почуваються літні люди у випадках, коли шахраї вимагають гроші методами соціальної інженерії.

Найбільш розповсюдженою відповіддю щодо усіх типів загроз залишається відповідь «не завжди почуваюся захищеним» -- її обирали від 37% до 57% респондентів у залежності від загрози. Утім, приблизно третина респондентів почувається повністю захищеними від більшості загроз, найменша частка відповідей «почуваюся повністю захищеним» припадає на ситуацію зламу облікових записів у соціальних мережах (24%) (див. Діаграма 33).

Діаграма 33. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами)

- Підлітки є досить самовпевненою групою інтернет-користувачів – від 34% до 43% з тих, хто стикався із загрозами, почуваються повністю захищеними (див. Діаграма 34).
- Молодь меншою мірою впевнена щодо зламу аккаунтів (31% почуваються повністю захищеними), а більшою мірою впевнена щодо захисту від вимагання паролів (43% почуваються повністю захищеними) (див. Діаграма 35).
- Доросла аудиторія також найменш впевнено почувається щодо зламу аккаунтів (21% почуваються повністю захищеними), для решти загроз повний захист відчувають від 30% до 34%) (див. Діаграма 36).
- Найстарші респонденти майже не відрізняються від загальної аудиторії за рівнем почуття захищеності: повністю захищеними почуваються 26%-32%, а повністю беззахисними – 12%-17%, у залежності від типу загроз (див. Діаграма 37).

Діаграма 34. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами, цільова група підлітки 11-17 років)

Діаграма 35. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами, цільова група молодь 18-25 років)

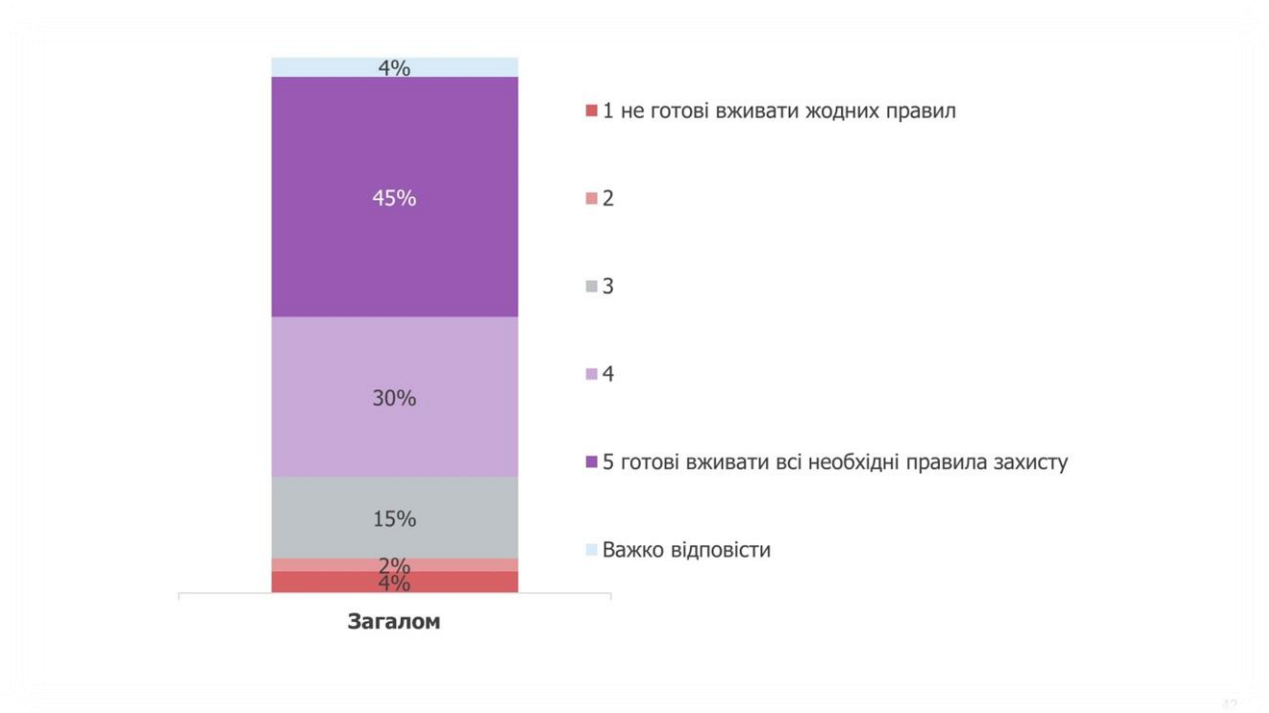
Діаграма 36. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами, цільова група дорослі 26-59 років)

Діаграма 37. Наскільки ви почуваєтеся захищеними щодо деяких загроз? (% відповідей, респонденти, які стикалися з загрозами, цільова група люди старшого віку понад 60 років)

Обізнаність із правилами кібербезпеки

Незважаючи на помірний рівень почуття захищеності, більша частина респондентів готові вживати правила захисту: 45% по вибірці в цілому готові, а 30% здебільшого готові вживати усіх необхідних правил захистку (або, принаймні, декларують таку готовність) (див. Діаграма 38).

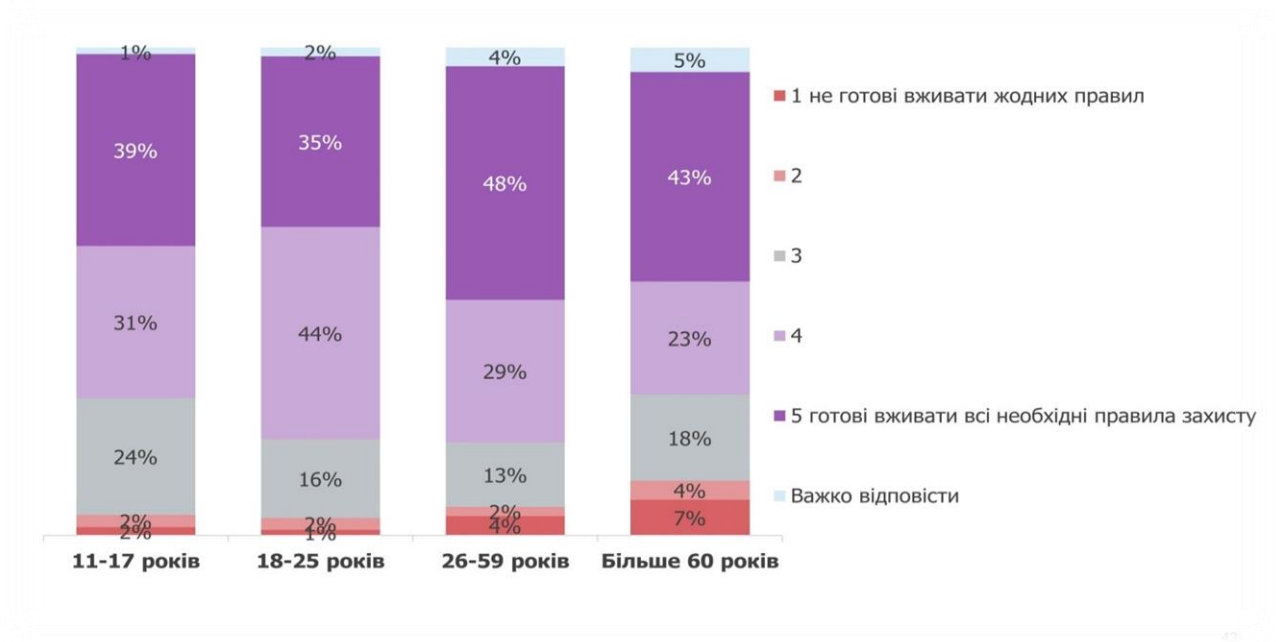
Діаграма 38. Наскільки ви готові вживати правила кібергігієни, щоб вберегтися від цих загроз? (% відповідей, респонденти, які почуваються не повністю захищеними щодо кіберзагроз)



