ХМЕЛЬНИЦЬКИЙ ОБЛАСНИЙ ІНСТИТУТ
ПІСЛЯДИПЛОМНОЇ ПЕДАГОГІЧНОЇ ОСВІТИ

Безпека в цифровому суспільстві та освітньому середовищі

Олександра СОЛОГУБ

2023

ХМЕЛЬНИЦЬКИЙ ОБЛАСНИЙ ІНСТИТУТ
ПІСЛЯДИПЛОМНОЇ ПЕДАГОГІЧНОЇ ОСВІТИ

Безпека в цифровому суспільстві та освітньому середовищі

Олександра СОЛОГУБ

2023

УДК 004.9:373.3(07)

Сологуб О. С. Безпека в цифровому суспільстві та освітньому середовищі /О. С. Сологуб. – Хмельницький: ОІППО, 2023. - 43 с.

Рецензенти:
Григорук Павло Михайлович, завідувач кафедри економіки, аналітики, моделювання та інформаційних технологій в бізнесі Хмельницького національного університету, доктор економічних наук, професор

Ребрина Віталій Арсенович, старший викладач кафедри теорії та методик природничо-математичних дисциплін та технологій Хмельницького обласного інституту післядипломної педагогічної освіти

Рекомендовано до друку рішенням вченої ради Хмельницького ОІППО (протокол № 2 від 4 липня 2023 року)

У посібнику розглядається питання безпеки в цифровому суспільстві та освітньому середовищі, зокрема кіберзезпеки та кібергігієни, основних видів кіберзагроз, захисту персональних даних, надійності джерел і достовірності даних, а також ролі педагогічного працівника в організації безпечного цифрового освітнього середовища.

Посібник призначений для педагогічних працівників закладів загальної середньої освіти, викладачів курсу з розвитку цифрової компетентності педагогів установ післядипломної педагогічної освіти, а також може бути корисним усім громадянам, які мають бажання підвищити свій рівень кіберграмотності.

Зміст

Вступ

В умовах введення воєнного стану в Україні особливої уваги заслуговує питання інформаційної безпеки учасників освітнього процесу. Масові дезінформаційні кампанії, інформаційна політика країни-агресора, соціальні мережі як суб'єкти впливу в інформаційному просторі, низький рівень інформаційної культури та медіаграмотності суспільства, – все це призводить до підвищення рівня інформаційної загрози як держави в цілому, так і її громадян.

У січні 2023 року в перший день роботи Всесвітнього економічного форуму в Давосі розглядалося питання “Кіберпандемія: потреба в посиленні кіберстійкості телекомунікацій”. Було зазначено, що через геополітичну нестабільність, кібертероризм та кібервійну невідворотним стає щоденне зростання кіберзлочинності. Тому важливою є кіберстійкість - здатність організації забезпечити розвиток власної діяльності за рахунок готовності до кіберзагроз, можливості реагування на них. Важко знайти організацію, працівники якої можуть з упевненістю сказати, що вони на 100 % захищені від кіберзагроз, навіть за умови функціонування структурного підрозділу, що опікується питанням безпеки. Наприклад, 14 січня 2022 року масштабної хакерської атаки зазнали портал Кабміну, ДСНС, Міносвіти, Мінспорту, Міненерго, Мінагрополітики, Мінстратегпрому, Держказначейства тощо. Тому в закладі освіти, де за безпеку в більшості випадків відповідає одна людина, кіберстійкість має бути результатом спільної роботи усіх педагогічних працівників, кожен з яких повинен з відповідальністю ставитись до цього питання та дотримуватись принципів кібергігієни.

У Стратегії кібербезпеки України, затвердженої Указом Президента України 26 серпня 2021 року за № 447/2021, перелічені виклики для України у сфері кібербезпеки:

- активне використання кіберзасобів у міжнародній конкуренції;
- розвиток засобів кібербезпеки в умовах швидких прогресуючих змін в цифрових технологіях;
- мілітаризація кіберпростору та розвиток кіберзброї для

прихованих атак та розвідувально-підривної діяльності;
- вплив пандемії COVID-19 на стрімкий розвиток суспільних відносин із використанням ІКТ;
- упровадження цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки [1].

Кіберзагрози та шляхи захисту від них

Розглянемо основні поняття, що стосуються кібербезпеки.

Кібербезпека - стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.

Кібергігієна — це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації.

Кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів.

Зростання кіберзагроз відбувається в усьому світі. Наприклад, у 2020 році 97% компаній у світі були атаковані хакерами, зокрема 607 японських організацій — від готелів і держустанов до криптокомпаній; щомісяця британські спеціалісти відбивали 3 мільйони атак на електронні адреси чиновників; в Ізраїлі фахівці досі оговтуються після атаки на 85 тисяч серверів, звідки викрали 250 тисяч баз даних. У 2022 році 61% з усіх зафіксованих у світі кібератак було здійснено проросійськими хакерськими групами.

Кіберінцидентами в Україні опікується Державна служба спеціального зв'язку та захисту інформації України (сайт https://cip.gov.ua/ua), зокрема урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA та Державний центр кіберзахисту, які досліджують інциденти, надають допомогу та рекомендації з питань протидії кіберзагрозам, накопичують та проводять аналіз даних про

кіберзагрози. Впродовж 2022 року Державним центром кіберзахисту було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2021 році. Кількість подій інформаційної безпеки в категорії «Шкідливий програмний код» зросла аж у 18,3 рази, на другому місці знаходиться категорія «Збір інформації зловмисником», кількість подій в якій зросла у 2,2 рази (рис. 1) [2].

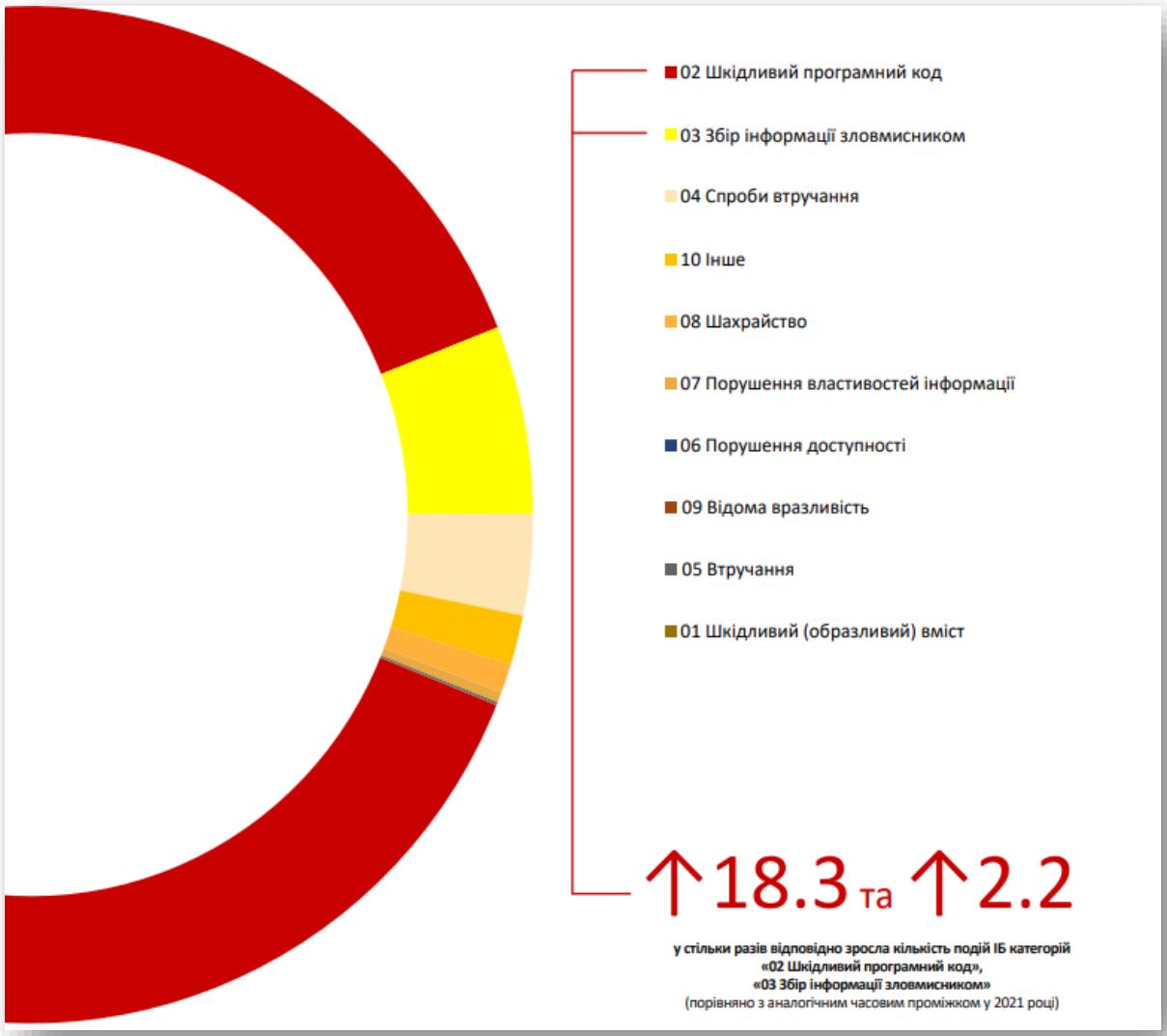


Рис.1. Статистика зростання подій інформаційної безпеки у 2022 році порівняно з 2021 роком

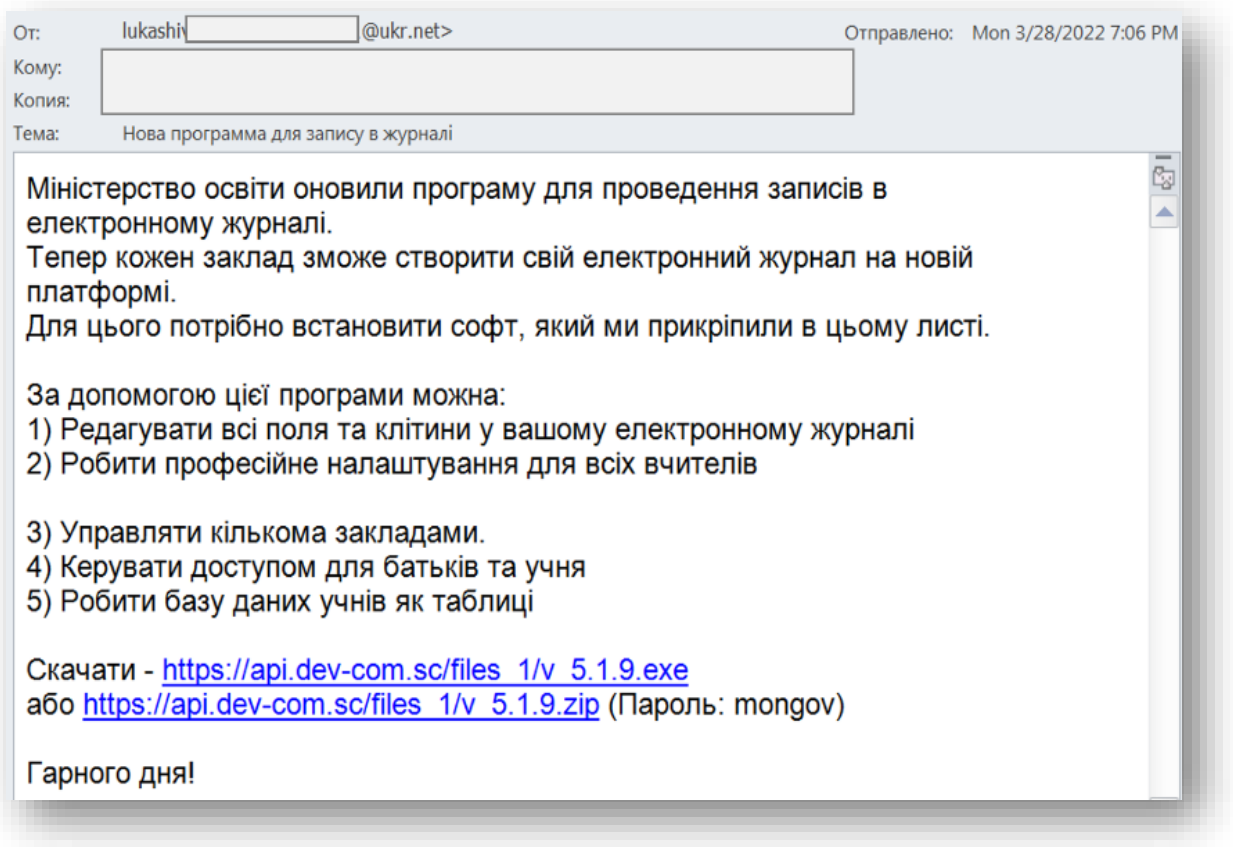
Розглянемо детальніше кіберінциденти в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником», що є найбільш поширеними.

Шкідливий програмний код - це код, що завдає шкоду комп'ютеру чи системі. Поширеним типом такого коду є вірус – невелика програма, яка приєднується до інших програм або файлів, може копіювати себе в комп’ютер і навіть поширюватися на інші комп'ютерні мережі. Шкідливий код може або активувати себе або вимагати від користувача дії, наприклад, натискання на щось або відкриття вкладення електронної пошти.

