
День безпечного Інтернету
11 лютого 2025 року

Що таке День безпечного Інтернету?

Міжнародна ініціатива (заснована в 2004 році) - Підтримується Insafe/INHOPE та Єврокомісією. Метою якої є підвищити обізнаність про безпеку в Інтернеті

11 лютого 2025 року у світі відзначається День безпечного Інтернету (Safer Internet Day). День безпечного Інтернету (SID/ДБІ) запровадили мережі Insafe та INHOPE за підтримки Європейської комісії для просування безпечного та позитивного використання цифрових технологій, особливо, дітьми й молоддю.

Основні загрози в Інтернеті

-Кібербулінг та онлайн хейт

- Фішинг та шахрайство

- Викрадення персональних даних

- Фейки та дезінформація

- Надмірне використання цифрових технологій

Кібербулінг

– це булінг із застосуванням цифрових технологій. Він може відбуватися в соціальних мережах, платформах обміну повідомленнями (месенджерах), ігрових платформах та мобільних телефонах. Це неодноразова поведінка, спрямована на залякування, провокування гніву чи приниження тих, проти кого він спрямований.

- поширення брехні про когось або розміщення фотографій, які компрометують когось, у соціальних мережах;
- надсилання повідомлень або погроз, які ображають когось або можуть завдати комусь шкоди, через платформи обміну повідомленнями;
- видання себе за когось іншого/іншу і надсилання повідомлень іншим людям від його/її імені.

Онлайн-хейт

Хейт, онлайн-ненависть – це будь-який вислів чи вираз, що заохочує або пропагує ненависть, огиду, нелюбов до того чи іншого явища або будь-кого.По суті, хейт є ворожнечею, яка не має наслідків, адже агресор, прикриваючись анонімністю, може уникнути покарання за свої слова.

Ознаки хейту (hate speech або мови ворожнечі) можуть включати:

Образи та приниження – негативні висловлювання, спрямовані на дискредитацію людини або групи.

Дискримінація – вираження зверхності або приниження за ознаками раси, статі, національності, релігії тощо.

Заклики до насильства – заохочення або виправдання агресії щодо певних осіб або груп.

Негативні стереотипи – поширення хибних чи спрощених уявлень про людей на основі їхньої ідентичності.

Знецінення або висміювання – насмішки, саркастичні коментарі, які мають на меті принизити когось.

Погрози або залякування – натяки чи прямі заяви про можливість заподіяння шкоди.

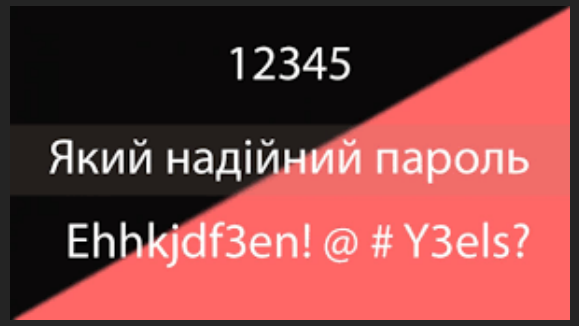
Фальшиві звинувачення – безпідставні заяви, які дискредитують особу чи групу.

Хейт може проявлятися як у відкритій, так і в завуальованій формі, наприклад, через меми, іронічні висловлювання або нібито жарти.

Як захистити себе в Інтернеті?

- Використовуйте надійні паролі

- Активуйте двофакторну автентифікацію
- Перевіряйте інформацію перед поширенням
- Будьте обережні з персональними даними



Використовуйте надійні паролі

- **Що робить пароль надійним**
- Хороший пароль – довгий пароль. Фахівці рекомендують використовувати пароль довжиною не менше 12 символів, але чим він довший, тим краще.
- Створюйте складні паролі, використовуючи поєднання великих і малих літер, цифр і символів. Можете навіть переключати при цьому розкладку на клавіатурі.
- Пам'ятайте, що навіть найкращі паролі з часом стають усе менш надійними. Тому, щоб залишатися в безпеці, не забувайте регулярно їх змінювати.

Викрадення персональних даних

або крадіжка особистої інформації – це незаконне отримання, використання або розповсюдження конфіденційної інформації без згоди власника.

Це може включати:
Фінансову інформацію (номери кредитних карток, банківські рахунки).
Особисті дані (ПІБ, адреса, номер телефону, паспортні дані, ІПН).
Облікові записи (логіни, паролі, електронна пошта, дані соцмереж).