Найбільшу готовність вживати правила захисту демонструють цільові групи «молодь» та «дорослі» - 79% та 77% респондентів відповідно декларують готовність вживати усіх необхідних правих захисту (сума оцінок «4» та «5» за п'ятибальною шкалою), при чому у групі «дорослі» беззаперечна готовність слідувати правилам (оцінка «5») складає 48% - це найвищий показник з-посеред усіх груп. За цим показником на другому місці люди найстаршого віку (понад 60 років) – 45% з них декларують готовність вживати усіх необхідних правих захисту. Утім, саме в цій групі найвищий рівень опору до вживання правил захисту: 7% не готові вживати жодних правил (оцінка «1»), ще 4% - скоріше не готові вживати (оцінка «2») (див.

Діаграма ***39***).

Діаграма 39. Наскільки ви готові вживати правила кібергігієни, щоб вберегтися від цих загроз? За цільовими групами (% відповідей, респонденти, які почуваються не повністю захищеними щодо кіберзагроз)



Ми надали аудиторії можливість оцінити ставлення до базових правил кібергігієни. З більшістю правил аудиторія хоча б обізнана: лише 5 правил отримали частку відповідей «вперше чую» більше 10% (див. Діаграма 40). Утім, знання правил досить значно варіює із віком.

Діаграма 40. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти)

Так, підлітки досить добре обізнані із усіма правилами, частка респондентів, які знають кожне правило, перевищує 90%. Найменше знають правила «Не встановлюйте додатки з неофіційних магазинів» (знають 92%) та «Не підключайтесь до загальнодоступних мереж Wi-Fi» (знають 93%). Решту правил знає ще більша частка респондентів. Утім, не всі вони виконуються: так, правило щодо утримання від підключення до загальнодоступних мереж Wi-Fi завжди виконують 40% респондентів, а не виконують – 22%.

Найчастіше підлітки виконують правила щодо заборони відправляти скани банківських карток або документів та контактних даних або фотографій – 83% та 80% відповідно декларують неуклінне виконання цих правил (див. Діаграма 41).

Діаграма 41. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти, цільова група підлітки 11-17 років)

Молодь також непогано знайома із більшістю запропонованих правил. Лише одне правило виявилося таким, що мало знайоме респондентам: 42% сказали, що вперше чують про необхідність повідомляти відповідні органи за підозри зараження або компрометації даних. Другим за рівнем поганої обізнаності є правило щодо використання двофакторної автентифікації: 15% вперше чують про це.

Два правила, яких молоді респонденти дотримуються краще за все, це «не відправляйте фото та скани банківських карток» та «не залишайте пристрій без нагляду» - дотримання цих правил декларують 94% та 87% респондентів відповідно (див Діаграма 42).

Ці ж два правила частіше за все (89% та 83% відповідно) використовують і дорослі респонденти (25-59 років). Вони так само, як і молодь, відносно погано ознайомлені із правилами про необхідність повідомляти відповідні органи за підозри зараження або компрометації даних (вперше чують 42%) та щодо використання двофакторної автентифікації

(вперше чують 39%). Також респонденти 25-59 років гірше за молодші групи обізнані про необхідність регулярно робити резервні копії (вперше чують 17%) (див. Діаграма 43).

Діаграма 42. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти, цільова група молодь 18-25 років)

Діаграма 43. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти, цільова група дорослі 26-59 років)

Респонденти найстаршого віку, як і інші групи, знають про небезпеку щодо відправки фото та сканів банківських карток або документів незнайомцям (90% дотримуються правила цього не робити). 81% не залишає пристрій без нагляду.

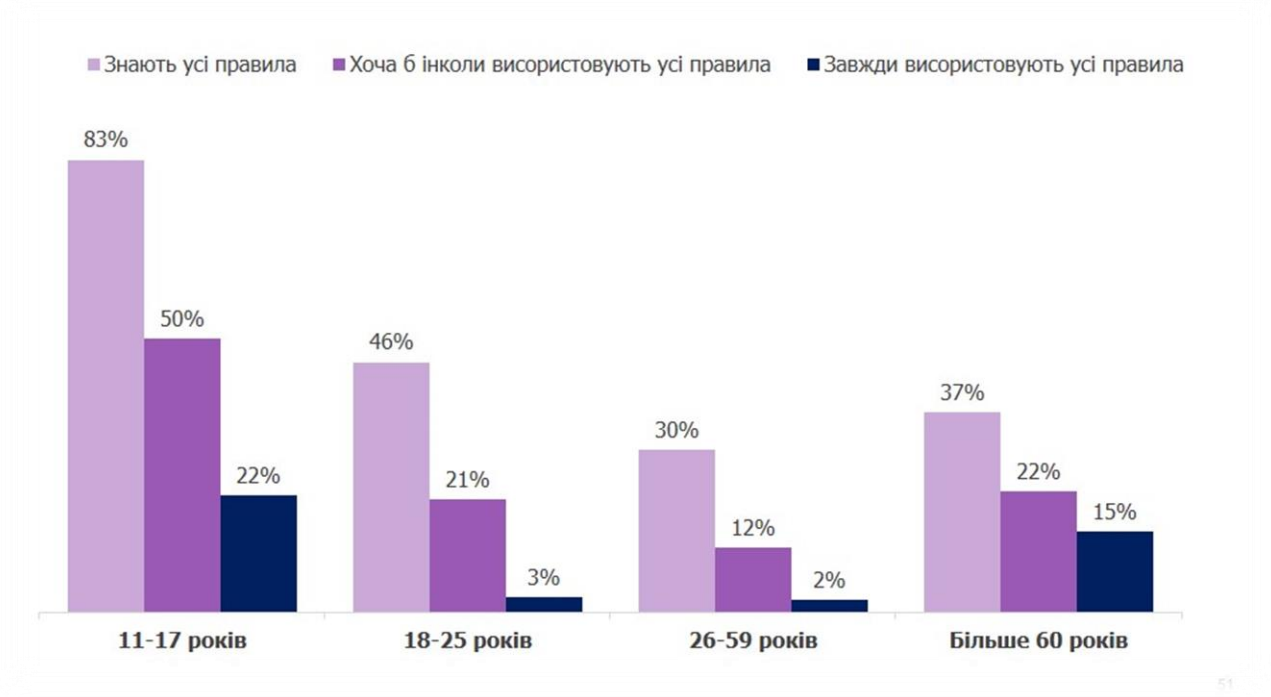
Лише 45% респондентів найстаршого віку використовують складні та різні паролі. Ця частка порівняна до відповідного показнику у групи дорослих респондентів (48%). Але якщо вікова група 26-59 років знає про необхідність використовувати складні та різні паролі, і свідомо не робить цього, то найстарші респонденти часто (23%) навіть не знають про таке правило безпеки (див. Діаграма 44).

