БЕЗПЕКА В ІНТЕРНЕТІ

Пропонуємо вашій увазі тематичну презентацію, присвячену Дню безпечного інтернету. Цей захід має на меті привернути увагу до важливості дотримання правил безпеки в онлайн-просторі.

У презентації розглядаються ключові аспекти, такі як захист персональних даних, уникнення кібербулінгу, розпізнавання фейкової інформації та відповідальне використання цифрових ресурсів. Особливу увагу приділено практичним порадам для дітей, підлітків та дорослих щодо уникнення ризиків в інтернеті.

Презентація підготовлена відділом інформаційно-електронних ресурсів та сервісів загальної бібліотеки НАВС.

/ до Дня безпечного Інтернету

ІСТОРІЯ ТА ЗНАЧЕННЯ ДНЯ БЕЗПЕЧНОГО ІНТЕРНЕТУ

ІСТОРІЯ

День безпечного інтернету — це міжнародна ініціатива, що була започаткована у 2004 році Європейською мережею центрів безпечного інтернету (Insafe). Метою цього дня є підвищення обізнаності суспільства про важливість безпечного й етичного використання цифрових технологій, особливо серед дітей і молоді. Щороку цей день відзначається у другий вівторок лютого та об'єднує мільйони людей по всьому світу. Особливу увагу приділяють питанням кібербезпеки, захисту персональних даних та боротьбі з онлайн-шахрайством.

ЗНАЧЕННЯ

- Підкреслює важливість захисту персональних даних та конфіденційності.
- Нагода підвищити обізнаність про кіберзагрози та способи їх уникнення.
- Сприяє популяризації етичної поведінки в цифровому середовищі.
- Заохочує до відповідального використання технологій серед молоді та дорослих.
- Допомагає формувати культуру цифрової грамотності у суспільстві.

ОСНОВНІ ЗАГРОЗИ ТА РИЗИКИ В ІНТЕРНЕТІ

Фішинг, шахрайство та зломи акаунтів є одними з найпоширеніших форм кіберзлочинності. Зловмисники використовують хитрощі, щоб отримати доступ до конфіденційної інформації, такої як паролі чи банківські дані.

Соціальні мережі та інші онлайн-платформи збирають величезну кількість даних про користувачів. Це може призводити до витоку інформації або її використання без згоди.

Віруси, трояни та інші види шкідливого ПЗ можуть завдати шкоди пристроям або викрасти дані.

Образи, цькування та погрози в інтернеті є серйозною проблемою, особливо серед молоді.

КІБЕРЗЛОЧИННІСТЬ

ВТРАТА ПРИВАТНОСТІ

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

КІБЕРБУЛІНГ

ЯК ЗАХИСТИТИСЯ?!

- Використовуйте антивірусне програмне забезпечення.
- Перевіряйте джерела перед введенням особистих даних.
- Створюйте складні паролі та регулярно їх змінюйте.
- Уникайте підключення до публічних мереж без VPN.

Дотримуючись цих порад, ви зможете мінімізувати ризики та насолоджуватися безпечним використанням інтернету.

БЕЗПЕКА ДІТЕЙ В ОНЛАЙН-ПРОСТОРІ

Розробка правил користування інтернетом:
визначте чіткі межі часу та ресурсів, які дозволені для дітей, щоб уникнути надмірного використання.

Навчання цифровій грамотності:
поясніть дітям, як розпізнавати фейкову інформацію, онлайн-шахраїв та небезпечний контент.

Використання програм батьківського контролю:
встановіть спеціальні додатки для моніторингу активності дітей у мережі та обмеження доступу до небезпечних сайтів.

Захист персональних даних:
поясніть важливість конфіденційності та навчіть не ділитися особистою інформацією з незнайомцями.

Побудова довірливих відносин:
заохочуйте дітей ділитися своїми онлайн-досвідом і проблемами, щоб вчасно реагувати на можливі ризики.

Інформування про кібербулінг:
навчіть дітей розпізнавати ознаки цькування в інтернеті та розкажіть, як діяти в таких ситуаціях.