Найчастіше шкідливі програмні коди поширюються електронною поштою, тому розглянемо, як аналізувати листи. Наприклад, урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA 30 березня 2022 року опублікувала на своєму сайті інформацію https://cert.gov.ua/article/38606 про виявлення масового розповсюдження серед громадян України, в тому числі працівників організацій, електронних листів з темою «Нова програма для запису в журнал». Текст листа містив повідомлення начебто від Міністерства освіти та науки України з покликанням на архів «програми» або файлами та паролем до архіву (рис. 2). Якщо особа завантажувала на комп’ютер програму та запускала EXE-файл, комп'ютер інфікувався шкідливою програмою, яку за сукупністю ознак класифіковано як MarsStealer. Метою такої програми є збір інформації про комп'ютер, викрадення автентифікаційних даних з браузерів, викрадення файлів, завантаження і запуск виконуваних файлів, виготовлення знімку екрану тощо.

Найбільше хакерів цікавить особиста інформація, дані платіжної картки, інтелектуальна власність (неопублікований контент), будь-які конфіденційні дані, які погано захищені. До найпоширеніших тем зловмисних листів відносять такі:

- до Вашого облікового запису отримано доступ;
- терміново сплатіть податок;
- отримайте відправлення;
- привітайте близьких подарунком за низькою ціною;
- документ про доставку;
- безкоштовна послуга;
- повідомлення від кіберполіції тощо.


От: lukashiv [redacted] @ukr.net> Отправлено: Mon 3/28/2022 7:06 PM
Кому:
Копия:
Тема: Нова программа для запису в журналі

Міністерство освіти оновили програму для проведення записів в електронному журналі.
Тепер кожен заклад зможе створити свій електронний журнал на новій платформі.
Для цього потрібно встановити софт, який ми прикріпили в цьому листі.

За допомогою цієї програми можна:
1) Редагувати всі поля та клітини у вашому електронному журналі
2) Робити професійне налаштування для всіх вчителів

3) Управляти кількома закладами.
4) Керувати доступом для батьків та учня
5) Робити базу даних учнів як таблиці

Скачати - https://api.dev-com.sc/files_1/v_5.1.9.exe
або https://api.dev-com.sc/files_1/v_5.1.9.zip (Пароль: mongov)

Гарного дня!

Рис.2. Зразок зловмисного листа, що розсилався освітянам

У разі виявлення подібних повідомлень команда реагування на комп'ютерні надзвичайні події України CERT-UA рекомендує не відкривати файлів та негайно повідомити про це на пошту cert@cert.gov.ua.

Проаналізуйте лист на рис. 2 за допомогою чек-листа нижче.

Чек-лист «Аналізуємо листи електронної пошти»

При отриманні листа звертаємо увагу на:

- адресу відправника (урядові структури мають скриньки із закінченням на «gov.ua»);
- дату та час відправлення (зловмисники зазвичай відправляють листи у вихідний день, в нічний час);
- текст листа (наявність помилок, невідформатоване повідомлення тощо);

- наявність архівів (розширення «zip»), файлів з розширенням «exe» (найнебезпечніші файли) або покликань на архів на хмарних сервісах, навіть безпечні на перший погляд файли з розширенням «docx», «pdf», адже вони можуть містити макроси та інші небезпеки;
- наявність прізвища, імені та по-батькові контактної особи, його посади (зловмисники не вказують такої інформації);
- покликання, на яке пропонують перейти, особливо для введення особистої інформації;
- безкоштовні чи дешеві послуги;
- неперсоналізоване звернення у листі «шановний клієнте» тощо (зловмисники, рекламодавці мають базу адрес, але не знають, кому відправляють повідомлення);
- емоційне забарвлення тексту листа, що викликає паніку, поспіх, страх, через що користувач не встигає проаналізувати лист.

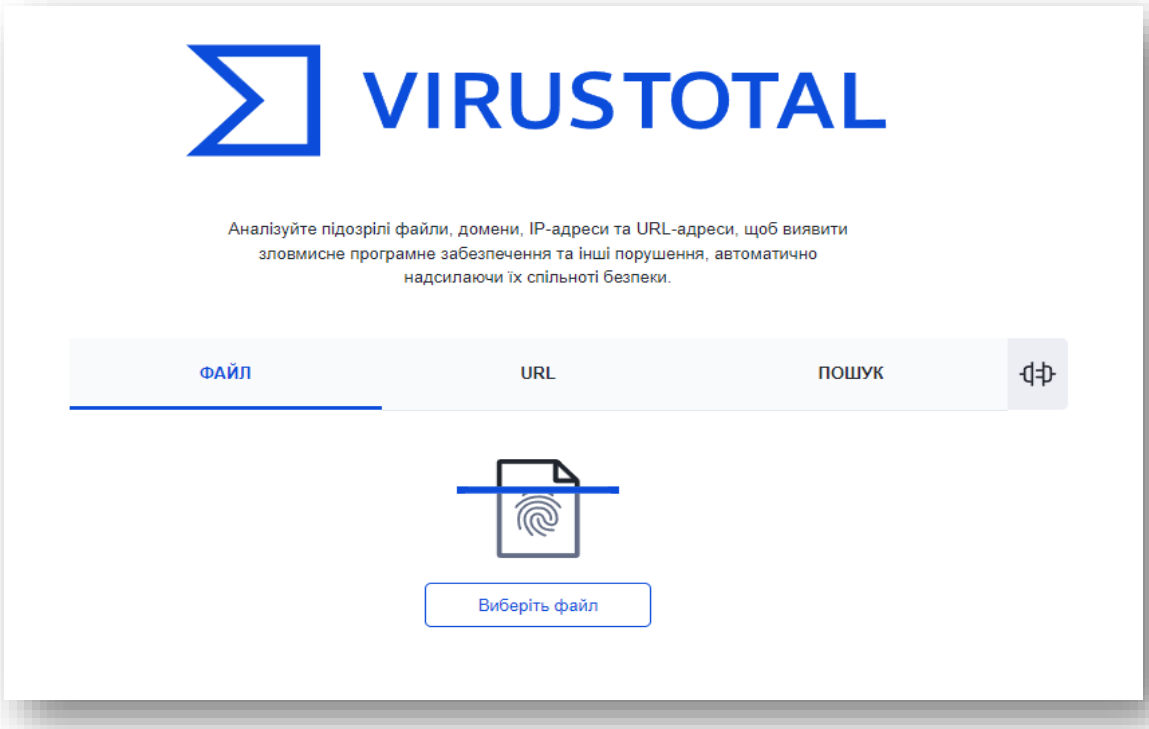


Рис. 3. Головна сторінка сервісу VirusTotal

Для перевірки підозрілих файлів та покликань Держспецзв'язку рекомендує використовувати сервіс VirusTotal (https://www.virustotal.com/), за допомогою якого відбувається одночасне сканування їх за допомогою понад 70 антивірусних сканерів і служб (рис. 3). Аналізуючи підозрілі файли, домени, IP-

адреси та URL-адреси, щоб виявити зловмисне програмне забезпечення та інші порушення, Ви автоматично надсилаєте їх спільноті безпеки, покращуючи таким чином роботу сервісу

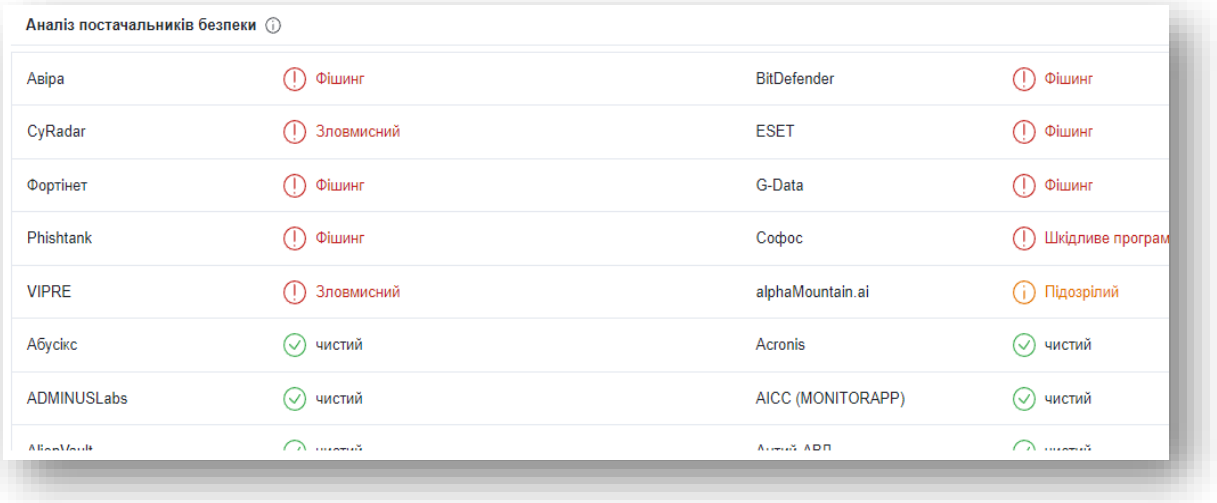


Рис. 4. Результат перевірки URL-адреси за допомогою сервісу VirusTotal

Щоб скористатись даним сервісом, необхідно обрати одну із трьох вкладок:

- «Файл» для перевірки файлу з комп'ютера, якщо користувач підозрює, що він може бути шкідливий;
- «URL», якщо користувачу пропонують перейти за покликанням в електронному листі, повідомленнях у месенджерах тощо, в такому випадку можна перевірити URL-адресу покликання;
- «Пошук» для пошуку хеша, домена, IP-адреси чи URL-адреси.

За результатами перевірки кожна служба (постачальник безпеки) надає звіт (рис.4). Також є можливість встановити від авторів даного сервісу розширення VT4Browsers для браузерів. Дане розширення дає можливість перевіряти покликання безпосередньо в електронних листах. Для цього після його встановлення достатньо клацнути правою кнопкою миші на покликанні в листі та в контекстному меню обрати VT4Browsers\ Scan selected link (рис. 5). Крім того, якщо користувач буде завантажувати будь-які файли з листа, розширення надаватиме звіт про те, чи є цей файл безпечним.

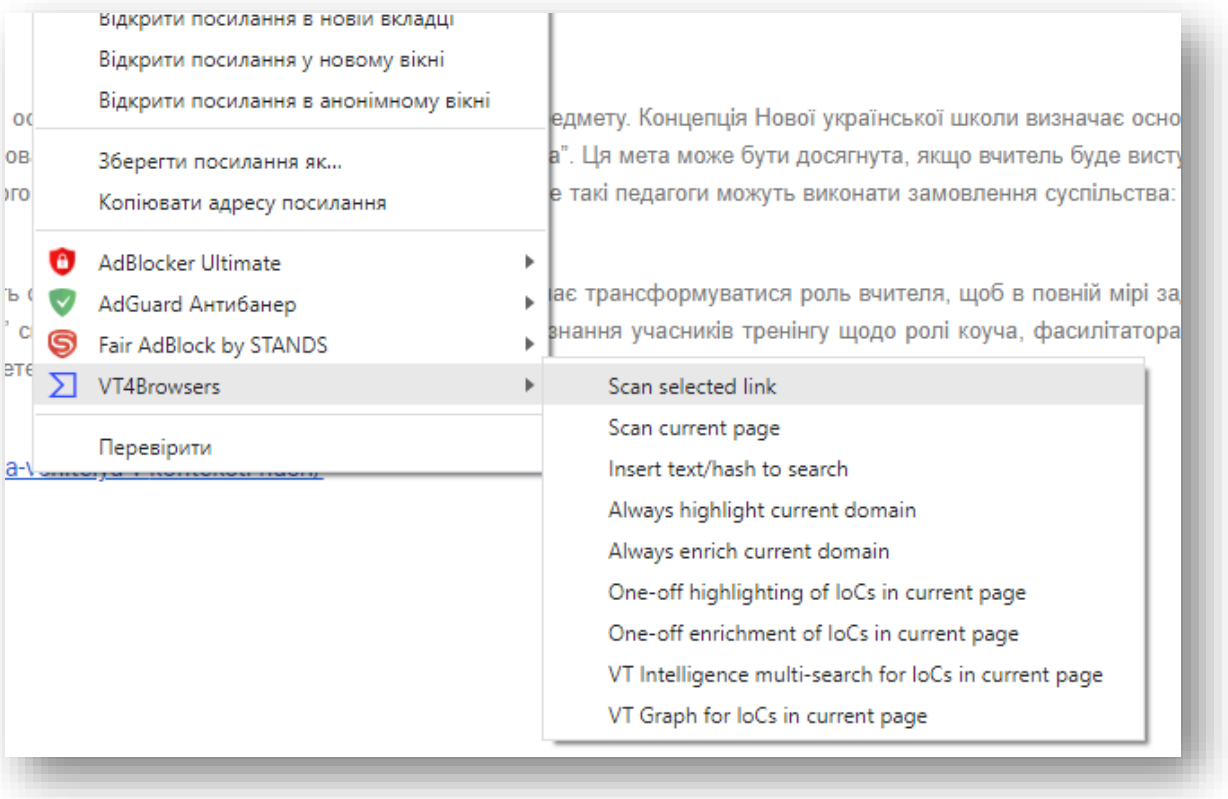


Рис. 5. Сканування покликання в листі засобами розширення VT4Browsers

На даний час таке розширення розроблене для браузерів:

- Google Chrome (http://surl.li/gktmg);
- Mozilla Firefox (https://addons.mozilla.org/en-US/firefox/addon/vt4browsers/);
- Internet Explorer (https://www.virustotal.com/static/bin/vtExplorer.exe).