Методи викрадення персональних даних

1.Фішинг – шахрайські листи або сайти, що імітують офіційні ресурси.

2.Злом акаунтів – використання слабких паролів або вразливостей систем.

3.Віруси та шкідливе ПЗ – програми, які збирають особисті дані.

4.Соціальна інженерія – маніпуляції для отримання інформації (наприклад, дзвінки від «банку»).

5.Збір даних через відкриті джерела – соцмережі, онлайн-форуми.

Як захистити свої персональні дані?

- ✓ Використовуйте **складні паролі** та двофакторну автентифікацію.,
- ✓ Не переходьте за **підозрілими посиланнями** та не відкривайте невідомі файли.
- ✓ Регулярно **оновлюйте програмне забезпечення** та антивірус.
- ✓ Не розголошуйте особисту інформацію **по телефону або в соцмережах**.
- ✓ Перевіряйте **налаштування конфіденційності** у своїх акаунтах.
- Якщо ваші дані вже викрадені – слід негайно змінити паролі, повідомити банк (якщо є фінансові ризики) та звернутися до кіберполіції.

Фейки та дезінформація

– це неправдива або маніпулятивна інформація, яка поширюється з метою впливу на суспільну думку, введення в оману або досягнення певних політичних, економічних чи соціальних цілей.

Основні види фейків та дезінформації:

- **Фейкові новини** – вигадані або перекручені факти, які подаються як справжні.
- **Пропаганда** – однобічна інформація, яка приховує частину правди.
- **Діпфейки** – змінені зображення чи відео, що імітують реальність.
- **Клікбейт** – сенсаційні заголовки, що вводять в оману.

Як розпізнати фейки?

✓ Перевіряйте джерела інформації.
✓ Аналізуйте, чи є підтвердження в офіційних джерелах.
✓ Використовуйте фактчекінгові ресурси.
✓ Будьте критичними до емоційно забарвлених заголовків.

Фейкові новини

Фейкові новини – це неправдиві або перекручені повідомлення, які подаються як реальні факти з метою маніпуляції суспільною думкою, створення паніки, дискредитації осіб або отримання фінансової вигоди.

Основні типи фейкових новин:
Повна вигадка – новина, яка не має жодних реальних підстав.
Перекручена інформація – правдиві факти подані з маніпулятивним акцентом.

Як розпізнати фейкові новини?
✓ **Перевіряйте джерело** – чи є воно надійним і відомим?
✓ **Шукайте підтвердження** – чи є новина в офіційних джерелах та авторитетних медіа?
✓ **Звертайте увагу на заголовки** – якщо вони надто сенсаційні або емоційні, це може бути маніпуляція.
✓ **Перевіряйте дату публікації** – старі новини можуть поширюватися як актуальні.
✓ **Аналізуйте автора** – чи має він репутацію експерта?
✓ **Фактчекінг** – використовуйте ресурси для перевірки інформації, наприклад, **StopFake, VoxCheck, Snopes.**

Фейки можуть мати серйозні наслідки: вони розпалюють паніку, створюють хаос і маніпулюють громадською думкою. Будьте уважні та не поширюйте неперевірену інформацію!

Пропаганда

– це цілеспрямоване поширення інформації, ідей або поглядів для впливу на суспільну думку, формування переконань та маніпуляції поведінкою людей. Вона може бути як позитивною (наприклад, соціальна реклама), так і негативною (маніпулятивна політична або військова пропаганда).

Як розпізнати пропаганду?

🔹 **Аналізуйте джерело** – чи воно надійне та незалежне?

🔹 **Перевіряйте альтернативні погляди** – чи є інші точки зору?

🔹 **Шукайте докази** – чи підкріплені твердження фактами?

🔹 **Звертайте увагу на емоційне забарвлення** – нейтральна інформація не має викликати сильних емоцій.

🔹 **Перевіряйте статистику** – чи вона реальна та об'єктивна?

Основні види пропаганди

- **Політична** – спрямована на підтримку певної ідеології, партії чи лідера.
- **Військова** – використовується під час воєн для деморалізації ворога або підняття бойового духу.
- **Комерційна (реклама)** – формування попиту на продукти чи послуги.
- **Релігійна** – поширення віровчень або релігійних ідей.
- **Соціальна** – спрямована на підвищення свідомості суспільства (наприклад, проти куріння або за екологію).