Діаграма 44. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, всі респонденти, цільова група люди старшого віку понад 60 років)

Ми проаналізували, наскільки кожна вікова група знає і виконує низку правил кібербезпеки загалом. Так, підлітки 11-17 років є найбільш обізнаною групою: 83% знають усі правила кібербезпеки. Утім, лише 50% виконують усі правила хоча б інколи, а постійно виконують усі правила лише 22%. Тим не менш, показники виконання правил у групі підлітків також найбільші серед решти цільових груп: серед молоді 18-25 років хоча б інколи виконують правила 21%, серед дорослих 25-59 років – 12%, а серед найстарших респондентів понад 60 років – 22%.

Найстарша група респондентів є найменш обізнаною: лише 37% знають про усі правила кібербезпеки для цієї групи. Але також ці респонденти є найбільш свідомими: частка тих, хто виконує усі правила, серед тих, хто з ними обізнаний, для найстаршої аудиторії становить 40%. Це найбільший показник серед інших груп: для підлітків він становить 26%, а для молоді 18-25 років і дорослих 26-59 років – лише 6% і 8% відповідно (див. Діаграма 46).

Діаграма 45. Знання і виконання правил кібербезпеки, загалом



Безпека поведінки в інтернеті

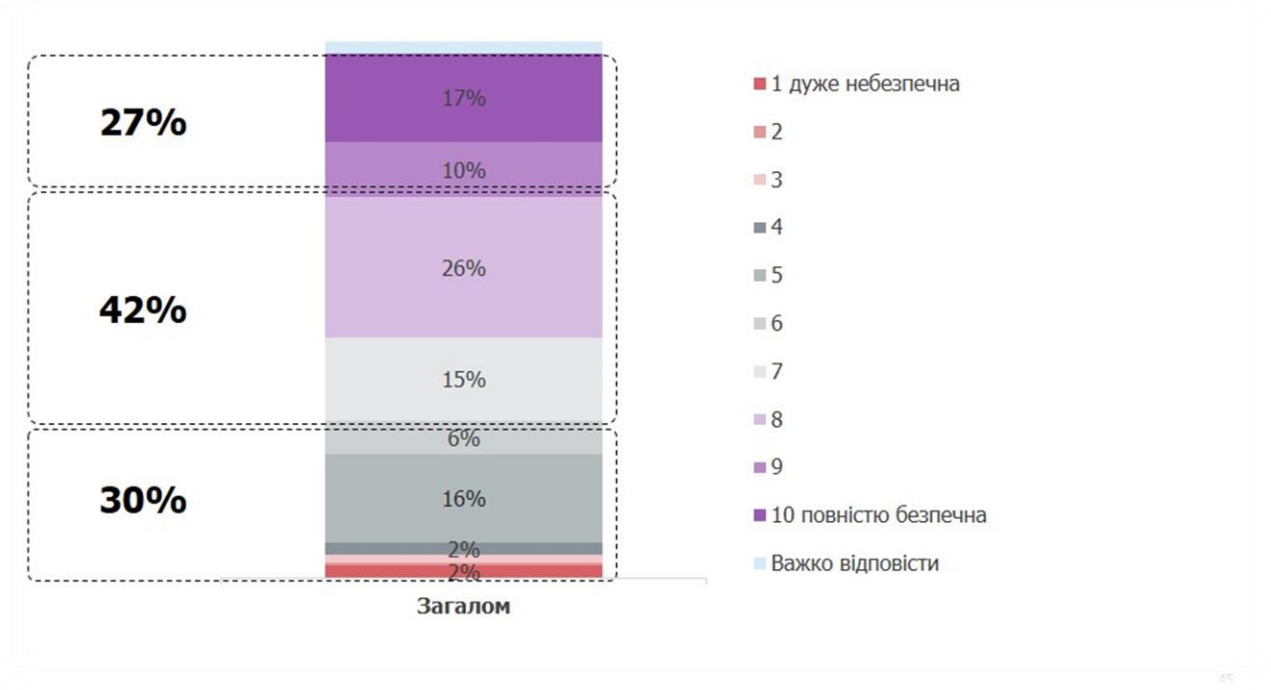
Ми запропонували респондентам оцінити безпеку власної поведінки в інтернеті за шкалою від 1 до 10, де 1 означає «дуже небезпечна», а 10 – «повністю безпечна». Загалом, трохи більше чверті респондентів оцінюють власну поведінку в інтернеті як повністю або доволі безпечну (поставили оцінки 9 або 10 за 10-бальнрою шкалою). Частка тих, хто вважає, що поводиться небезпечно (оцінки від 1 до 6 включно) становить 30% (див. Діаграма 46).

Ці оцінки значною мірою варіюють із віком: так, серед підлітків (11-17 років) та молоді (18-25 років) менша частка, хто вважає, що поводиться небезпечно (19% та 17% відповідно), тоді як серед людей старше 25 років кожен третій вважає поведінку небезпечною.

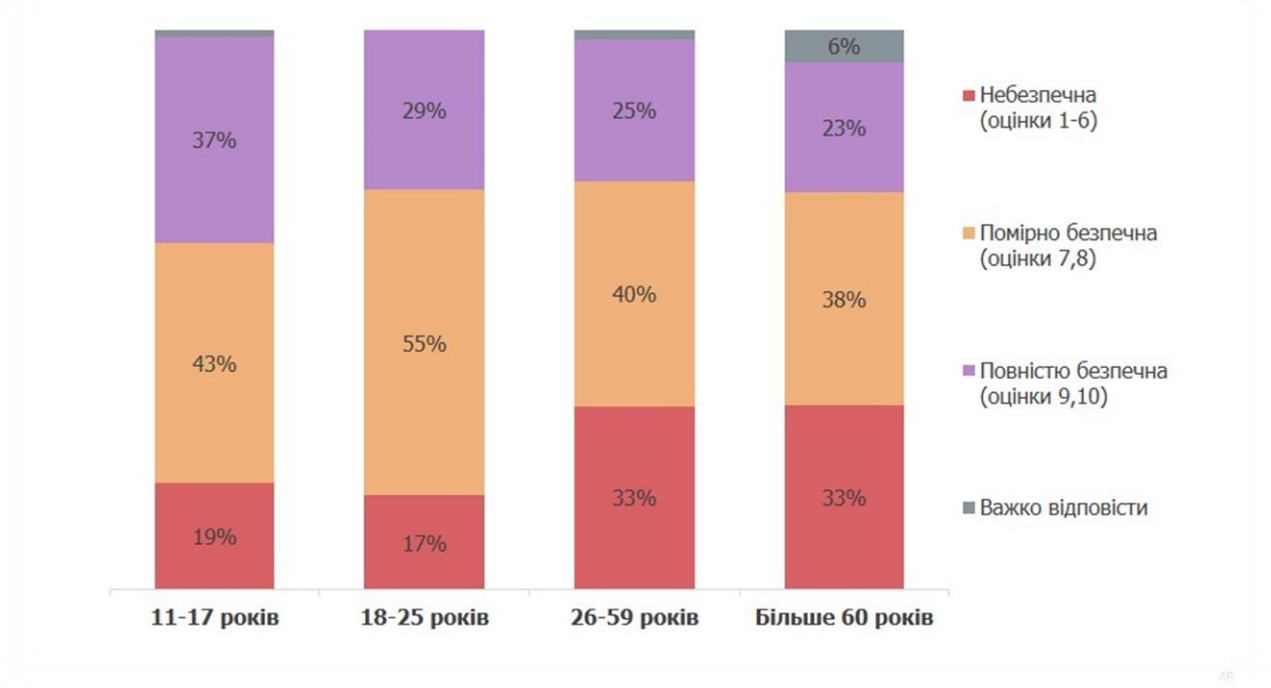
Серед підлітків найбільша частка тих, хто вважає, що поводиться повністю безпечно (37%), тоді як серед інших вікових груп ця частка суттєво менша.