Алгоритм їх встановлення складається з таких кроків (розглянемо на прикладі Google Chrome):

- перейти у веб-магазин Chrome і знайти потрібне розширення, наприклад, VT4Browsers;
- ознайомитись із вкладкою «Забезпечення конфіденційності», зокрема з інформацією про те, чи збирає розширення дані користувача, і якщо так, то які;
- натиснути на кнопку «Додати в Chrome». Після цього

розширення можна знайти в переліку встановлених розширень за допомогою піктограми у вигляді пазлу у верхньому правому кутку екрану та відобразити потрібне розширення, прикріпивши його.

Перегляньте відео, як користуватись сервісом VirusTotal та розширенням VT4Browsers за покликанням http://surl.li/gkxgn або QR-кодом.

Ще один тип розширень для безпеки користувачів інтернету - це розширення від шпигунських дій та реклами. Серед них для браузера Chrome найпоширенішими є AdGuard Антибанер, AdBlocker Ultimate та Fair AdBlocker. До їх функцій належить:

- блокування реклами включно з YouTube, анімованої реклами, небажаних виринаючих вікон, банерів і текстових оголошень (включно з рекламою на Facebook);
- прискорення завантаження сторінок, економія трафіку, уникнення завантаження реклами і виринаючих вікон;
- захист приватних даниих користувача, блокування сторонніх систем стеження за його діями в інтернеті;
- блокування шпигунських та рекламних програм;
- захист від зловмисних програм та шахрайства.

Перегляньте відео, як встановити розширення AdGuard Антибанер, за покликанням http://surl.li/gkxfb або QR-кодом.

Збір інформації зловмисником. Розглянемо детальніше кіберінцидент в категорії «Збір інформації зловмисником», який розміщений на другому місці за поширенням за 2022 рік: кількість таких інцидентів порівняно з 2021 роком зросла у 2,2 рази.

Найпоширенішим засобом уведення в оману в мережі Інтернет є фішинг. Фі́шинг (англ. *phishing* від *fishing* — риболовля) — вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані. Користувач думає, що переходить на заявлений сайт, але фактично його перенаправляють на підставний сайт. Як правило, жертвами фішерів є клієнти банків і користувачі платіжних систем.

Особливу увагу варто звертати на доменне ім'я Інтернет-ресурсу, що запитує автентифікаційні дані, перш ніж натиснути на покликання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (facelook.com, goooogle.com тощо). В такому випадку є велика ймовірність перейти на фішингову сторінку, ззовні ідентичну справжній, та самостійно «віддати» власні дані.

Тривалість життя фішингового сайту - кілька днів, але за цей час зловмисники встигають зібрати чималий “врожай” конфіденційної інформації. Так, у 2021 році на сайті http://diia8000.gov.me/, оформленому в стилі, ідентичному сайту “Дія”, який проіснував 5 днів, користувачам пропонувалось перевірити доступність виплати у 8 тис. грн, для цього потрібно було ввести дані банківської картки. Небезпека використання цього сайту була не лише тоді, коли користувач натискав кнопку «Надіслати», але й під час введення даних на сайт через використання зловмисниками спеціального сканера, який зчитував поля введення. Зверніть увагу: сайт «Дія» розміщений на державному домені https://diia.gov.ua/.

Щоб зрозуміти, як сайти, додатки, розширення браузерів можуть збирати дані, звернемося до довідки Google (https://support.google.com/). Цілі збирання даних з користувачів можуть бути такі:

- керування обліковим записом (для налаштування облікових

записів користувачів, наприклад, щоб користувач міг створити свій обліковий запис, робити в ньому зміни, входити в додаток і підтверджувати свої облікові дані тощо);

- реклама й маркетинг (для показу рекламних оголошень, вимірювання ефективності реклами, передачі даних рекламним партнерам);
- функції додатка (для підтримки функцій додатка, авторизації користувачів);
- аналітика (для відстеження взаємодії користувача з додатком, відстеження справності додатка, виправлення помилок та збоїв, підвищення його продуктивності);
- сповіщення від розробника (для надсилання інформації про нові функції додатка, оновлення його системи безпеки);
- запобігання шахрайству, безпека й відповідність вимогам (для виявлення потенційних шахрайських дій шляхом невдалих спроб входу в додаток);
- персоналізація (для показу у додатку персоналізованих рекомендацій, наприклад, пропонування музичних творів на основі уподобань, місцевих новин тощо).

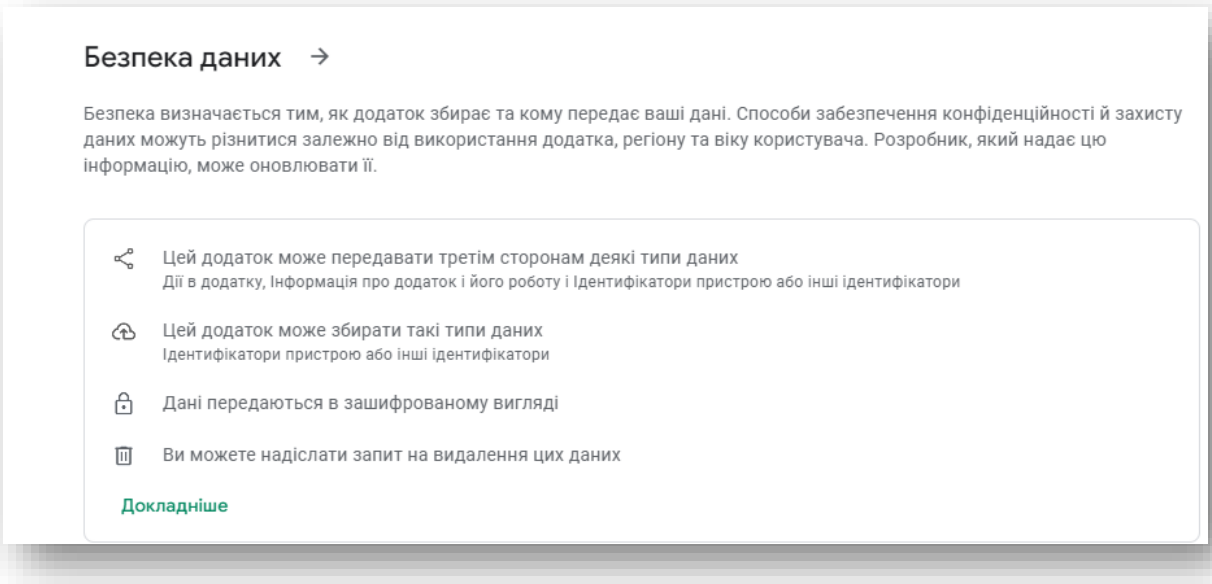


Рис.6. Розділ “Безпека даних” одного з додатків у Google Play

Про те, як перевірити, яку інформацію збирає певне розширення для браузера, ми вже з’ясовували. Для того, щоб перевірити це для

додатків, які Ви встановлюєте на мобільний телефон, необхідно знайти відповідний додаток у https://play.google.com/ та ознайомитись із розділом “Безпека даних” (рис 6).

Аналіз інтернет-ресурсів. Алгоритм аналізу інтернет-ресурсу складається з двох основних кроків:

- аналіз URL-адреси ресурсу;
- аналіз контенту, розміщеного на ресурсі.

Перший крок. Аналізуємо URL-адресу ресурсу, зокрема, який протокол (http, https тощо) використовує сайт та його доменне ім'я. Щоб дізнатися, чи безпечно відвідувати веб-сайт, необхідно впевнитися в тому, що сайт має сертифікат безпеки, тобто чи використовує він протокол https. В такому випадку адреса ресурсу починається саме з нього, наприклад, як сайту «Дія»: https://diia.gov.ua/. Якщо Ви використовуєте браузер Google Chrome, він сповістить Вас, коли з’єднання із сайтом буде незахищене або неконфіденційне. Для цього потрібно відкрити веб-сторінку та перевірити, який значок статусу безпеки сайту відображається ліворуч від веб-адреси:

 З’єднання безпечне

 Є додаткова інформація, або з’єднання незахищене

 З’єднання незахищене або небезпечне

Довідка Google так описує ці типи з’єднань з веб-сторінками:

- з’єднання безпечне означає, що інформація, якою Ви обмінюєтесь із сайтом, залишається конфіденційною. Але навіть якщо цей символ відображається, обачно надсилайте приватну інформацію. Кожного разу перед введенням її переконайтеся, що Ви потрібному сайті і чи не перенаправили зловмисники Вас на інший сайт;
- є додаткова інформація, або з’єднання незахищене означає, що конфіденційного з’єднання із сайтом немає. Стороння особа зможе

переглядати або змінювати інформацію, якою ви обмінюєтесь із сайтом;

- з’єднання незахищене або небезпечне. В такому випадку фахівці від Google не радять вводити конфіденційну або особисту інформацію на ресурсі і по можливості не користуватись ним. Якщо Ви бачите червоне попередження, яке відображається на всю сторінку, цей сайт позначено як небезпечний. Імовірно, використання його поставить конфіденційність Вашої інформації під загрозу.

Щоб переглянути інформацію про дозволи й захист конфіденційності для сайту, натисніть значок безпеки (рис. 7).

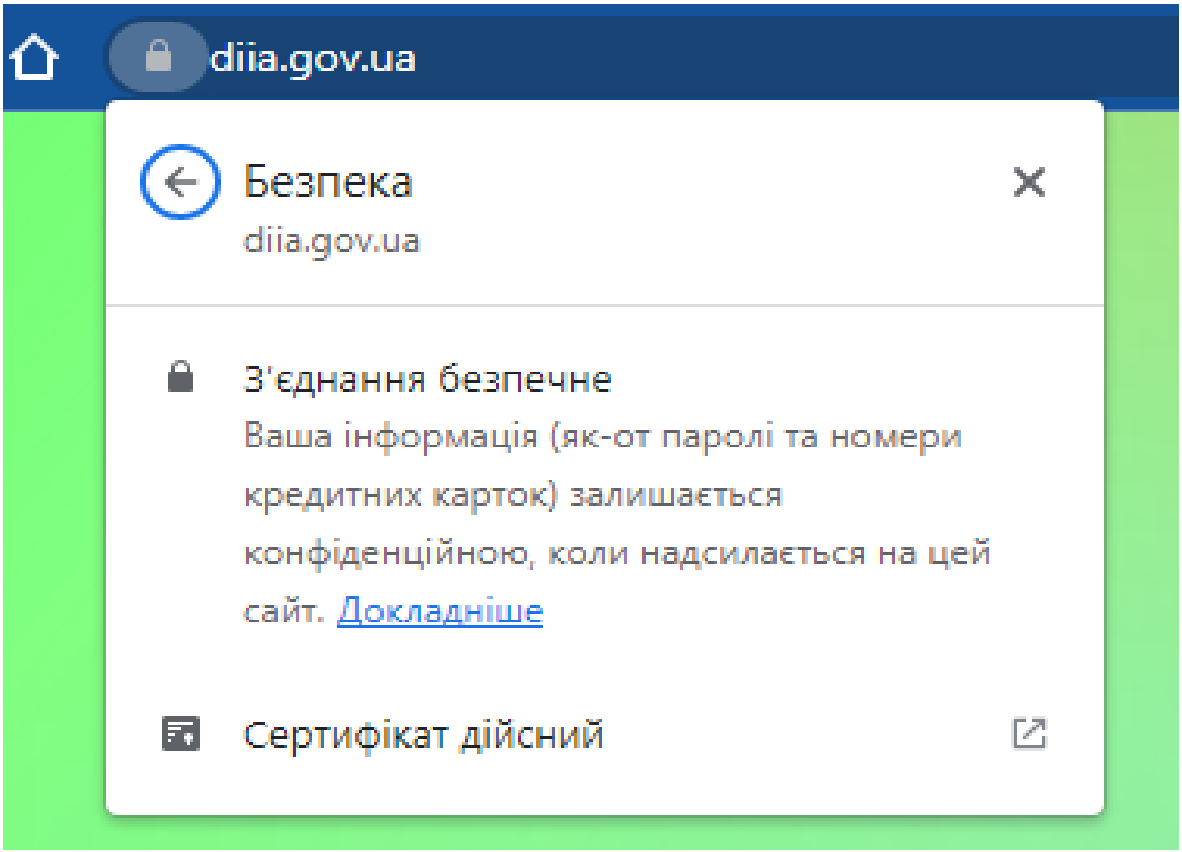


Рис. 7. Інформація про сайт, який використовує безпечне з’єднання

Крім протоколу потрібно звернути увагу в адресі сайту на його доменне ім’я. Доменне ім'я — це символьне позначення, яке служить для адресації вузлів мережі Інтернет і розташованих на них мережевих ресурсів (веб-сайтів, серверів електронної пошти, мережевих сервісів) в зручній для людини формі.

Будь-який домен складається з рівнів. Рівні домену — це частини, які ділять крапки. Рівні зазвичай рахують справа наліво. Наприклад, перший рівень домену (домен верхнього рівня) — це частина імені, яка розташована праворуч від останньої крапки. Загалом доменні імена є загальні та національні.