Методи пропаганди

- Маніпуляція фактами – висвітлення подій вибірково, щоб створити потрібне враження.
- Демонізація противника – представлення опонента в негативному світлі (наприклад, як загрозу).
- Апелювання до емоцій – використання страху, гніву, патріотизму або гордості.
- Повторення (ефект 25-го кадру) – чим частіше люди чують інформацію, тим більше вони в неї вірять.
- Авторитетні джерела – посилання на «експертів» або відомі особистості для підсилення довіри.
- Спотворені статистичні дані – маніпулювання цифрами для підтвердження потрібної точки зору.

Пропаганда є потужним інструментом, який може впливати на суспільство в глобальному масштабі. Тому важливо критично мислити, аналізувати інформацію та не піддаватися маніпуляціям.

Клікбейт

– це маніпулятивний метод подачі інформації, коли заголовок або зображення штучно привертають увагу користувача, змушуючи його клікнути на матеріал. При цьому зміст часто не відповідає очікуванням або значно перебільшений.

Основні ознаки клікбейту:

- **Сенсаційні заголовки** – **«ЦЕ ЗМІНИТЬ ВАШЕ ЖИТТЯ!», «ВАМ НЕ ПОВІРИТЬСЯ, ЩО СТАЛОСЯ ДАЛІ!»**
- **Емоційний тиск** – страх, обурення або захоплення (**«ВАС ОБМАНЮЮТЬ!», «НЕЙМОВІРНЕ ВІДКРИТТЯ!»**).
- **Недосказаність** – заголовок інтригує, але не дає конкретних фактів (**«ВІН ЗРОБИВ ЦЕ І ВСІ БУЛИ ШОКОВАНІ!»**).
- **Перебільшення або спотворення інформації** – «СМЕРТЕЛЬНА НЕБЕЗПЕКА У ВАШОМУ БУДИНКУ!» (а йдеться просто про пил).
- **Маніпулятивні зображення** – фото, що не відповідає змісту статті.

Чому клікбейт використовується?

Збільшення трафіку – чим більше кліків, тим більше переглядів і доходів.

Вірусний ефект – провокативний контент швидко поширюється.

Вплив на емоції – змушує користувача діяти імпульсивно.

Як розпізнати та уникати клікбейту?

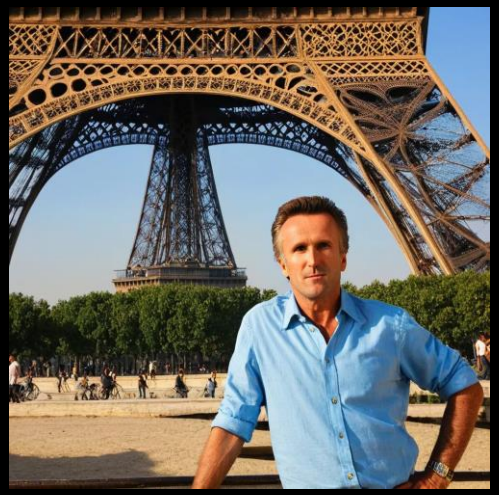
- **Читайте не лише заголовок**, а й перевіряйте зміст.
- **Перевіряйте джерело** – якщо сайт сумнівний, краще уникати.
- **Порівнюйте з іншими джерелами** – чи є ця новина в авторитетних медіа?
- **Не піддавайтеся на маніпуляції** – якщо заголовок надто емоційний, це привід засумніватися.
- **Використовуйте розширення для блокування клікбейту**, наприклад, Stop Clickbait.

Клікбейт – це не лише спосіб заманити читачів, але й інструмент маніпуляції. Будьте критичними до інформації, щоб не потрапити на гачок фейкових чи маніпулятивних новин!

Фотошоп та діпфейки

Фотошоп – це редагування фотографій за допомогою графічних редакторів (наприклад, Adobe Photoshop). Зображення можуть змінюватися для покращення якості або для введення в оману (наприклад, підроблені новини, зміна контексту фото).

Діпфейки (Deepfake) – це відео або зображення, створені за допомогою штучного інтелекту. Вони дозволяють замінювати обличчя людей, змінювати їхні голоси та імітувати рухи так, що це виглядає правдоподібно.



Як це використовують?