Загалом серед молоді до 25 років частка тих, хто вважає свою поведінку безпечною, більша, ніж частка тих, хто вважає, що поводиться небезпечно. Серед респондентів, старших 25 років, частка тих, хто усвідомлює небезпеку поведінки, більша, ніж частка тих, хто думає, що поводиться безпечно (див. Діаграма 47).

Діаграма 46. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? (% відповідей, всі респонденти)



Діаграма 47. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? За цільовими групами (% відповідей, всі респонденти)



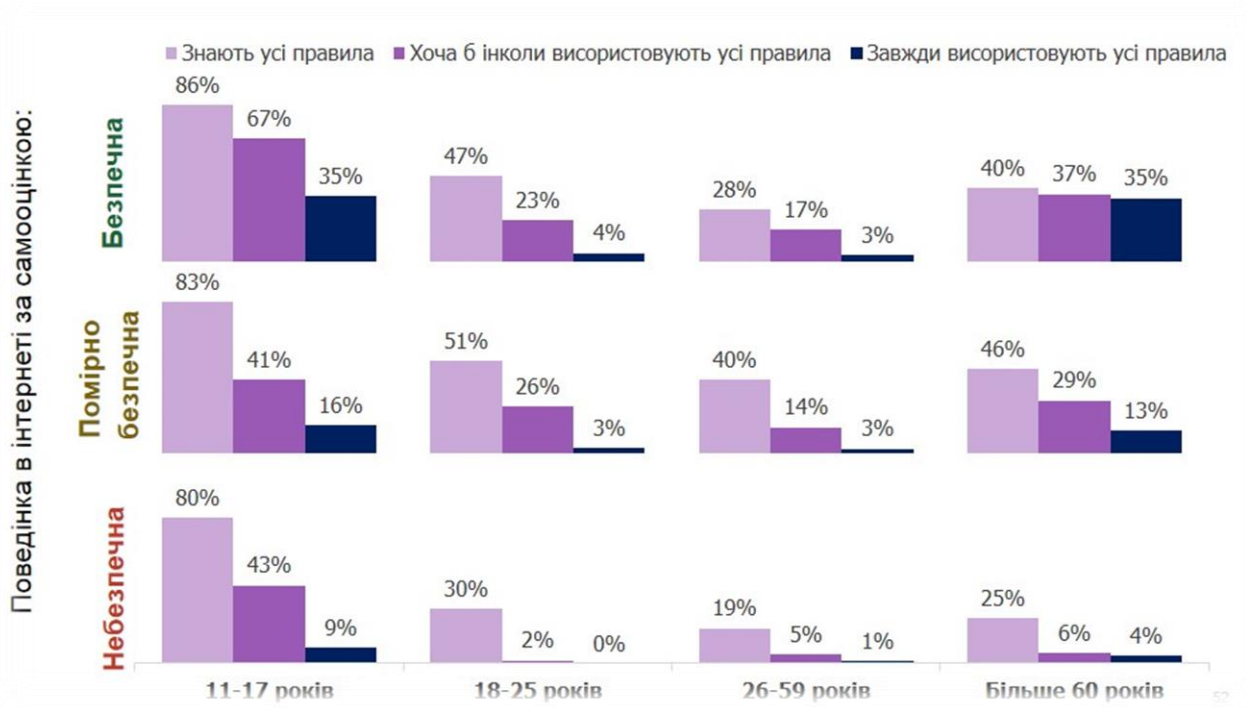
Самооцінка поведінки в інтернеті залежить від знання та виконання правил кібербезпеки: чим вище людина оцінює безпеку своєї поведінки, тим краще вона знає і частіше виконує правила кібербезпеки. Ця кореляція прослідковується для всіх вікових груп. Так, ті, хто оцінює свою поведінку як небезпечну, або не знає правил, або знає, але нехтує ними.

Підлітки, як найбільш обізнана група, оцінює свою поведінку за рівнем додержання правил. Для решти вікових груп самооцінка безпеки корелює в першу чергу із рівнем знання.

Група респондентів найстаршого віку (понад 60 років), які оцінюють свою поведінку як безпечну, є найбільш сумлінною групою щодо виконання правил кібербезпеки: якщо людина знає правило, вона його неуклінно додержується.

Утім, показовим є факт, що часткове виконання деяких правил також дає почуття безпеки: особливо це помітно в сегменті респондентів від 18 до 59 років: серед тих, хто вважає свою поведінку повністю безпечною, лише 3-4% додержуються усіх правил (див. Діаграма 48).

Діаграма 48. Знання і виконання правил кібербезпеки у розбивці за рівнем самооцінки безпеки поведінки в інтернеті



Утім, декларування виконання правил кібербезпеки не означає справжнього виконання цих правил. Так, ми проаналізували відповіді респондентів, які заявили, що виконують певне правило, і подивилися, наскільки їм притаманна ризикована поведінка, пов'язана із невиконанням цього правила.

Наприклад, серед тих, хто задекларував виконання правила «*Використовуйте складні паролі і не використовуйте одні і ті ж самі паролі для реєстрації на онлайн-ресурсах, у соціальних мережах та ігрових мобільних додатках, звикайте користуватись менеджерами паролі*», лише приблизно ¾ дійсно поводяться таким чином (див. Таблиця 1).