Загальні домени означають сферу діяльності та тип власника сайту, наприклад: .com, .biz — для комерційний підприємств та бізнес-установ, скорочено від *company*. Такі сайти зазвичай містять рекламні матеріали, а також інформацію з упередженою думкою; .org — для некомерційних організацій, скорочено від *organization*; .edu — для освітніх закладів, скорочено від *education*. Такі сайти публікують навчальні матеріали, зазвичай достовірні.

Національні домени - це домени верхнього рівня, які виділили для конкретних держав. У більшості випадків за основу національних доменів верхнього рівня брали дволітерні коди країн. Тому всі національні домени першого рівня складаються з двох літер. Наприклад, .UK означає — Велика Британія, .UA — Україна, .FR — Франція тощо. Для органів державної влади України призначений спеціальний національний домен GOV.UA. Сайти з таким доменом містять достовірні факти та офіційні документи.

Проаналізуємо сайт https://diia.gov.ua. Очевидно, що він використовує безпечний протокол https, а його власник - орган державної влади. На відміну від нього, фішинговий сайт, про який ми уже згадували, http://diia8000.gov.me не використовує безпечне з’єднання, а його власником не є державна установа.

Звертаємо також увагу, що шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів та/або роздруковані на папері, у тому числі у формі скорочених URL, згенерованих спеціальними сервісами. Не

вводьте ці покликання до браузера та не скануйте QR-коди Вашим смартфоном, якщо ви не впевнені у їх вмісті та походженні.

Другий крок алгоритму аналізу інтернет-ресурсу - ознайомлення з контентом, розміщеним на ньому. Для цього потрібно дати собі відповіді на запитання чек-листа.

Чек-лист «Аналізуємо контент сайту: даємо відповіді на запитання»

- Чи зазначено інформацію про авторів сайту?
- Чи зазначено мету створення сайту і для кого він створений?
- Чи розміщена на сайті Політика конфіденційності (правила, якими регламентується збір, обробка, використання і захист персональних даних, що можуть бути запитані/отримані при його використанні)?
- Чи є Угода користувача? Користувач шляхом переходу на сайт зазвичай надає свою згоду на дотримання всіх умов Угоди, у тому числі шляхом авторизації на сайті свого облікового запису (Акаунту)
- Чи зазначено фізичну адресу власників сайту? Якщо так, здійсніть пошук засобами Google карти, щоб впевнитись у тому, що вона існує. Використайте функцію «Супутник», щоб побачити, як виглядає будівля, зазначена в адресі
- Чи є на сайті контактні дані з можливістю поставити запитання авторам?
- Чи узгоджуються відомості, отримані на сайті, з інформацією з інших джерел?
- Чи регулярно оновлюється інформація на сайті?
- Чи публікуються матеріали на сайті від його авторів чи здебільшого це репости з інших джерел?
- Чи дотримуються журналістських стандартів автори повідомлень?
- Чи немає помилок на сайті (граматичних, орфографічних)? Звертайте увагу також на форматування інформації на сайті
- Чи не пропонують Вам поширити інформацію скріншоту сайту? Скріншот - це зображення, яке не має першоджерела і яке можна

змінити у графічному редакторі, тому поширюючи його, Ви ризикуєте стати джерелом фейків та дезінформації

Незахищені мережі. В офісах, кав'ярнях, готелях, аеропортах та інших громадських місцях можна зустріти відкриті бездротові мережі. Зазвичай Wi-Fi мережі небезпечні, адже вони незахищені паролем та використовують незашифровані з'єднання, які наражають користувачів на небезпеку. Серед таких мереж можуть виявитися і мережі зловмисників, мета яких - вкрасти Ваші особисті дані. Це може статися в тому випадку, якщо у смартфоні включена функція автоматичного підключення до мережі Wi-Fi. Якщо мережа, до якої телефон підключиться, належить зловмисникам, вони можуть отримати доступ до Вашої інформації (повідомлень з пошти, паролей, фотографій, номерів телефонів, банківських рахунків тощо).

Щоб «заманити» довірливих користувачів, зловмисники можуть створювати фейкові Wi-Fi, використовуючи назву точки, близьку до справжньої, наприклад, назву кав'ярні, готелю, аеропорту («airport» та «airport-guest», де одна з них може бути фейковою), або ж називають її "Free Wi-Fi", тоді до неї матимуть бажання підключитися багато користувачів мережі.

Наявність пароля у мережі Wi-Fi теж не гарантує безпеку: такі мережі залучають велику кількість довірливих користувачів. Найнадійнішим способом є підключення у громадських місцях шляхом створення точки доступу до Інтернету 3G/4G за допомогою власного смартфона.

Якщо ж Ви все ж підключились до невідомої мережі Wi-Fi, не використовуйте особисті сторінки і не вводьте паролі. Крім того, налаштуйте параметри бездротового зв'язку на своїх пристроях, щоб

вони не могли автоматично підключатися до вільних точок Wi-Fi.

Паролі: правила їх створення та захисту

Одним із ключових елементів надійного пароля є його унікальність. Онлайн-видання https://cybernews.com/, засноване на дослідженнях, що допомагають людям йти безпечним шляхом у цифровому світі, оприлюднило топ-10 найпоширеніших паролів у 2023 році. До них увійшли: 123456; 123456789; qwerty; пароль; 12345; qwerty123; 1q2w3e; 12345678; 111111; 1234567890.

Крім того, паролі легко зламати, оскільки більшість людей дотримуються схожих шаблонів під час їх створення:

– 50% шансів, що в паролі є принаймні одна літера, що позначає голосний звук;
– у паролях зазвичай є цифри 1 або 2, які розміщені в кінці пароля;
– великі літери зазвичай стоять на початку, після них йде голосний звук;
– жінки часто використовують в паролі своє ім’я;
– чоловіки часто використовують своє хобі;
– найпоширенішими символами є: -~@#$%&?
– 66% людей використовують лише 1 або 2 паролі для всіх своїх облікових записів.

Для створення та захисту паролів дотримуйтесь рекомендацій чек-листа.

Чек-лист «Створюємо та захищаємо паролі»

– для кожного ресурсу створюйте окремий пароль. 91 % людей знають про небезпеку однакових паролів, але 59 % продовжують використовувати його всюди. Якщо зловмисник зламає один пароль, він може отримати доступ до всіх інших облікових записів;
– для робочого та особистого акаунтів створюйте різні

паролі;

– не використовуйте повторно той самий пароль принаймні протягом року, періодично змінюйте його: мати один і той самий замок на дверях упродовж багатьох років – це все рівно, що запрошувати до себе злодія;

– один із варіантів створення надійного пароля – абревіатура. Придумайте чи пригадайте довге речення, стовпчик з вірша тощо та створіть пароль із перших літер кожного слова, поміняйте деякі літери на цифри та символи;

– використовуйте генератор паролів, якщо Вам не вдається придумати надійний пароль;

– не створюйте пароль з набору букв, які перебувають на клавіатурі по-сусідству: всі популярні комбінації давно включені в бази даних програм підбору паролів;

– тримайте свій пароль у безпеці та ніколи нікому не повідомляйте його;

– не переходьте за невідомими покликаннями, які просять ввести логіни та паролі;

– завжди виходьте з власного акаунту, особливо якщо Ви користуєтесь чужим комп'ютером або Ваш пристрій увімкнено поблизу інших людей;

– не вводьте свій пароль на загальнодоступних комп'ютерах у громадських місцях (бізнес-центрах, готелях, кав'ярнях, автовокзалах тощо);

– використовуйте менеджери паролів, які ми детальніше розглянемо нижче.

Для зберігання паролів використовують менеджери паролів – це програми та ресурси, які є «сейфами» для ваших паролів і допомагають зберігати їх у безпеці завдяки шифруванню. Менеджери використовують як на персональних комп'ютерах, так і на смартфонах. За способом зберігання даних їх поділяють на такі види:

- хмарні у «хмарах» (такі менеджери паролів найпопулярніші, забезпечують синхронізацію даних на різних пристроях);
- локальні (дані зберігаються на одному пристрої, тож потрібно пам'ятати, що у разі виведення його з ладу або викрадення доступ до

паролів може бути втрачений);

- комбіновані (у разі використання рішень, що зберігають базу даних локально, проте користувач розміщує її у хмарному середовищі, яке він використовує).

Один із рекомендованих менеджерів від Держспецзвязку є ресурс https://bitwarden.com/ - простий та безпечний спосіб зберігати всі ваші логіни та паролі та легко їх синхронізувати між усіма Вашими пристроями.

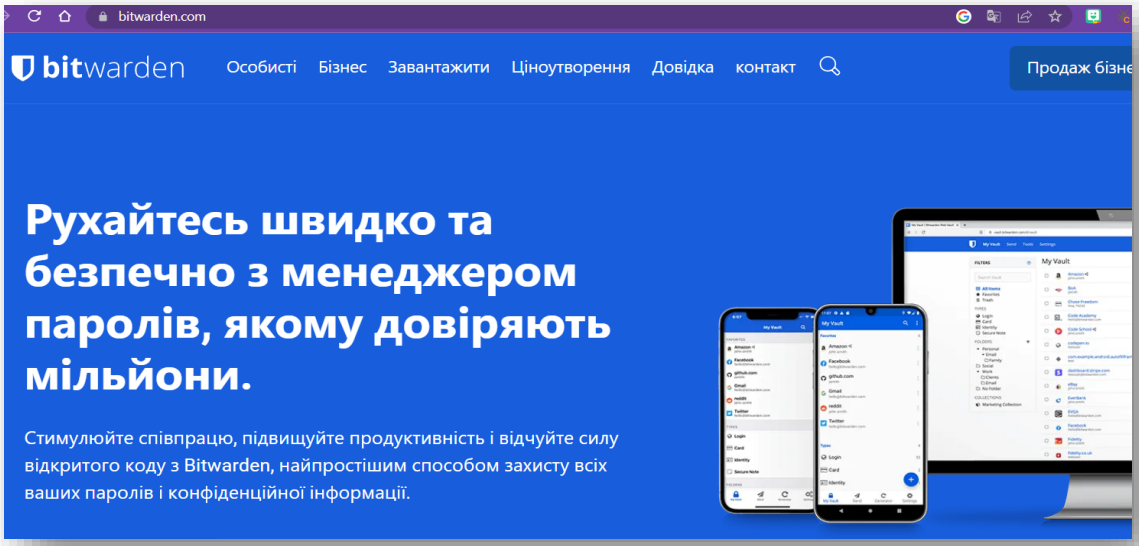


Рис. 8. Головна сторінка менеджера паролів bitwarden

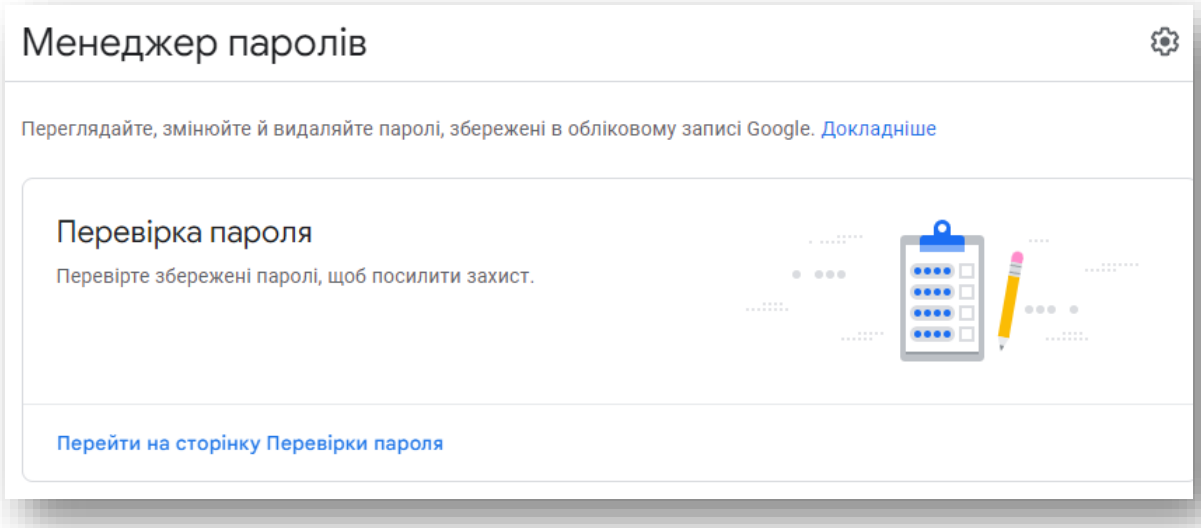


Рис. 9. Головна сторінка менеджера паролів від Google

Крім того, перейшовши за покликанням https://passwords.google.com/?hl=uk під своїм акаунтом, Ви можете перевірити стан Ваших паролів менеджером від Google (рис. 9). Для цього потрібно натиснути на пункт «Перейти на сторінку перевірки пароля», на наступному кроці – на кнопку «Перевірити паролі» (рис. 10).