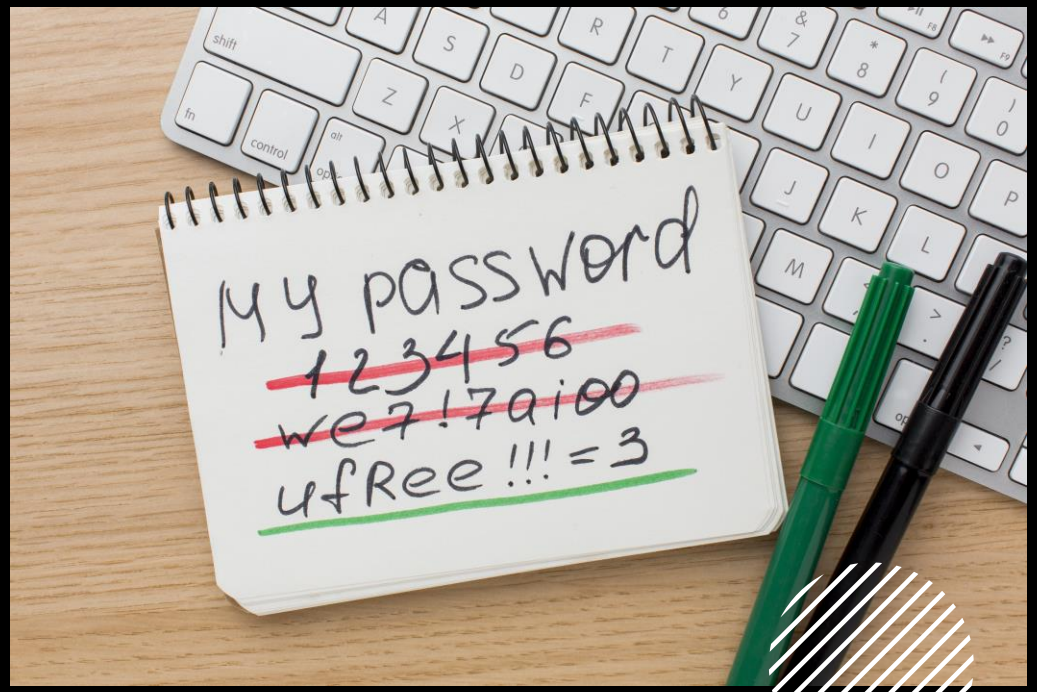
- ✓ У розвагах – фільми, меми, заміна акторів у кіно.
- У шахрайстві – підроблені відео або голоси для виманювання грошей.
- У пропаганді – фейкові виступи політиків, спотворення подій.
- У дискредитації людей – створення компрометуючих відео.

Як розпізнати підроблені фото та діпфейки?

Перевірте джерело – якщо фото чи відео з'явилося лише в одному місці, варто сумніватися.
Зверніть увагу на деталі – діпфейки часто мають нереалістичні очі, дивні тіні або спотворення навколо обличчя.
Використовуйте інструменти перевірки – Google Reverse Image Search, FotoForensics, Deepware Scanner.
Дивіться на природність рухів – у діпфейках можуть бути неприродні вирази обличчя або неправильна синхронізація губ і голосу.
Будьте критичними – якщо відео викликає сильні емоції або здається "занадто шокуючим", перевірте його ще раз.

Як створити надійний пароль

Не використовуйте як частину пароля адресу своєї вулиці, ім’я/прізвище, ім’я домашнього улюбленця чи іншу інформацію, яку легко дізнатися. Також ненадійним є поєднання послідовних літер і цифр на клавіатурі — саме по них насамперед проходяться зловмисники.



Використовуйте менеджери паролів. Це найпростіший спосіб убезпечити ваші облікові записи. Програма автоматично генеруватиме паролі і сама буде змінювати їх у встановлені терміни.

Не використовуйте пароль, який легко пригадати. У ньому не має бути інформації, яку про вас легко дізнатися.

Створюйте унікальні паролі з цілих речень, просто вставляючи в них перші літери кожного слова. Можете при цьому додавати цифри і додаткові символи — символіку такого пароля навряд чи хтось розгадає.

Змішайте в паролі не менше чотирьох випадкових слів. Вибір випадкових слів зазвичай добре працює, адже їх послідовність нелогічна.

Не використовуйте той самий пароль у різних місцях, наприклад, на роботі та вдома.

Нікому не повідомляйте свої паролі. Взагалі нікому — ця інформація повинна бути тільки у вас.

Не створюйте окремого файлу з усіма своїми паролями — його можуть викрасти й тоді неприємностей не уникнути.

Використовуйте багатофакторну автентифікацію.

Думайте, коли вигадуєте відповідь контрольне питання. Хакери можуть легко підібрати відповідь. Наприклад, на те, щоб дізнатися дівоче прізвище вашої матері, зловмисникам знадобиться всього кілька хвилин.