Таблиця 1. Реальна поведінка щодо паролів серед тих, хто декларує використання відповідного правила

Відповіді респондентів, які сказали, що завжди виконують правило: *«Використовуйте складні паролі і не використовуйте одні і ті ж самі паролі для реєстрації на онлайн-ресурсах, у соціальних мережах та ігрових мобільних додатках, звикайте користуватись менеджерами паролі» (49% респонденів)*	Це точно про мене	Частково про мене	Це точно НЕ про мене	Важко відповісти
У мене простий пароль, тому що я боюся забути складний	9%	13%	77%	1%
У мене один пароль на все, щоб завжди його пам'ятати	12%	13%	74%	1%
Я не розумію, навіщо створювати різні паролі	8%	17%	73%	2%

Ситуація із використанням двофакторної автентифікації суттєво гірша: лише половина з тих, хто декларує виконання цього правила, дійсно це роблять, а кожен п'ятий – не робить взагалі (див. Таблиця 2).

Таблиця 2. Реальна поведінка щодо використання двофакторної автентифікації серед тих, хто декларує використання відповідного правила

Відповіді респондентів, які сказали, що завжди виконують правило: *«За можливості, використовуйте двофакторну автентифікацію» (28% респондентів)*	Це точно про мене	Частково про мене	Це точно НЕ про мене	Важко відповісти
Я використовую двофакторну автентифікацію, навіть якщо цього не вимагає політика безпеки сайту (наприклад, банківські додатки)	49%	28%	20%	3%

Ситуація із резервним копіюванням іще гірша: серед тих, хто знає і, за їхніми словами, завжди дотримується правила «*Завжди створюйте резервні копії важливих даних на окремому локальному пристрої чи хмарному сховищі*», менше половини дійсно декларують таку поведінку, а кожен третій каже, що не робить цього (див. Таблиця 3).

Таблиця 3. Реальна поведінка щодо використання резервного копіюванням серед тих, хто декларує використання відповідного правила

Відповіді респондентів, які сказали, що завжди виконують правило: *«За можливості, використовуйте двофакторну автентифікацію» (30% респондентів)*	Це точно про мене	Частково про мене	Це точно НЕ про мене	Важко відповісти
Я регулярно роблю резервні копії документів, фотографій – для захисту даних	44%	21%	35%	0%

Ситуації, де декларування виконання правила і реальна поведінка збігаються, стосуються заборони відправляти незнайомцям фото та скани банківських карток та особистих документів (показово, що цього правила інтуїтивно дотримуються навіть ті, хто формально

про нього не знає), а також застереження проти відкриття сумнівних листів (94% тих, хто знає і дотримується цього правила, дійсно сказали, що не відкривають листи і вкладення з невідомих адрес електронної пошти або від незнайомців у месенджері).

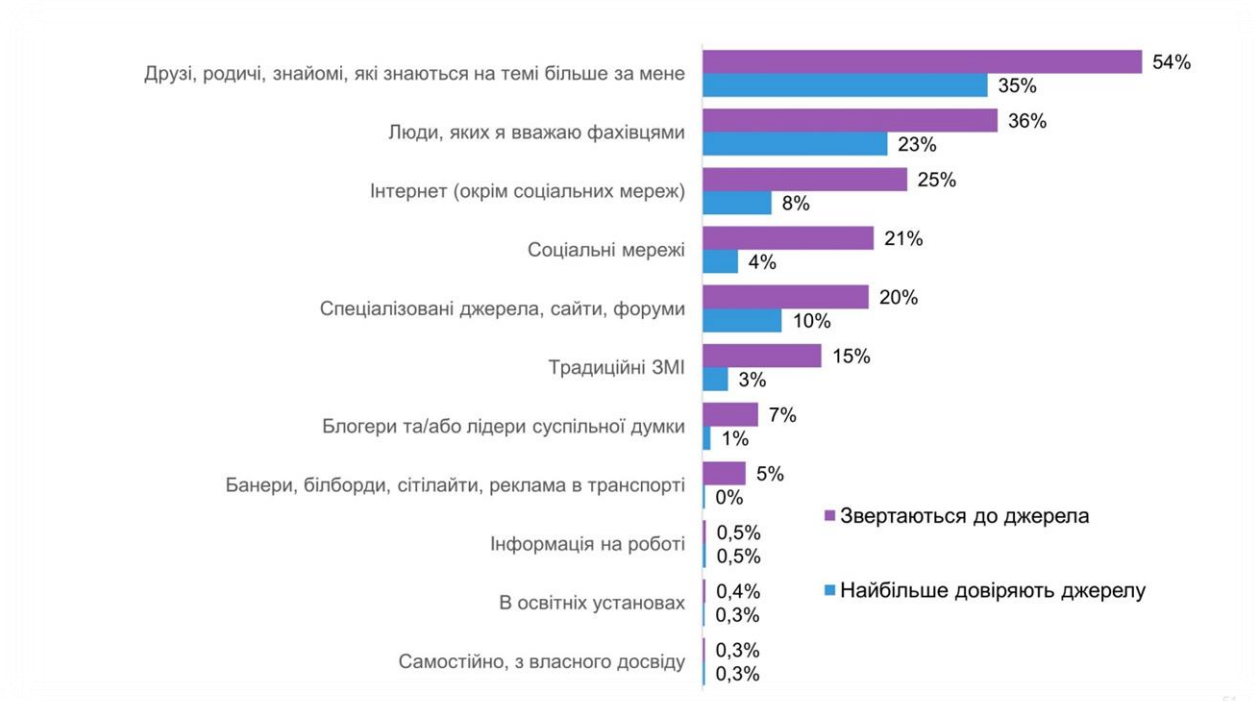
Джерела інформації про правила безпечної поведінки в інтернеті

Більше половини (54%) респондентів по вибірці загалом про правила безпечної поведінки в інтернеті дізнаються від друзів, знайомих родичів. На другому місці – люди, яких респонденти вважають фахівцями (до цього джерела звертаються 36%). До інтернету, у той чи інший спосіб (сайти, соціальні мережі, форуми) звертаються від 20 до 25% респондентів.

За показником довіри до джерел також перші місця посідають друзі, родичі знайомі (35%) та люди, яких респонденти вважають фахівцями (23%).

Інформацію з місця роботи або навчання отримує дуже незначна частка респондентів (0,5% та 0,4% відповідно), але ті, хто використовує ці джерела саме їх вважають найбільш надійними і вартими довіри (див Діаграма 49).

Діаграма 49. Які джерела інформації ви використовуєте, щоб дізнатися про правила безпечної поведінки в інтернеті? Якому з цих джерел інформації ви довіряєте найбільше? (% відповідей, всі респонденти)



Джерела інформації, якими користуються, та яким довіряють респонденти, досить сильно варіюють за цільовими групами. Так, для підлітків на друге місце у списку джерел ділять соціальні мережі та люди, яких респонденти вважають фахівцями (утім, довіряють соціальним мережам менше). Для молоді на перше місце вийшли люди, яких респонденти вважають фахівцями (38% звертаються до цього джерела і 24% довіряють йому найбільше).

Дорослі люди 26-59 років найчастіше звертаються до знайомих та (51%), але рівень довіри до фахівців вище. Люди найстаршого віку частіше за інших звертаються до друзів або родичів (68%) і відповідно довіряють цьому джерелу найбільше (55%) (див. Діаграма 50, Діаграма 51).