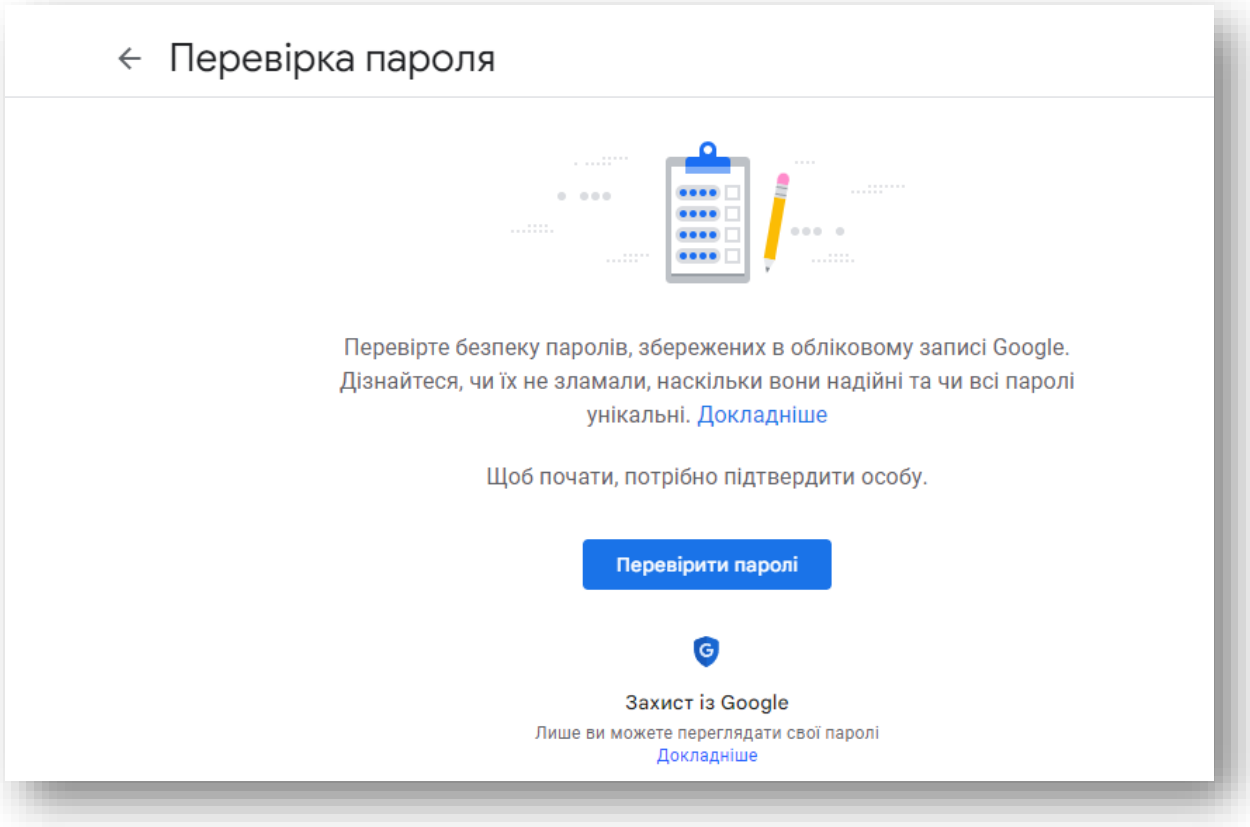


Рис. 10. Перевірка паролів менеджером від Google

Після цього менеджер надасть інформацію про зламані паролі, якщо такі є; ті, що використовувались повторно і на яких ресурсах; перелік облікових записів із ненадійним паролем.

Небезпеки соцмереж

Використання соціальних мереж є одним із найпопулярніших видів діяльності в Інтернеті. За даними платформи https://www.statista.com, що об'єднує статистичні дані з-понад 80 000 тем із-понад 22 500 джерел і робить їх доступними, лідером ринку є Facebook – перша соціальна мережа, яка перевищила один мільярд зареєстрованих

облікових записів і наразі має понад 2,9 мільярда активних користувачів щомісяця (рис. 11). У середньому користувачі Інтернету витрачають 144 хвилини на день у соціальних мережах і програмах для обміну повідомленнями, що на півгодини більше, ніж у 2015 році.

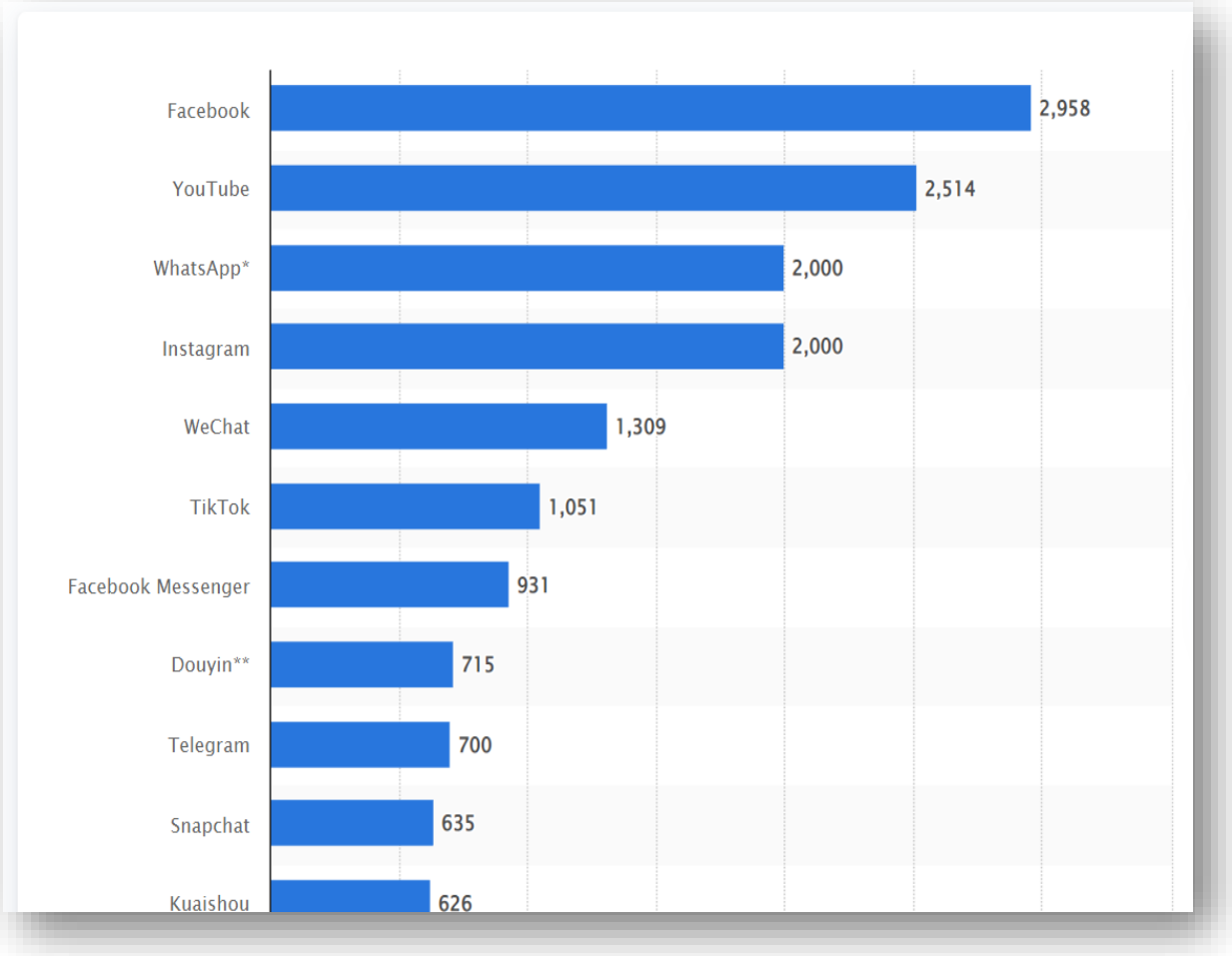


Рис. 11. Найпопулярніші соціальні мережі в усьому світі станом на січень 2023 року за кількістю активних користувачів щомісяця (в мільйонах)

Однак соцмережі містять чимало небезпек. За останні роки вони стали осередком фейкових новин, психологічної залежності, а кількість фейкових профілів може бути більшою, ніж мешканців великих країн.

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA у серпні 2022 року виявлено зростання кількості шахрайських сторінок у соціальній мережі Facebook у зв’язку з

наданням грошових компенсацій на платформі єДопомога та фінансової допомоги від різних організацій (ООН, ЄС, Товариства Червоного Хреста тощо) (рис.12). Із зображеннями таких сторінок Ви можете детальніше ознайомитись за покликанням https://cert.gov.ua/article/1545776. Їх об'єднують спільні риси, аби викликати довіру в користувачів: відкриті руки, фото першої особи держави, жовто-блакитні логотипи з зображенням державних символів, логотипом єДопомоги, відомі словосполучення на кшталт «новини 24», «виплата компенсації» тощо.

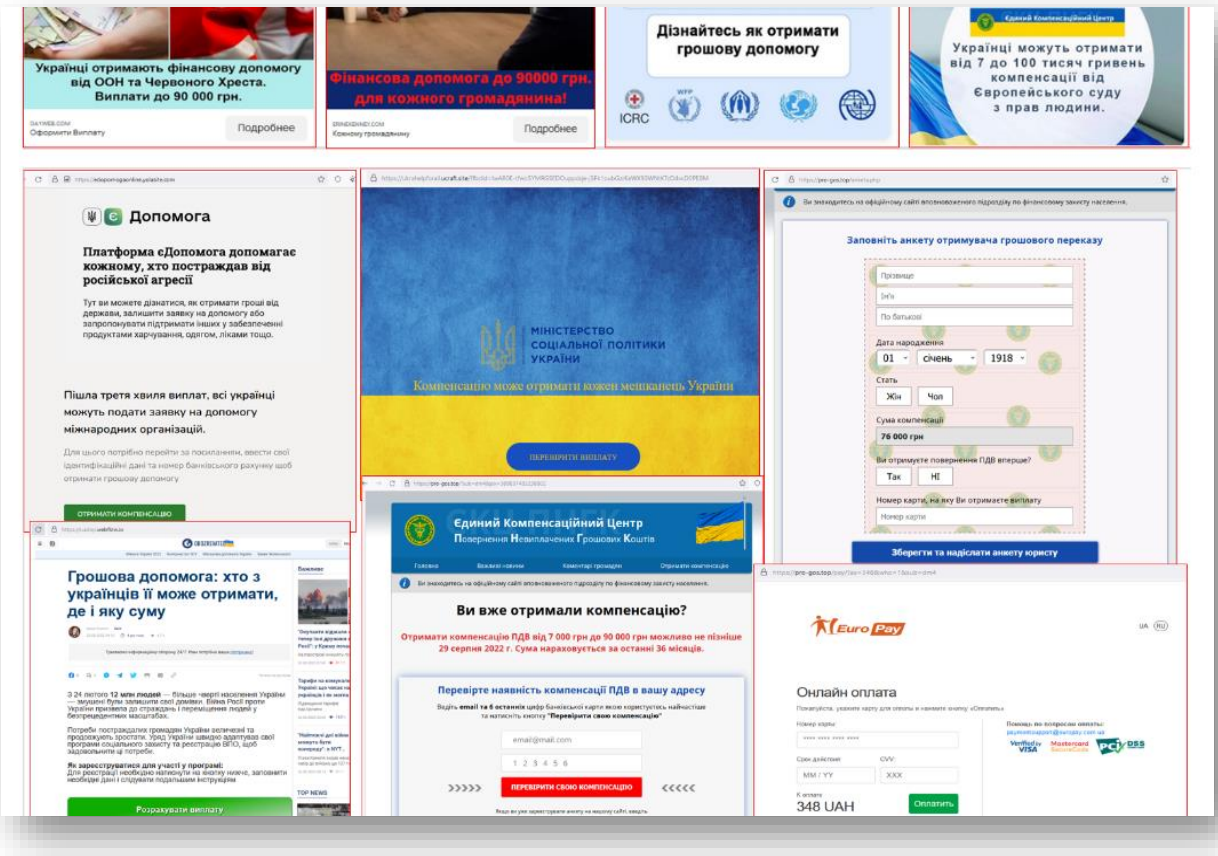


Рис. 12. Графічні зображення шахрайських сторінок, пов'язаних із грошовими компенсаціями

На даних сторінках користувачам пропонувалось перейти за покликанням, що веде на фішингову сторінку так званого «Єдиного Компенсаційного Центру Повернення Невиплачених Грошових Коштів» та отримати виплату після надання персональної інформації та здійснення додаткового платежу. Зверніть увагу, що допомога громадянам надається через офіційний сайт платформи єДопомога

https://aid.edopomoga.gov.ua/, який має безпечний протокол з'єднання, а його домен свідчить про те, що сайт створено урядовою організацією. Тому ніколи не вводьте реквізити платіжних карток на незнайомих та підозрілих веб-сайтах, якщо ж Ви зробили це помилково, негайно заблокуйте платіжну картку за допомогою мобільного застосунку, телефону гарячої лінії банку, зазначеної на звороті платіжної картки, або за допомогою Інтернет-банкінгу.

Інколи пересічному користувачу важко визначити, фейкова це сторінка чи справжня, адже якщо зловмисники здійснюють дублювання акаунтів, вони створюють облікові записи, що спочатку повністю копіюють контент, оформлення справжніх акаунтів користувачів, а лише потім сторінки використовуються для шахрайства та поширення дезінформації. З цією метою соцмережі верифікують профілі публічних осіб та організацій та позначають їх блакитним кружечком із білим прапорцем або іншим подібним зображенням. При наведенні мишею на відповідну позначку з'являється виринаюче вікно про підтвердження соцмережею даного профілю (рис.13).