Змінивши пароль, більше ніколи не використовуйте його для інших облікових записів.

Захищайте свій комп’ютер та смартфон від кіберзагроз, встановивши антивірус і регулярно його оновлюючи.

Уважно дивіться на URL-адреси сайтів, на які заходите. Часто зловмисники підробляють їх, щоб обдурити своїх жертв. Особливо актуальна ця інформація для сайтів, на яких можна щось купити/продати.

У сучасному світі де цифрові технології займають центральне місце в усіх сферах життя, суспільство відіграє ключову роль у створенні безпечного цифрового середовища. Ця роль охоплює кілька важливих аспектів:

Роль суспільства у створенні безпечного цифрового середовища

- **Освіта та підвищення обізнаності:**
  Громадяни повинні знати як безпечно користуватися Інтернетом, захищати свої дані та розпізнавати кіберзагрози. Проведення інформаційних запитів та навчальних програм полегшення формування відповідної цифрової культури.
- **Формування етичних норм та стандартів:**
  Суспільство через активну участь громадських організацій, експертних груп і навіть окремих користувачів може сприяти створенню та впровадженню етичних стандартів, які регулюють поведінку в мережі. Це призведе до зниження рівня кіберзлочинності та нетерпимості.
- **Співпраця між прогресивними:**
  Безпечне цифрове середовище неможливо звільнити від труднощів окремих осіб або організацій. Співпраця державних установ, бізнесу та громадянського суспільства дозволяє створювати ефективні стратегії кібербезпеки, обмінюватися досвідом та швидко реагувати на нові загрози.
- **Активна участь у формуванні політики:**
  Громадяни можуть брати участь у дискусіях та консультаціях щодо розробки законодавчих ініціатив, що стосуються цифрової безпеки. Їхній досвід і відгуки допомагають прийняти більш збалансовані та ефективні рішення.
- **Підтримка інновацій та технологічного розвитку:**
  Суспільство сприяння розвитку інновацій через підтримку стартапів, наукових досліджень та новітніх технологій, які допомагають забезпечити високий рівень захисту даних і боротьби з кіберзагрозами.

Надмірне використання інтернету

або інтернет-залежність, є серйозною проблемою сучасного суспільства. Цей стан характеризується нав'язливим бажанням постійно бути онлайн та нездатністю контролювати час, проведений у мережі

Негативні наслідки надмірного користування інтернетом:

Фізичне здоров'я: Тривале перебування перед екраном може призвести до головного болю, нудоти, погіршення зору та проблем зі сном.

Психічне здоров'я: Надмірне використання інтернету пов'язане з підвищеним ризиком розвитку депресії, тривожних розладів та зниженням самооцінки.

Соціальна ізоляція: Люди, які проводять багато часу онлайн, можуть відчувати відчуження від реального світу, нехтувати стосунками з родиною та друзями, що призводить до соціальної ізоляції.

Зниження продуктивності: Надмірне перебування в інтернеті може негативно впливати на навчання та роботу, знижуючи концентрацію та ефективність виконання завдань.

Ознаки інтернет-залежності:

- Постійне бажання перевіряти повідомлення або оновлення.
- Відчуття тривоги або роздратування при неможливості доступу до інтернету.
- Нехтування повсякденними обов'язками та інтересами на користь онлайн-активностей.
- Спроби скоротити час онлайн без успіху.

Рекомендації для зменшення надмірного використання інтернету:

- Встановлення часових обмежень: Визначте конкретний час для перебування онлайн і дотримуйтесь його.
- Розвиток офлайн-хобі: Займайтеся діяльністю, яка не пов'язана з інтернетом, наприклад, спортом, читанням або творчістю.
- Соціальна взаємодія: Проводьте більше часу з родиною та друзями в реальному житті.
- Пошук професійної допомоги: Якщо ви відчуваєте, що не можете самостійно контролювати своє використання інтернету, зверніться до психолога або консультанта.
- Усвідомлення проблеми та активні кроки до її вирішення допоможуть підтримувати баланс між онлайн- та офлайн-життям, зберігаючи ваше фізичне та психічне здоров'я.

Висновки

Отже день безпечного Інтернету (Safer Internet Day) важливий, тому що він привертає увагу до безпеки в онлайн-просторі та допомагає формувати відповідальне цифрове середовище для:

Захист дітей та підлітків

Підвищення цифрової грамотності

Боротьба з кіберзлочинністю

Захист персональних даних

Відповідальна онлайн-поведінка

Об’єднання суспільства