Діаграма 50. Які джерела інформації ви використовуєте, щоб дізнатися про правила безпечної поведінки в інтернеті? За цільовими групами (% відповідей, всі респонденти)

Діаграма 51. Якому з цих джерел інформації ви довіряєте найбільше? За цільовими групами (% відповідей, всі респонденти)

V Додаток 1. Міста 50+, де проводилося опитування

Бахмут (колишнє Артемівськ)
Бердичів
Бердянськ
Біла Церква
Бориспіль
Бровари
Дніпро (колишнє Дніпропетровськ)
Дрогобич
Енергодар
Житомир
Запоріжжя
Івано-Франківськ
Ізмаїл
Ірпінь
Кам'янське (колишнє Дніпродзержинськ)
Кам'янець-Подільський
Київ
Ковель
Коломия
Конотоп
Костянтинівка
Краматорськ
Кременчук
Кривий Ріг
Кропивницький (колишнє Кіровоград)
Лисичанськ
Лозова
Луцьк
Львів
Маріуполь
Мелітополь
Миколаїв
Мукачеве
Ніжин
Нікополь
Нововолинськ
Новоград-Волинський
Новомосковськ
Одеса
Олександрія
Павлоград
Покровськ (колишнє Красноармійськ)
Полтава
Рівне
Рубіжне
Сєвєродонецьк
Слов'янськ
Сміла
Суми
Тернопіль
Ужгород
Умань
Харків
Херсон
Хмельницький
Черкаси
Чернівці
Чернігів
Чорноморськ (колишнє Іллічівськ)
Шостка

VI Додаток 2. Опитувальник

Вітання

Доброго дня, мене звати _____, я представляю компанію Смарт Дата Сервіс. Ми проводимо опитування населення на різні теми. Наразі ми проводимо опитування про безпеку поведінки в мережі Інтернет. Ваші відповіді суворо конфіденційні, ми не будемо питати про ваші паролі або сайти, які ви відвідуєте. Опитування триватиме до 20 хвилин, будемо вдячні, якщо ви зможете відповісти на наші питання .

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 (F2F)**
2	18-25 років	➔ Продовжити, КВОТА N = 300 (CATI)
3	26-59 років	➔ Продовжити, КВОТА N = 300 (CATI)
4	Більше 60 років	➔ Продовжити, КВОТА N = 300 (CATI)
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 (не зачитувати!)	КІНЕЦЬ

S4. З яких пристроїв ви заходите в інтернет?

Кілька відповідей, зачитати

S5. [Якщо в S4 згадано більше одного пристрою, інакше – перенести відповідь]
З якого пристрою ви заходите в інтернет найчастіше?

Одна відповідь, із тих, що згадані в S4.

	S4.	S5.
Стаціонарний комп'ютер	1	1
Ноутбук	2	2
Планшет	3	3
Смартфон (за необхідності пояснити: телефон, на який можна встановлювати додатки, зокрема для виходу в інтернет)	4	4
Інше	5	5
Важко відповісти (не зачитувати!)	99 → КІНЕЦЬ	99 → КІНЕЦЬ

S6. [Якщо S5 =1 або 2]

Уточніть, будь ласка, цей комп'ютер/ноутбук належить вам особисто?

Одна відповідь, зачитати за необхідності

1	Так, це мій особистий комп'ютер / ноутбук (користуюся лише я)
2	Комп'ютер / ноутбук належить родині, користуюся я та інші члени сім'ї
3	Комп'ютер / ноутбук належить роботодавцю, компанії, школі, навчальному закладу
4	Інше: записати _____
99	Важко відповісти (не зачитувати!) → КІНЕЦЬ

ОСНОВНИЙ ОПИТУВАЛЬНИК

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

Зачитати альтернативи. Одна відповідь у рядку.

Програміст: РОТАЦІЯ РЯДКІВ		Щодня	Кілька разів на тиждень	Раз на тиждень	Раз на місяць	Кілька разів на рік	Ніколи	ВВ (не зачитувати)
1	Заходите на сторінки, читаєте стрічки соціальних мереж (такі як Тік Ток, Фейсбук, Інстаграм)	1	2	3	4	5	6	99
2	Дописуєте або розміщуєте фотографії в соціальних мережах	1	2	3	4	5	6	99
3	Купуєте товари в інтернет-магазинах (в тому числі у соціальних мережах, таких як Фейсбук, Інстаграм)	1	2	3	4	5	6	99
4	Сплачуєте за товари або послуги банківською карткою через інтернет	1	2	3	4	5	6	99
5	Користуєтеся інтернет-банкінгом (переказуєте кошти, переглядаєте залишок на рахунку, управляєте рахунками)	1	2	3	4	5	6	99
6	Завантажуєте відео, музику, статті, книги, інші матеріали	1	2	3	4	5	6	99

7	Підключаєтеся до публічних вай-фай мереж (в кафе, публічних місцях)	1	2	3	4	5	6	99
8	Користуєтеся електронною поштою	1	2	3	4	5	6	99
9	Користуєтеся месенджерами (Вайбер, Телеграм, Вотсап, Фейсбук)	1	2	3	4	5	6	99
10	Користуєтеся ВіПіЕн (наприклад, для доступу на сайти, які заблоковано)	1	2	3	4	5	6	99
11	Граєте в ігри онлайн	1	2	3	4	5	6	99
12	Робите покупки з ігрових акаунтів	1	2	3	4	5	6	99
13	Завантажуєте безкоштовні програми, ігри	1	2	3	4	5	6	99
14	Встановлюєте різні програми, доповнення до браузерів	1	2	3	4	5	6	99

A1.2 **[Якщо відповіді «1..4» обрані для наступних тверджень в A1: 6, 13, 14]**

Коли ви завантажуєте матеріали, програми, ігри, як ви перевіряєте, що ресурс надійний?

Не зачитувати! Можна кілька відповідей

1	Ніяк не перевіряєте, просто завантажуєте, і все
2	Завантажуєте лише з офіційних ресурсів
3	Давно користуєтеся цими ресурсами, тож упевнені в їхній надійності
4	Інше: записати _____
99	Важко відповісти (не зачитувати!)

A2. 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
Важко відповісти (не зачитувати!)	99	99

А3. 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.