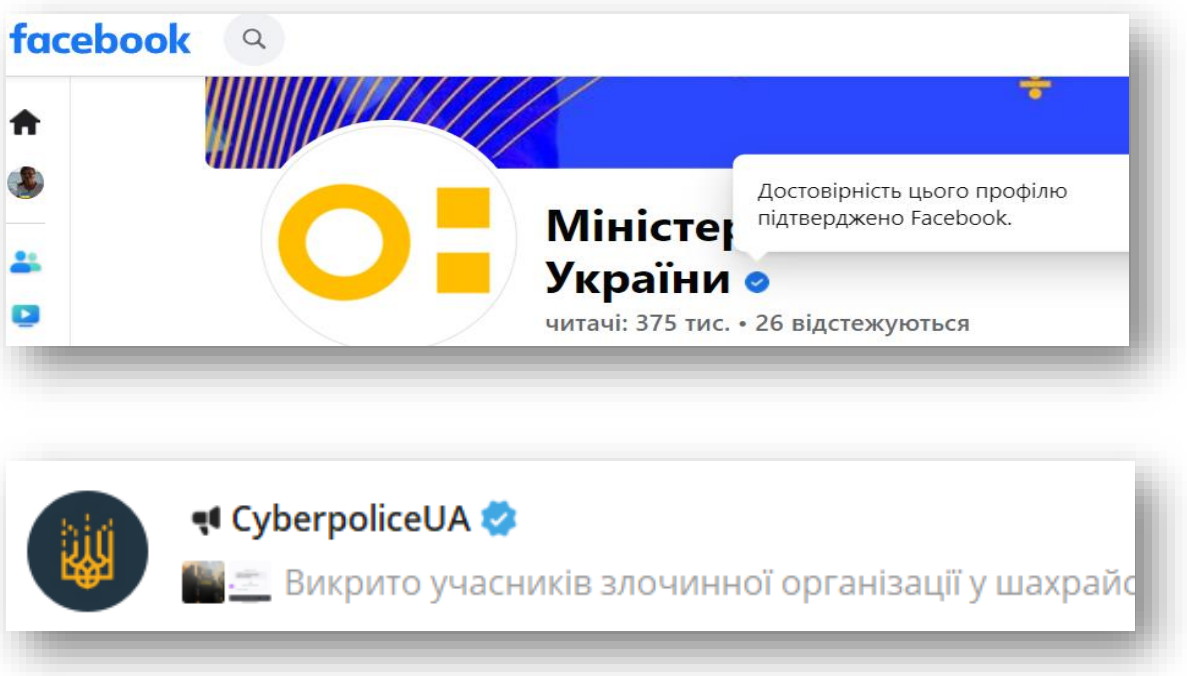


Рис. 13. Верифіковані профілі у соцмережі Facebook та месенджері Телеграм

Для безпечного користування соцмережами дотримуйтесь рекомендацій чек-листа.

Чек-лист «Користуємося соцмережами безпечно»

– перевірте, чи акаунт верифікований (блакитна галочка біля назви);

– зверніть увагу, чи розміщене в акаунті реальне фото чи абстрактне зображення, чи правильно написана назва акаунту та чи грамотно веде свій акаунт його власник;

– проаналізуйте оригінальність контенту: чи все скопійовано з інших джерел чи містяться унікальні дописи;

– якщо дописи автора акаунту викликають у Вас обурення, агресію, страх або контент може завдати шкоду іншим користувачам, зупиніться і добре проаналізуйте їх;

– ігноруйте людей, які просяться до Вас «у друзі», а Ви не знаєте їх у реальному житті;

– перш, ніж поширити фото чи відео, зупиніться: щойно Ви це зробите, Ви втратите над ним контроль, адже будь-хто може перетворити фото у фотофейк у графічному редакторі;

– ігноруйте повідомлення, в яких Вам пропонують перейти за покликанням та ввести додаткову інформацію про себе (наприклад, дату народження, щоб «дізнатись», ким Ви були у минулому житті тощо), адже таким чином Ви добровільно віддаєте особисту інформацію, яку зловмисники можуть використати у власних цілях;

– проаналізуйте інформацію у власному акаунті, який цифровий слід залишаєте, адже це впливає не лише на Вашу репутацію, але й репутацію освітньої установи, в якій працюєте. Пам’ятайте, що ваші дії та слова в інтернеті можуть вплинути неї. Перевіряйте інформацію, яку поширюєте в соціальних мережах, перед тим, як її опублікувати, подумайте, хто може її побачити;

– нагадуйте здобувачам освіти про важливість онлайн-репутації та як правильно її формувати.

Роль педагога в організації безпечного цифрового освітнього середовища

У статті 57-1 Закону України «Про освіту» зазначено державні гарантії в умовах воєнного стану, надзвичайної ситуації або надзвичайного стану, зокрема йдеться про те, що здобувачам освіти на час особливого періоду «гарантується організація освітнього процесу в дистанційній формі або в будь-якій іншій формі, що є найбільш безпечною для його учасників» [3].

На нашу думку, для організації безпечного цифрового освітнього середовища необхідне виконання таких умов:

- захист особистих даних;
- безпека мережі;
- етичне поводження усіх учасників освітнього процесу;
- освіта з питань кібербезпеки;
- заходи захисту від шкідливих впливів інтернету (рис. 14).

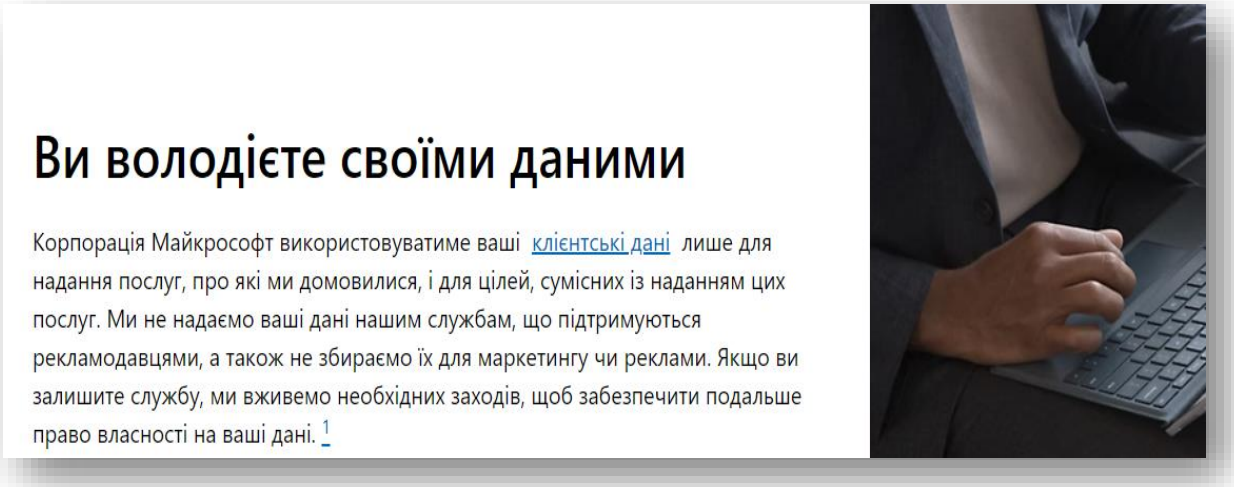
Для захисту особистих даних учасників освітнього процесу необхідно аналізувати додатки, сайти, розширення, платформи щодо того, які дані вони збирають і з якою метою. Як здійснювати аналіз ресурсів, ми вже описали вище.

Важливо використовувати рішення, призначені саме для освіти, наприклад, Google Workspace for Education, який є набором інструментів та сервісів Google, а також ресурси Microsoft. Вони не збирають дані з користувачів з метою реклами та маркетингу, натомість дбають про конфіденційність і безпеку особистої інформації (рис. 15).

Рис. 14. Умови функціонування безпечного цифрового освітнього середовища

Зверніть також увагу на те, що у додатках Google Play є контент для дітей, схвалений викладачами (рис. 16). На сторінці кожного з таких додатків можна ознайомитись, чому саме він отримав таку оцінку. Ці додатки для зручності пошуку об’єднані за віковими категоріями.

Державна служба якості освіти України радить використовувати для фіксації результатів навчання учнів та надання їм зворотного зв’язку електронний журнал, обравши у закладі освіти найбільш зручний ресурс, враховуючи вимоги та рекомендації МОН, а також єдину платформу з навчальними матеріалами, тобто цілісні електронні курси, які враховують повний цикл навчання та містять відеопояснення, текстові матеріали, завдання для закріплення матеріалу, його практичного застосування, рефлексії [4].



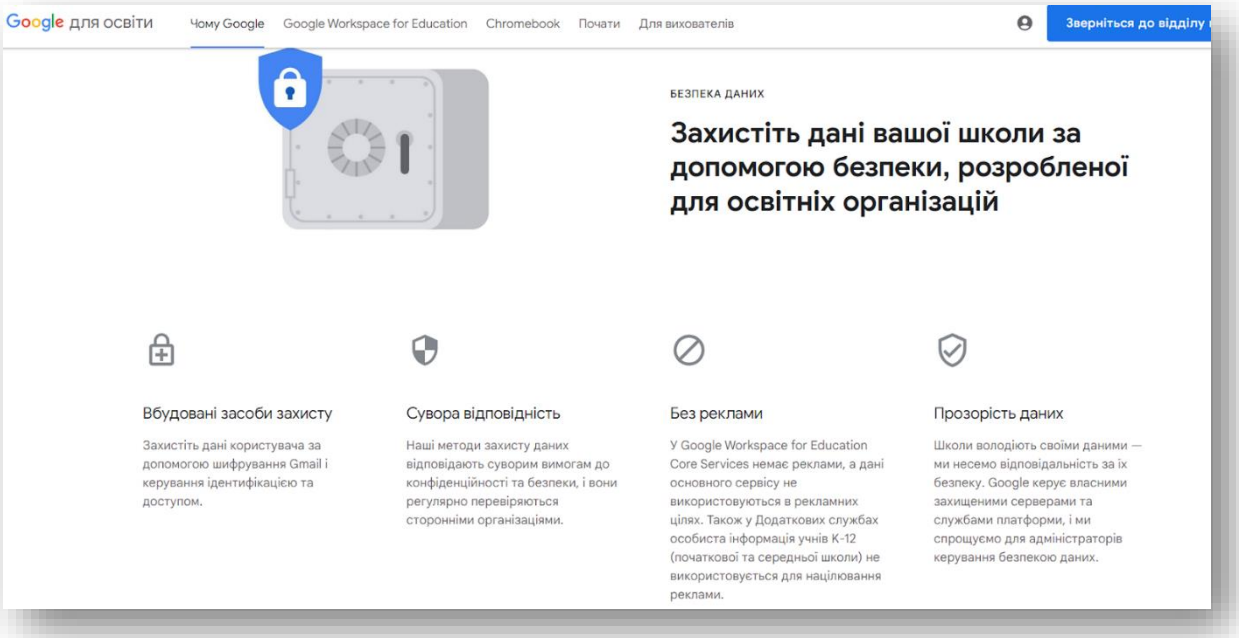


Рис. 15. Інформація про збір даних у рішеннях для освіти від Google та Microsoft

Безпечне цифрове освітнє середовище неможливе без організації безпечних уроків. Для занять з використанням технологій дистанційного навчання можна скористатись додатками Google Meet, Zoom, Cisco WebEx, Microsoft Teams, кожний з яких має свої особливості захисту.

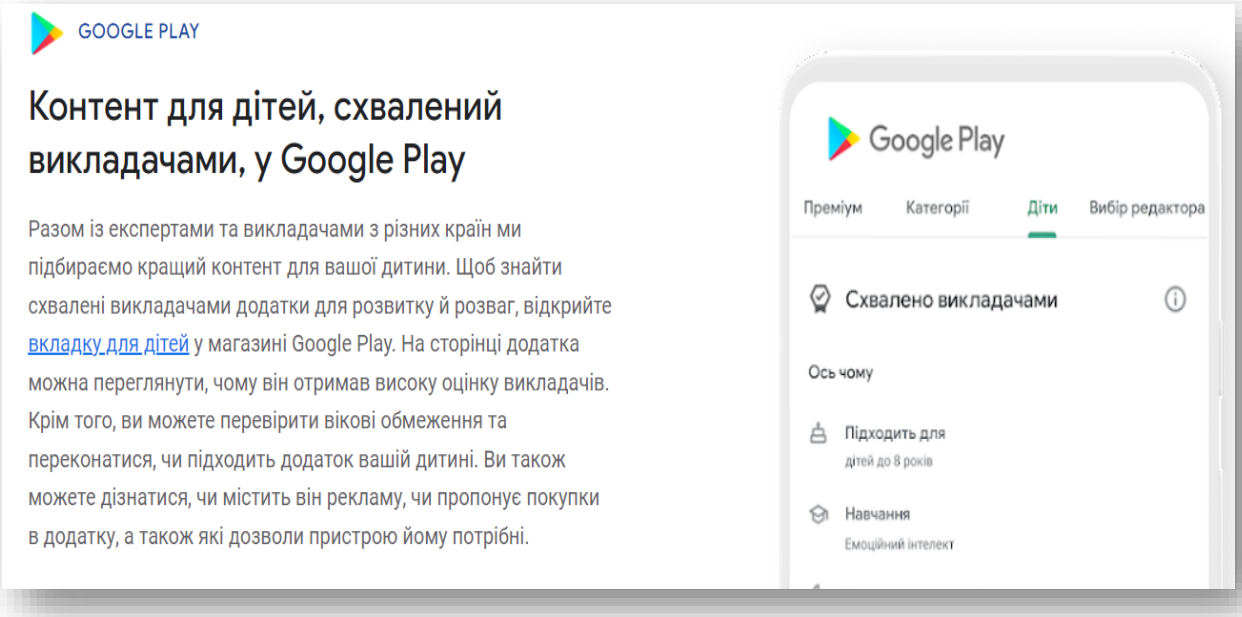


Рис. 16. Інформація про збір даних у рішеннях для освіти від Google та Microsoft

Наприклад, для відеозустрічей у Meet використовуються заходи захисту від зламу та підключень із телефону: коди зустрічей складаються з 10 символів, кожен із яких може мати одне з 25 значень, завдяки чому зловмисникам важко їх підбирати. Якщо повністю змінити запрошення на відеозустріч, зміниться код зустрічі та код для підключення з телефону, це корисно, якщо когось вилучено із запрошення на урок. Під час приєднання до відеозустрічі застосовуються обмеження: учасники не можуть приєднатися раніше, ніж за 15 хвилин до її запланованого початку; без запиту можуть приєднуватися лише користувачі, запрошені в календарі, інакше потрібно надсилати запит на приєднання, який має схвалити організатор зустрічі; є можливість керувати засобами безпеки, зокрема вимикати мікрофони учасників та вилучати їх; про порушення під час зустрічей користувачі можуть надсилати повідомлення (рис. 17).