Регулярні перевірки активності:
переглядайте історію переглядів і спілкувань дитини, щоб запобігти можливим загрозам.

ВІДПОВІДАЛЬНЕ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ

УСТАНОВІТЬ ЧАСОВІ ОБМЕЖЕННЯ	• Використовуйте таймери або спеціальні додатки, щоб контролювати час, проведений у соціальних мережах. Це допоможе зосередитися на важливих завданнях
ФІЛЬТРУЙТЕ КОНТЕНТ	• Підписуйтесь лише на корисні та надихаючі сторінки. Уникайте токсичних або деструктивних акаунтів, які негативно впливають на ваш емоційний стан
ДОТРИМУЙТЕСЯ ПРИВАТНОСТІ	• Не публікуйте особисту інформацію, яка може бути використана зловмисниками. Регулярно перевіряйте налаштування конфіденційності
БУДЬТЕ КРИТИЧНИМИ ДО ІНФОРМАЦІЇ	• Перевіряйте джерела новин і не поширюйте неперевірені дані. Це допоможе уникнути дезінформації
РОЗДІЛЯЙТЕ РЕАЛЬНЕ ЖИТТЯ ТА ОНЛАЙН-ПРОСТІР	• Пам’ятайте про важливість живого спілкування та відпочинку без гаджетів
ВИКОРИСТОВУЙТЕ СОЦІАЛЬНІ МЕРЕЖІ ДЛЯ РОЗВИТКУ	• Беріть участь у професійних групах, навчальних курсах або вебінарах, щоб отримувати нові знання та навички

КІБЕРБУЛІНГ: причини, прояви та боротьба з ними

Кібербулінг є серйозною проблемою сучасного цифрового суспільства. Основними причинами цього явища є анонімність у мережі, недостатній контроль за поведінкою користувачів та низький рівень цифрової грамотності. Прояви кібербулінгу можуть включати образи, погрози, поширення неправдивої інформації або публікацію особистих даних без згоди.

Для боротьби з кібербулінгом важливо підвищувати обізнаність про його наслідки, впроваджувати освітні програми з цифрової етики та забезпечувати механізми захисту жертв.

ПРИЧИНИ КІБЕРБУЛІНГУ

Анонімність в інтернеті, відсутність контролю, бажання самоствердитися, помста або заздрість

ПРОЯВИ КІБЕРБУЛІНГУ

Образливі коментарі, поширення неправдивої інформації, погрози, створення фейкових акаунтів, публікація приватних даних

ШЛЯХИ БОРОТЬБИ

Підвищення цифрової грамотності, блокування кривдників, звернення до адміністрації платформи, підтримка жертв, розробка законодавчих механізмів

ПРОФІЛАКТИКА

Навчання етичної поведінки в інтернеті, проведення інформаційних кампаній, залучення батьків та вчителів до обговорення проблеми

ПІДСУМКИ ТА РЕКОМЕНДАЦІЇ

Інтернет є невід'ємною частиною нашого життя, але його використання вимагає обережності. Неправильна поведінка в мережі може призвести до витоку персональних даних, фінансових втрат або навіть психологічних проблем.

1

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Не розголошуйте конфіденційну інформацію, таку як паролі, банківські реквізити чи адреси. Використовуйте складні паролі та двофакторну аутентифікацію.

2

ОБЕРЕЖНІСТЬ ІЗ ПОСИЛАННЯМИ

Не переходьте за підозрілими посиланнями, навіть якщо вони надійшли від знайомих. Це може бути фішингова атака.

3

АНТИВІРУСНИЙ ЗАХИСТ

Встановіть та регулярно оновлюйте антивірусне програмне забезпечення.

4

КОНТРОЛЬ ДОСТУПУ ДІТЕЙ

Використовуйте батьківський контроль для обмеження доступу до небезпечного контенту.

5

КРИТИЧНЕ МИСЛЕННЯ

Перевіряйте достовірність інформації та джерел перед тим, як ділитися нею.