Програміст: РОТАЦІЯ РЯДКІВ		Це точно про мене	Частково про мене	Це точно НЕ про мене	ВВ (не зачитувати)
1	У мене простий пароль, тому що я боюся забути складний	1	2	3	99
2	У мене один пароль на все, щоб завжди його пам'ятати	1	2	3	99
3	Друзі або рідні знають мої паролі на випадок, якщо я забуду	1	2	3	99
4	Я не розумію, навіщо створювати різні паролі	1	2	3	99
5	Я не цікавий(-а) для інтернет-шахраїв	1	2	3	99
6	Якщо є антивірус, то мені нічого не загрожує	1	2	3	99
7	Я відкриваю електронні листи і вкладення навіть з невідомих мені адрес електронної пошти або від незнайомців у месенджері	1	2	3	99
8	Я можу вставити чужу або незнайому флешку у свій комп'ютер	1	2	3	99
9	Я можу випадково «засвітити» дані банківської картки, паспорту, к'ю-ар коди квитків у соціальних мережах	1	2	3	99
10	Я використовую двофакторну автентифікацію, навіть якщо цього не вимагає політика безпеки сайту (наприклад, банківські додатки) * для групи 11-17 років додати інструкцію. *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.*	1	2	3	99
11	Я регулярно роблю резервні копії документів, фотографій – для захисту даних	1	2	3	99
12	Я відвідую російські сайти (які закінчуються на «крапка РУ»)	1	2	3	99
13	Я маю поштові електронні скриньки на російських поштових серверах	1	2	3	99
14	Я відвідую заблоковані в Україні російські ресурси та соціальні мережі (такі як Яндекс, Вконтакті)	1	2	3	99

15	З російських ресурсів (точка РУ) я іноді завантажую файли, ігри або програми, заповнюю там анкети, реєструюсь чи вношу певні дані	1	2	3	99

А4. 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.

Програміст: РОТАЦІЯ РЯДКІВ		Траплялося з вами особисто	Траплялося із вашими реальними знайомими	Траплялося із вашими віртуальними знайомими	Чули про це, але із знайомими не траплялося	Навіть не чули про таке	ВВ (не зачитувати)	Увага, програміст: Виводити альтернативи відповідно до вікових груп **S1 = …**			
								1	2	3	4
1	Крадіжка (злам) облікових записів у соціальних мережах	1	2	3	4	5	99	x	x	x	
2	Крадіжка (злам) ігрових акаунтів у комп'ютерних іграх	1	2	3	4	5	99	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) **[Формулювання для S1 =2,3,4]** Вимагання паролів до облікових записів акаунтів, електронних поштових скриньок з використанням методів соціальної інженерії (маніпуляцій, погроз, шантажу)	1	2	3	4	5	99	x	x	x	x
4	Люди стають жертвами кібершахраїв на онлайн-аукціонах	1	2	3	4	5	99		x	x	
5	Вимагання особистих даних через телефон, месенджери, поштові скриньки, облікові записи у соціальних мережах	1	2	3	4	5	99			x	x
6	Вимагання банківських даних, паролів та доступу до облікових записів	1	2	3	4	5	99			x	x

	банківських мобільних додатків, банківських рахунків (у т.ч. через телефон, месенджери)										
7	Вимагання грошей задля розблокування роботи комп'ютерних систем та ґаджетів (електронних пристроїв)	1	2	3	4	5	99			x	
8	Вимагання службових даних від працівників державних або комерційних компаній	1	2	3	4	5	99			x	
9	Кібершахраї вимагають гроші, використовуючи методи соціальної інженерії (маніпуляції, погрози, шантаж), а також особисті та родинні дані (через телефон та месенджери)	1	2	3	4	5	99				x

A5. Чи була у вас ситуація, коли вам здавалося, що ви стикалися зі зловмисними діями під час користування цифровими пристроями, але ви не можете точно сказати, що це було?

1	Ні	
2	Так, протягом останніх трьох місяців	→ Уточніть, будь ласка:
3	Так, раніше	_____
99	ВВ (не зачитувати)	

A6. Ви сказали, що деякі загрозливі ситуації траплятися з вами особисто. Уточніть, будь ласка, коли саме це трапилося останній раз?

Зачитати альтернативи. Одна відповідь у рядку.

Програміст: РОТАЦІЯ РЯДКІВ		Протягом останніх 3 місяців	Протягом року, але більше 3 місяці тому	Більше року тому	ВВ (не зачитувати)
1	Увага, програміст: Виводити альтернативи для яких **A4 =1**	1	2	3	99
2		1	2	3	99
…		1	2	3	99

A7. Наскільки ви почуваєтеся захищеними щодо деяких загроз? Ви можете відповісти «Почуваюся повністю захищеним»; «Не завжди почуваюся захищеним» або «Почуваюся беззахисним».

Зачитати альтернативи. Одна відповідь у рядку.

Програміст: РОТАЦІЯ РЯДКІВ		Почуваюся повністю захищеним	Не завжди почуваюся захищеним	Почуваюся беззахисним	ВВ (не зачитувати)
1	Увага, програміст: Виводити альтернатив, для яких A4={1..4}	1	2	3	99
2		1	2	3	99
..		1	2	3	99

0.1 [Якщо в 0 є відповіді 2 або 3] Ви сказали що інколи почуваєтеся не повністю захищеним щодо кіберзагроз. Наскільки ви готові вживати правила кібергігієни, щоб вберегтися від цих загроз? Оцініть за шкалою від 1 до 5, де 1 – «не готові вживати жодних правил», а 5 – «готові вживати всі необхідні правила захисту»

1	2	3	4	5	ВВ=99

A8. 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.

Програміст: РОТАЦІЯ РЯДКІВ		Вперше чую	Знаю, але не дотримуюся	Знаю і дотримуюся інколи	Знаю і завжди	ВВ (не зачитувати)	Увага, програміст: Виводити альтернативи відповідно до вікових груп S1 =			
							1	2	3	4
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, звикайте користуватись менеджерами паролів [Формулювання для S1 =2,3,4] Використовуйте складні паролі і не використовуйте одні і ті ж самі паролі для	1	2	3	4	99	x	x	x	x

	реєстрації на онлайн-ресурсах, в банківських системах тощо, звикайте користуватись менеджерами паролів.									
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	1	2	3	4	99	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	1	2	3	4	99	x	x	x	x
4	Не відправляйте ваші контактні телефони, особисті фото незнайомцям, особливо тим, які просять оголені фотографії	1	2	3	4	99	x			
5	Не встановлюйте на ваші ґаджети додатки та програми з неофіційних магазинів	1	2	3	4	99	x	x	x	x
6	Не підключайтеся до загальнодоступних, невідомих або незахищених мереж Wi-Fi	1	2	3	4	99	x	x	x	x
7	У разі вимагання паролів, даних, фото незнайомцями або отримання сумнівних повідомлень, негайно повідомте батьків	1	2	3	4	99	x			
8	Регулярно оновлюйте ваші пристрої. За можливості, увімкніть автоматичне оновлення всіх програм	1	2	3	4	99		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	1	2	3	4	99		x	x	
10	Завжди створюйте резервні копії важливих даних на окремому локальному пристрої чи хмарному сховищі	1	2	3	4	99		x	x	
11	За можливості, використовуйте двофакторну аутентифікацію	1	2	3	4	99		x	x	
12	Не залишайте ваш пристрій без нагляду, особливо коли він працює у публічних місцях	1	2	3	4	99		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	1	2	3	4	99		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	1	2	3	4	99				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	1	2	3	4	99				x

A9. 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	ВВ=99

A10. Які джерела інформації ви використовуєте, щоб дізнатися про правила безпечної поведінки в інтернеті?

A11. [Якщо в A10 згадано більше одного джерела] Якому з цих джерел інформації ви довіряєте найбільше?