Захист конфіденційності уроків у Zoom забезпечується шляхом шифрування зустрічей, використання паролів; надання можливостей викладачу створювати зали очікування для учнів, виключати будь-якого учасника чи всіх учасників, призупиняти їх дії, блокувати

конференцію, використовувати звукові підписи, застосовувати водяні знаки для показу екрана, включати чи відключати можливість запису зустрічі, призупиняти демонстрацію екрана під час відкриття нового вікна, дозволяти приєднуватися до конференції лише особам із встановленим доменом електронної пошти.

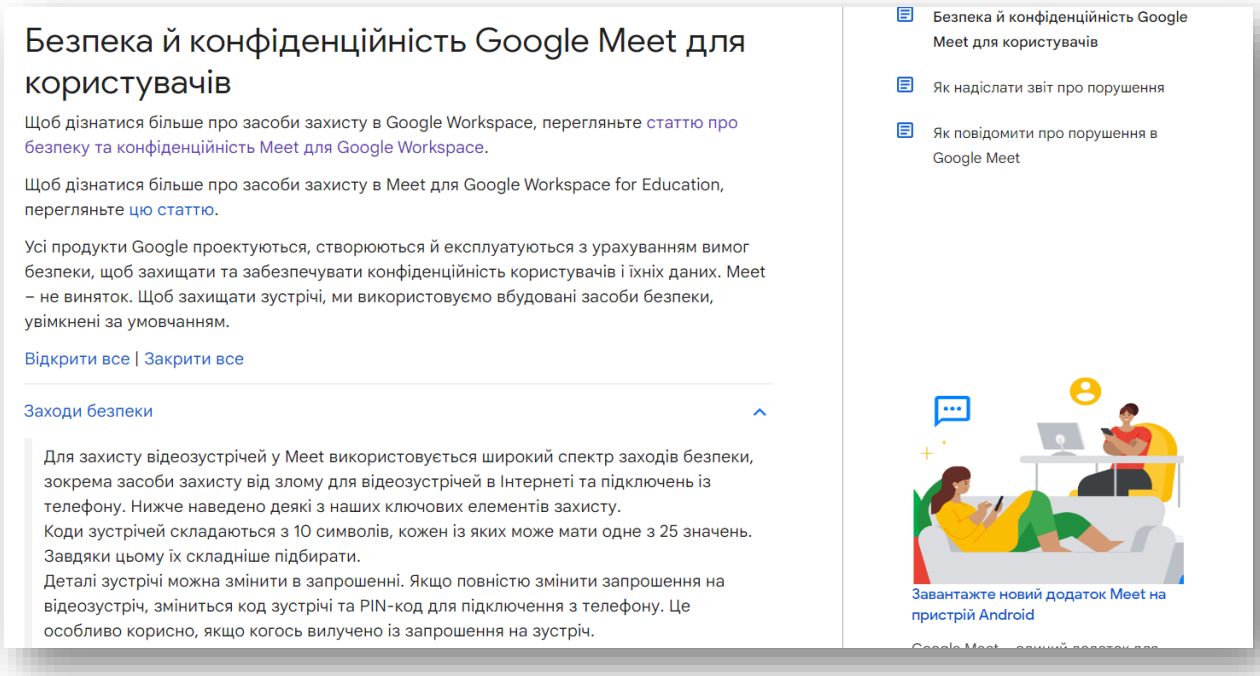


Рис. 17. Сторінка довідки Google Meet щодо безпеки і конфіденційності

Для проведення безпечних онлайн-уроків скористайтесь загальними порадами чек-листа.

Чек-лист «Проводимо онлайн-уроки безпечно»

- добре подумайте, перш ніж публікувати покликання на зустрічі на загальнодоступних ресурсах;
- якщо потрібно зробити знімок екрана зустрічі доступним для всіх, вилучіть із нього URL-адресу;
- для дистанційних уроків використовуйте тільки перевірені ресурси, які забезпечують шифрування зустрічей;
- обов'язково перевіряйте нових учасників і дозволяйте приєднуватися до зустрічі лише тим, кого Ви знаєте;
- якщо хтось заважає проведенню уроку, скористайтеся засобами

модерування: вилучіть такого учасника, вимкніть його мікрофон тощо;
- намагайтеся прислухатися до учнів та отримувати зворотний зв'язок щодо уроків;
- слідкуйте за фоном під час відеодзвінків, на ньому не має бути сторонніх предметів, що надавали б особисту інформацію (ім'я, прізвище, особисті фото, сертифікати та інше);
- обачно діліться під час зустрічей особистою інформацією, наприклад, паролями, номерами банківських рахунків чи кредитних карток, Вашою датою народження;
- створюйте спільно правила комунікації під час онлайн-уроків. (рис. 18).

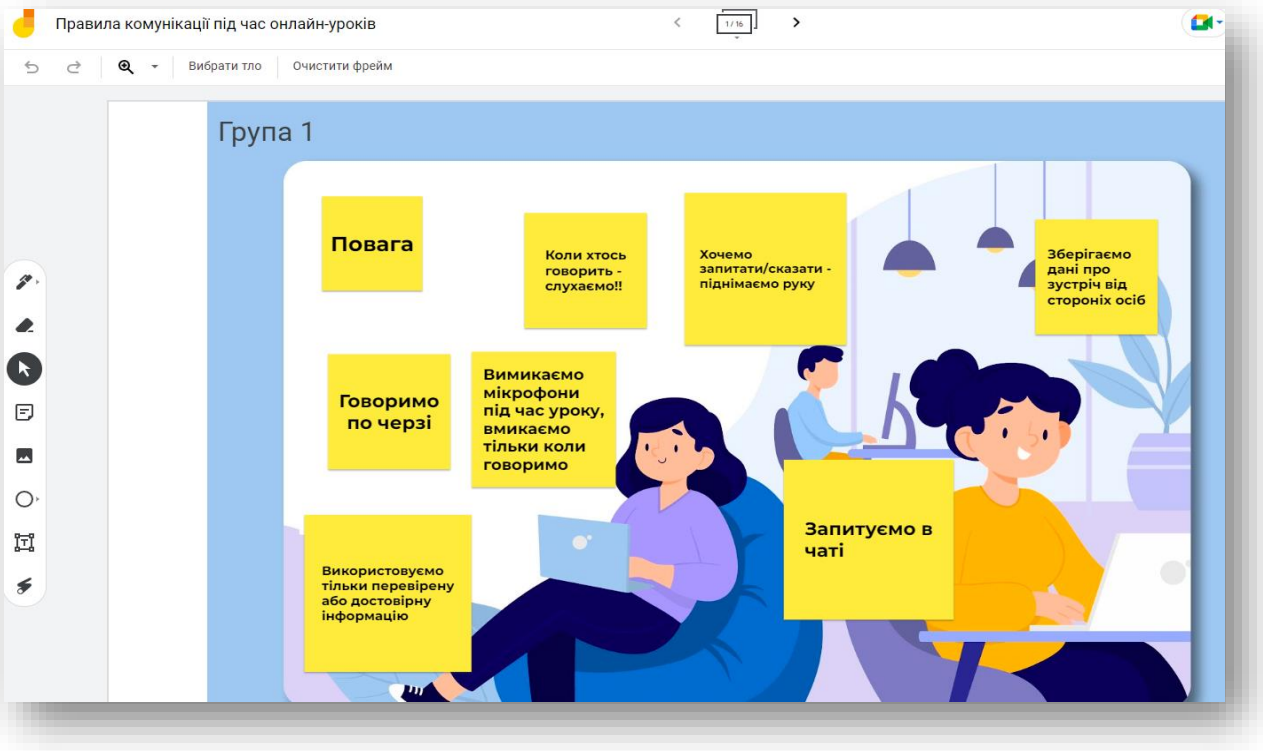


Рис. 18. Спільне створення правил комунікації під час онлайн-уроків засобами Google Jamboard

Ресурси для розвитку кіберграмотності учасників освітнього процесу. Важливою є неперервна освіта всіх учасників освітнього процесу з розвитку кіберграмотності. Фонд цивільних досліджень і розвитку (CRDF Global), метою якої є сприяння міжнародному науково-технічному співробітництву заради миру і процвітанню шляхом надання грантів і технічних ресурсів для виконання спільних науково-дослідних проєктів, а також проведення навчальних програм, розробив онлайн-курс «Основи кібербезпеки для представників державних органів» [5], який може бути корисним педагогічним працівникам. Тут пропонуються як теоретичні матеріали, так і практичні завдання. Курс дозволить дізнатися про основні загрози в інформаційному просторі, ознайомитись із ризиками ігнорування правил кібербезпеки, рекомендаціями щодо захисту власних та корпоративних даних, пройти фінальне тестування та отримати сертифікат (рис. 19).

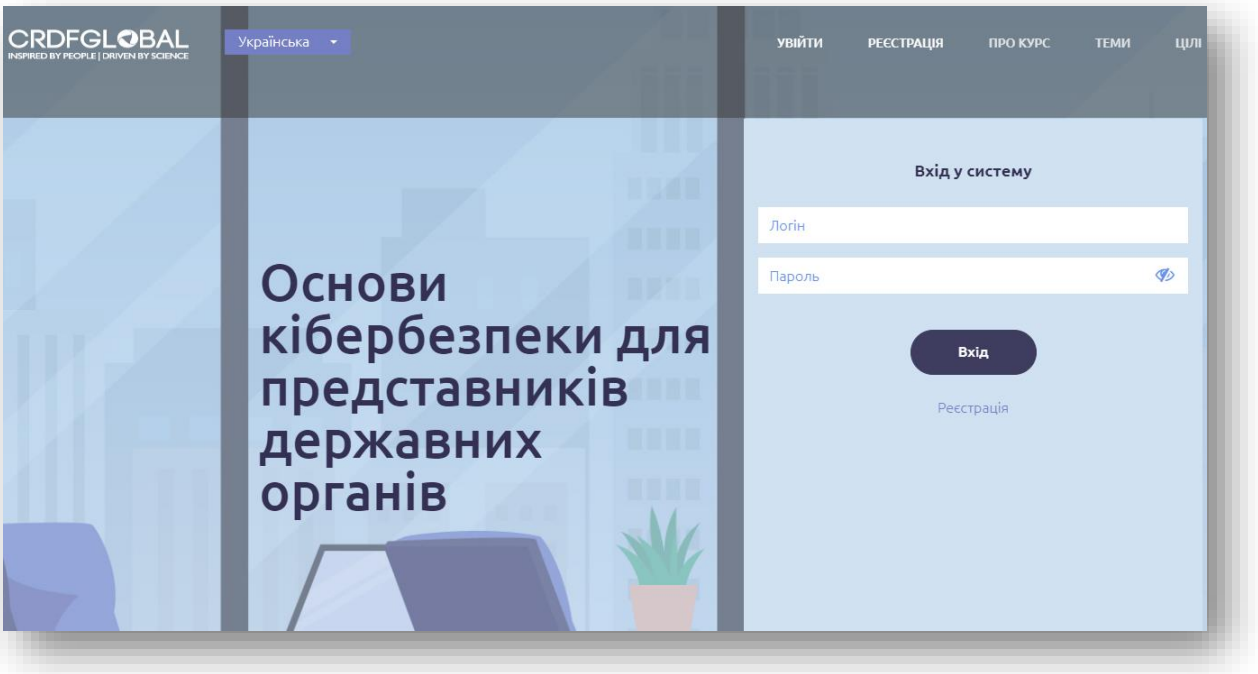


Рис. 19. Головна сторінка курсу з основ кібербезпеки

Фондом також розроблено курс «Основи кібербезпеки для школярів» для учнів 1-11 класів [6] (рис. 20).