Зачитати за необхідності, одна відповідь із тих, що згадані в A10

	A10	A11
Спеціалізовані джерела, сайти, форуми	1	1
Люди, яких я вважаю фахівцями (наприклад, системний адміністратор на роботі, в школі, в університеті)	2	2
Друзі, родичі, знайомі, які знаються на темі більше за мене	3	3
Соціальні мережі	4	4
Інтернет (окрім соціальних мереж)	5	5
Традиційні ЗМІ (телебачення, газети, радіо)	6	6
Блогери та/або лідери суспільної думки	7	7
Жодне	8	8
Банери, білборди, сітілайти, реклама в транспорті	9	9
Інше (записати _____)	98	98
Важко відповісти (не зачитувати!)	99	99

A12. [Якщо A10 = 7] Яких саме блогерів та/або лідерів суспільної думки ви вважаєте джерелом інформації про безпечну поведінку в інтернеті?

Запишіть: _____

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	Важко відповісти (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, пилосос, 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	Важко відповісти (не зачитувати!)

Це всі питання.

Подякуйте респондентові за участь в опитуванні!

VII Додаток 3. Портрет респондента

		TOTAL		Вік респондента							
				11-17 років		18-25 років		26-59 років		Більше 60 років	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Стать	Чоловік	570	47,47%	154	51,38%	159	52,94%	212	47,02%	65	43,17%
	Жінка	630	52,53%	146	48,62%	141	47,06%	238	52,98%	85	56,83%
	TOTAL	1200	100,00%	300	100,00%	300	100,00%	450	100,00%	150	100,00%
Регіон	Київ	98	8,20%	22	7,42%	24	8,04%	38	8,43%	12	8,07%
	Північ	162	13,46%	38	12,78%	39	13,12%	64	14,11%	18	12,02%
	Захід	295	24,55%	84	27,89%	83	27,54%	105	23,25%	37	24,77%
	Центр	290	24,14%	73	24,37%	71	23,63%	109	24,12%	37	24,35%
	Південь	206	17,19%	49	16,34%	50	16,58%	80	17,79%	24	16,22%
	Схід	149	12,45%	34	11,19%	33	11,08%	55	12,30%	22	14,56%
	TOTAL	1200	100,00%	300	100,00%	300	100,00%	450	100,00%	150	100,00%
Розмір населеного пункту (тис. жителів)	Село	352	29,29%	102	34,07%	102	34,03%	128	28,45%	39	26,11%
	0-50	247	20,61%	63	21,11%	57	19,04%	94	20,90%	30	20,30%
	51-500	299	24,91%	64	21,41%	68	22,79%	111	24,76%	43	28,89%
	500+	302	25,19%	70	23,41%	72	24,14%	117	25,90%	37	24,70%
	TOTAL	1200	100,00%	300	100,00%	300	100,00%	450	100,00%	150	100,00%

		TOTAL		Вік респондента							
				11-17 років		18-25 років		26-59 років		Більше 60 років	
Основний рід занять	Працюю за наймом	445	37,04%	0	0,00%	103	34,25%	233	51,68%	24	16,07%
	Зареєстрований приватний підприємець	82	6,81%	0	0,00%	25	8,20%	40	8,97%	5	3,50%
	Самозайнятий	58	4,82%	0	0,00%	20	6,66%	28	6,17%	4	2,54%
	Студент / учень	176	14,68%	299	99,63%	74	24,68%	1	0,23%	0	0,00%
	Веду домашнє господарство	111	9,25%	1	0,37%	33	10,94%	59	13,03%	3	1,97%
	Пенсіонер	225	18,73%	0	0,00%	3	1,10%	36	8,06%	112	74,96%
	Тимчасово не працюю, але шукаю роботу	94	7,82%	0	0,00%	38	12,50%	48	10,71%	1	0,96%
	Інше	4	0,30%	0	0,00%	1	0,49%	2	0,41%	0	0,00%
	Важко сказати	7	0,56%	0	0,00%	4	1,18%	3	0,73%	0	0,00%
	TOTAL	1200	100,00%	300	100,00%	300	100,00%	450	100,00%	150	100,00%
Місце навчання	У школі	120	67,96%	251	84,08%	0	0,00%	0	0,00%	0	0,00%
	В професійно-технічному навчальному закладі	8	4,27%	12	3,91%	5	6,10%	0	0,00%	0	0,00%
	В коледжі	14	7,69%	18	5,91%	12	15,94%	0	0,00%	0	0,00%
	В вищому навчальному закладі	35	20,08%	18	6,11%	58	77,96%	1	100,00%	0	0,00%
	Інше	0	0,00%	0	0,00%	0	0,00%	0	0,00%	0	0,00%
	TOTAL	176	100,00%	299	100,00%	74	100,00%	1	100,00%	0	0,00%

		TOTAL		Вік респондента							
				11-17 років		18-25 років		26-59 років		Більше 60 років	
Рівень освіти	Немає початкової освіти	1	0,08%	2	0,71%	0	0,00%	0	0,00%	0	0,00%
	Початкова середня освіта	80	6,65%	159	53,07%	1	0,23%	2	0,33%	1	0,58%
	Базова загальна середня	82	6,83%	105	35,03%	10	3,22%	17	3,69%	1	0,74%
	Повна загальна середня	129	10,78%	16	5,37%	41	13,62%	57	12,68%	10	6,59%
	Спеціальна середня освіта	311	25,94%	5	1,58%	61	20,30%	128	28,52%	55	36,76%
	Неповна вища/початкова вища	61	5,09%	13	4,25%	51	16,87%	16	3,66%	5	3,26%
	Вища освіта, бакалаврат	124	10,31%	0	0,00%	82	27,20%	46	10,20%	11	7,39%
	Вища освіта, магістратура	407	33,91%	0	0,00%	52	17,37%	183	40,64%	66	44,10%
	Важко відповісти	5	0,39%	0	0,00%	4	1,18%	1	0,27%	1	0,58%
	TOTAL	1200	100,00%	300	100,00%	300	100,00%	450	100,00%	150	100,00%
Фінансове становище сім'ї	Змушені економити на харчуванні	119	9,94%	1	0,49%	17	5,61%	43	9,50%	30	19,94%
	Для придбання одягу, взуття необхідно заощадити або позичити	218	18,15%	18	5,92%	29	9,62%	83	18,39%	45	30,23%
	Для таких покупок як гарний костюм, мобільний телефон, необхідно заощадити або позичити	266	22,18%	133	44,18%	69	23,14%	87	19,22%	25	16,84%
	Для придбання речей, які дорого коштують необхідно заощадити або позичити	280	23,37%	66	21,99%	71	23,56%	122	27,10%	18	12,32%
	Для таких покупок як машина, квартира необхідно заощадити або позичити	189	15,78%	38	12,79%	63	20,99%	72	15,95%	21	14,14%
	Будь-які необхідні покупки можу зробити в будь-який час	52	4,31%	5	1,52%	29	9,58%	21	4,64%	3	1,95%
	Важко відповісти	75	6,28%	39	13,12%	23	7,50%	23	5,20%	7	4,58%
	TOTAL	1200	100,00%	300	100,00%	300	100,00%	450	100,00%	150	100,00%