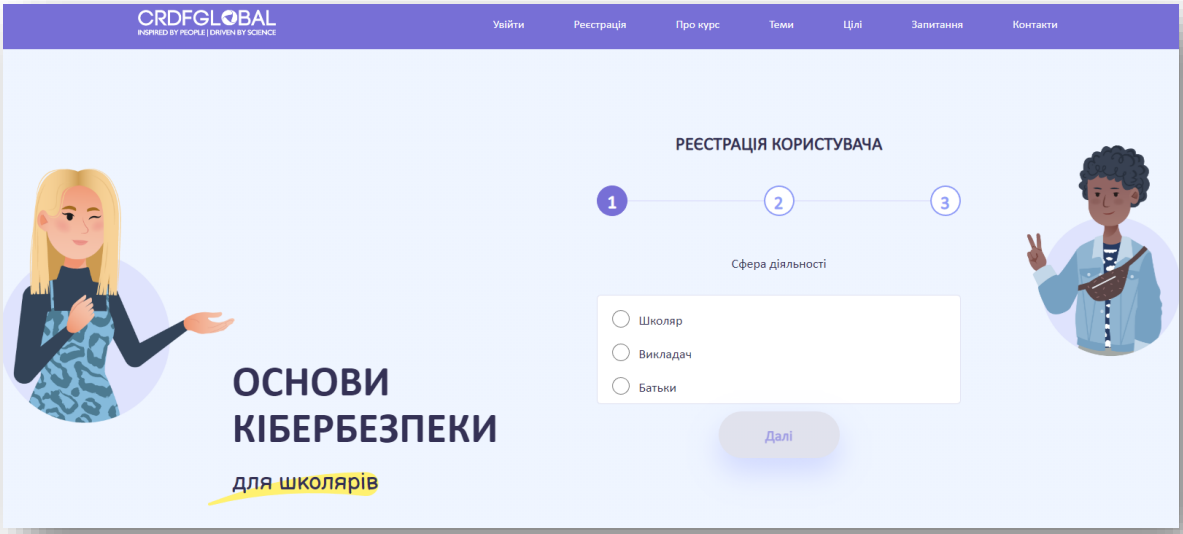


Рис. 20. Головна сторінка курсу «Основи кібербезпеки для школярів»

Зареєструватись на нього можна в ролі вчителя для відслідковування прогресу учнів, у ролі учня або батьків. З матеріалом слухачі курсу знайомляться, гортаючи слайд-шоу, переглядаючи відео (рис. 21) та виконуючи інтерактивні вправи, які максимально наближені до реальних ситуацій (рис. 22). Переконатися, що засвоїли весь матеріал, учні можуть, пройшовши фінальний тест та отримавши сертифікат.

Тематика і покликання на модулі курсу:

1-4 класи:
Модуль 1: Як захистити ґаджет
Модуль 2: Як шукати безпечне відео в інтернеті
Модуль 3: Як шукати інформацію в інтернеті
Модуль 4: Як спілкуватися в інтернеті
Модуль 5: Якою інформацією можна ділитися в інтернеті
5-6 класи:
Модуль 1: Електронна пошта і шахрайство
Модуль 2: SMS-шахрайство
Модуль 3: Цифрові сліди
Модуль 4: Пароль точно захищає?
Модуль 5: Онлайн-ігри та офлайн-проблеми
Модуль 6: Перевіряємо безпеку комп'ютера
Модуль 7: Ми просто спілкуємось в інтернеті

Модуль 8: В новинах про це не написали: фейки та як їх розпізнати
Модуль 9: Я вмію захищати інформацію

7-9 класи:

Модуль 1: Наскільки безпечний твій смартфон?
Модуль 2: Злий хакер чи поганий захист?
Модуль 3: Про що розповідають акаунти?
Модуль 4: Соціальні мережі
Модуль 5: Загрози інформаційного простору
Модуль 6: Соціальна інженерія
Модуль 7: Заробіток в інтернеті
Модуль 8: Банківська картка
Модуль 9: Онлайн-ігри

10-11 класи:

Модуль 1: Основні помилки користувачів та можливі наслідки
Модуль 2: Безпечне використання мобільного телефону
Модуль 3: Безпечне використання комп'ютерів
Модуль 6: Безпека в соціальних мережах
Модуль 7: Інтернет-безпека
Модуль 8: Фейкові новини
Модуль 9: Основні правила захисту інформації
Модуль 10: Що робити, якщо кіберзлочин все-таки стався

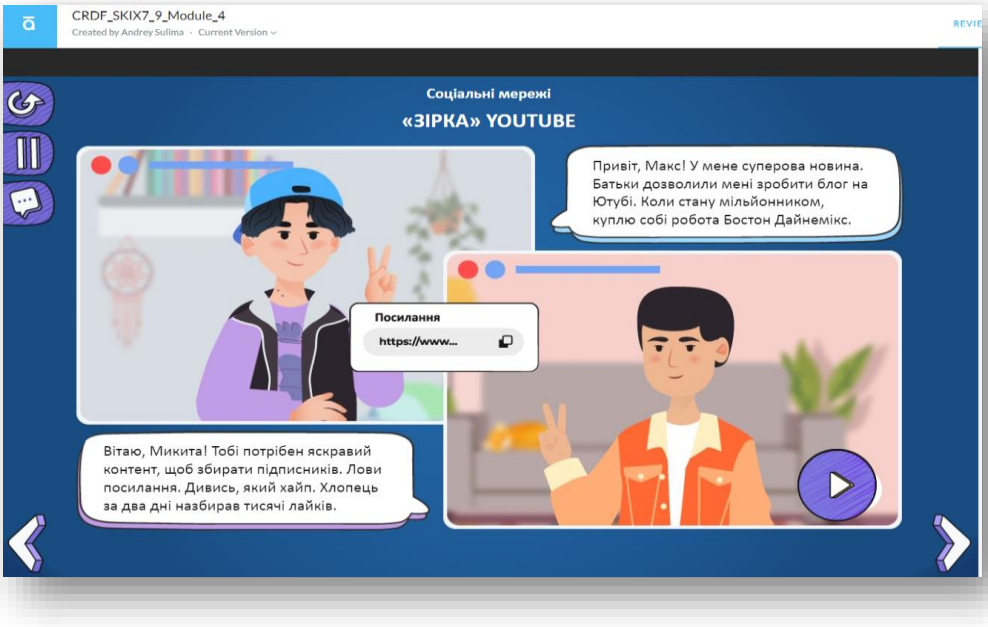


Рис. 21. Теоретичний матеріал до теми «Соціальні мережі»

Рис. 22. Вправи до теми «Соціальні мережі»

Підвищити свій рівень кіберграмотності учні та вчителі можуть і на платформі «Дія» (рис. 23). Тут розміщені ресурси:

- пам'ятка по кібергігієні https://osvita.diia.gov.ua/tips-for-cybersecurity;
- гайд https://osvita.diia.gov.ua/guide;
- освітні серіали https://osvita.diia.gov.ua/courses?param_category=32.

Від компанії Google корисними можуть бути такі ресурси:

- гра Interland https://g.co/Interland, яка наповнена пригодами і робить вивчення цифрової безпеки та громадянства інтерактивним і веселим (рис. 18);
- посібник для вчителів із безпеки дітей в Інтернеті https://bit.ly/bia_ua;
- центр безпеки Google https://safety.google.

Також рекомендуємо скористатись навчально-методичними матеріалами проєкту «Вивчай та розрізняй: інфо-медійна грамотність» https://drive.google.com/file/d/1iixCOKQo9n-o2SxQ9CUOHXN7Zz2kHy7H/view.

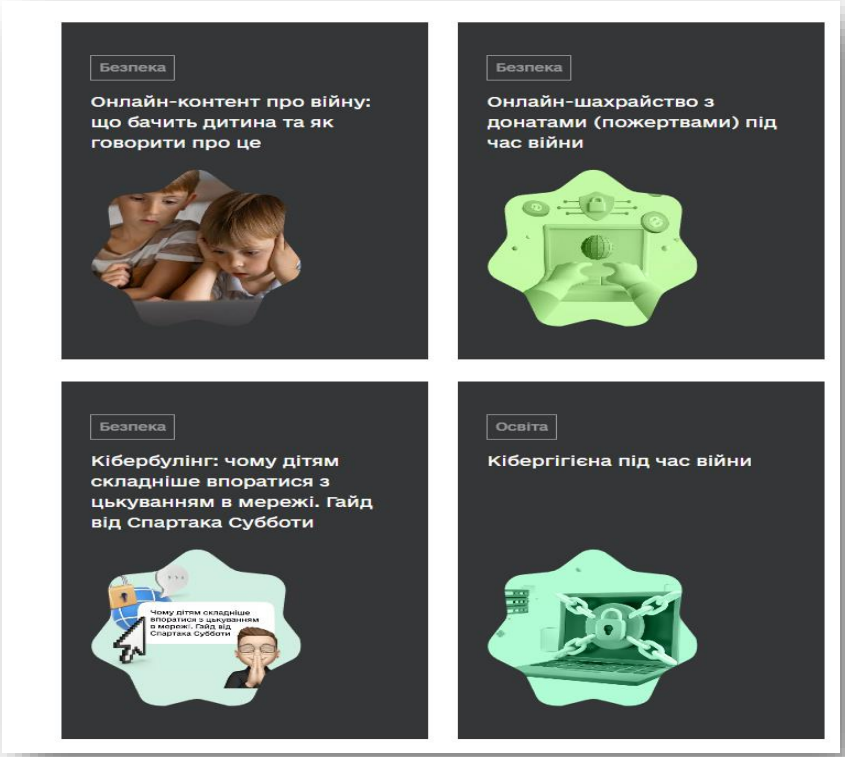


Рис. 23. Матеріали з розвитку кіберграмотності на платформі «Дія»

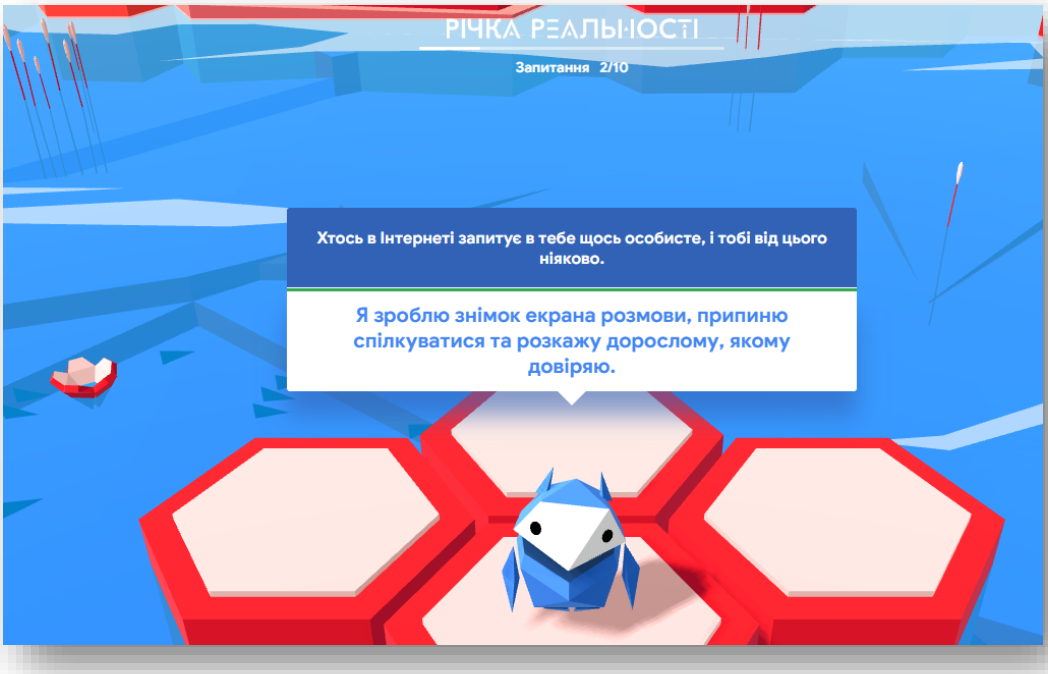


Рис. 24. Гра Interland від Google

Висновки та рефлексія

Підбиваючи підсумки, зазначимо, що кіберграмотність усіх учасників освітнього процесу – це одне з першочергових завдань освітян на даний час, адже це не лише захист інтересів кожного громадянина, але й стан захищеності державного суверенітету та територіальної цілісності України, тому важливим є усвідомлення педагогами важливості як власного неперервного розвитку в частині кібербезпеки, так і розвитку своїх учнів.

Перевірте себе

Вправа «Безпека в цифровому суспільстві». Перейдіть за покликанням https://learningapps.org/view29185429 або QR-кодом

Вправа «Роль педагога в організації безпечного цифрового освітнього середовища». Перейдіть за покликанням https://learningapps.org/view30421515 або QR-кодом

Використані джерела

1. Про Стратегію кібербезпеки України: УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013.

2. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Звіт про роботу 2022. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=50943.

3. Про освіту: ЗУ від 05.09.2017 № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/card/2145-19

4. Безпечне освітнє середовище: нові виміри безпеки /Державна служба якості освіти України. URL: https://sqe.gov.ua/bezpechne-osvitnie-seredovishhe-novi-vim/.

5. Основи кібербезпеки для представників державних органів /CRDF Global. URL: https://state-cyber-edu.org/mc/index.php/usr/login/login

6. Основи кібербезпеки для школярів /CRDF Global. URL: https://cyberkidsukraine.org/mc/index.php/usr/login/login.

Для нотаток