«Що мені загрожує в Інтернеті?»

МЕТА ПРОЕКТУ:

Дослідити ризики, пов'язані з використанням Інтернету

ЗАВДАННЯ ПРОЕКТУ:

Хто прагне проникнути до мого комп’ютера?

Хто за мною спостерігає?

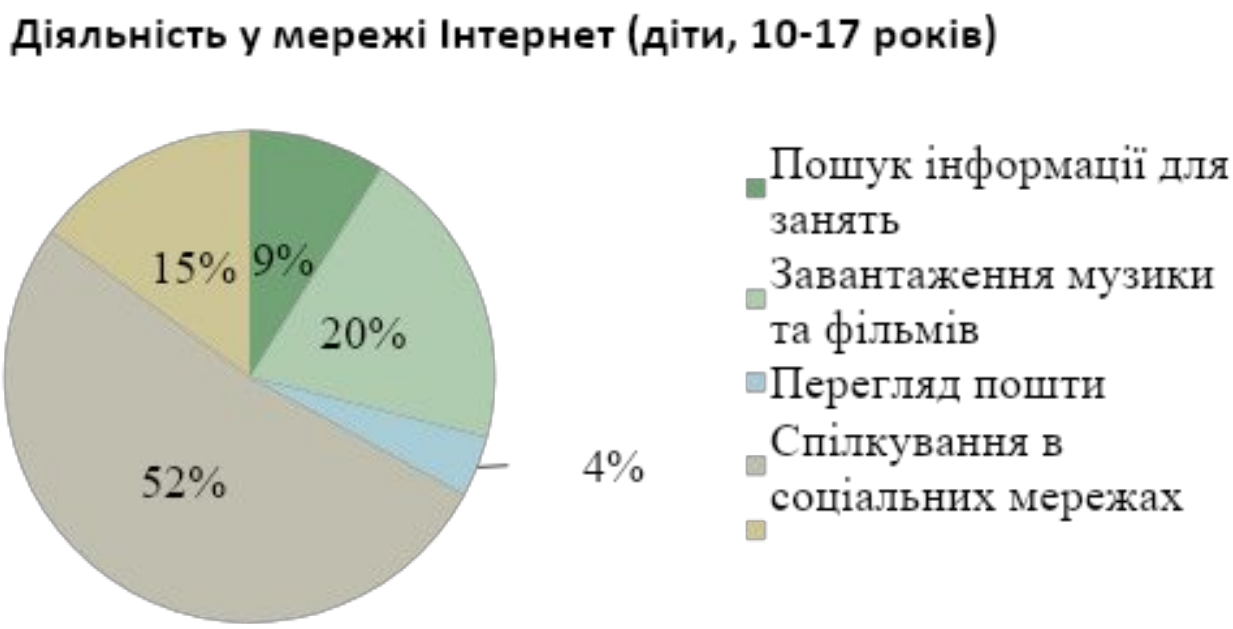
Як уберегтися від непроханих візітерів?

Як уберегти персональну інформацію від викрадення?

Як убезпечити себе в Інтернеті?

Завдяки інтернету діти та підлітки шукають необхідну інформацію для занять, завантажують музику та фільми, переглядають пошту, спілкуються з іншими користувачами Інтернету. Інтернет-технології стали природною складовою життя дітей і сучасної молоді. Комп'ютер є не тільки розвагою, але й засобом спілкування, самовираження та розвитку особистості

Що діти роблять в Інтернеті?



Що таке інформаційна безпека?

Інформаційна безпека — це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).

Що таке інформаційна загроза?

Загроза — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають атакою.

До переліку інтернет-загроз можна віднести:

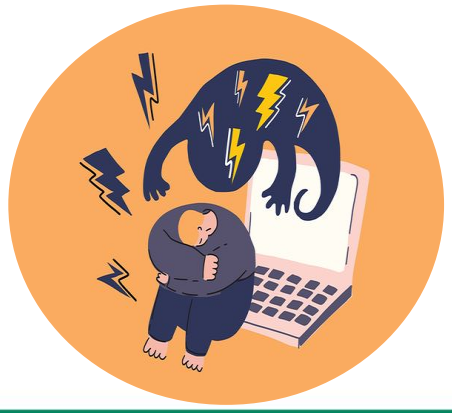
- Комп’ютерну залежність;
- Розходження між реальним «я» і своїм інтернет-образом;
- Доступ до небажаного контенту (дорослий контент);
- Інтернет-шахрайство;
- Зараження комп’ютера шкідливим програмним забезпеченням;
- Онлайн насильство.

Кібербулінг – це один із різновидів булінгу і є новітньою формою агресії, що передбачає жорстокі дії з метою дошкулити, нашкодити, принизити людину з використанням інформаційно-комунікаційних засобів: мобільних телефонів, електронної пошти, соціальних мереж тощо.

До найпоширеніших видів кібербулінгу належать: використання особистої інформації, анонімні погрози, хепіслепінг, переслідування, тролінг і флеймінг.

Флеймінг – це улюблений метод «тролів» (провокаторів), що полягає в обміні короткими, гнівними і запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології. Частіше за все розгортається в «публічних» місцях Інтернету: на чатах, форумах, у дискусійних групах, спільнотах. Інколи він перетворюється у затяжну війну.

Хепіслепінг – один із видів кібербулінгу, його назва походить від випадку в англійському метро, де підлітки били перехожих, тоді як інші записували це на камеру мобільного телефону. Тепер ця назва закріпилася за будь-якими відеороликами з записами реальних сцен насильства.



Спам

Спам - це масові розсилки, реклама, та будь-яка інша інформація, яка надходить до нас всупереч нашій волі. Спамом можуть бути в першу чергу електронні листи, пости та коментарі на блогах, форумах, інших сайтах, а також оффлайнова реклама.

Вебмайстри винайшли чимало способів незаконної реклами. Серед них - власне, сама реклама, антиреклама, т.зв. “нігерійські листи” (листи із закликом вислати гроші, щоб отримати взамін щось набагато більше), фішинг та інше.

Фішинг - це засоби та дії, які імітують поведінку будь-кого іншого. Метою зловмисників у випадку фішингу є викрадення паролів або пін-кодів, щоб в кінці перевести гроші жертви на свій рахунок.

Засоби захисту від спаму

- без потреби не публікуйте свою e-mail адресу будь-де.
- без потреби не реєструйтесь на сайтах, форумах чи блогах - ви таким передаєте їм свою інформацію, тим більше не треба реєструватися на підозрілих сайтах.
- не відповідати на спам чи переходити за посиланнями, що містяться в ньому.
- користуватись останніми версіями браузерів, котрі самі визначають чи підозрюється сайт у фішингу, а також останньою версією антивірусу.
- не тримати важливу інформацію в одному місці, завести хоча б кілька другорядних електронних скриньок.

Хакери

Хакери - це користувачі, що добре володіють всіма програмами по злому персональних комп'ютерів через мережу Інтернет. Хакери своїми діями намагаються отримати незаконний доступ до комп'ютерних даних іншого користувача.

Хакер зламує комп'ютер користувача шляхом програми шпигуна, яку він відправляє жертві в спамерському листі. І після прочитання такого листа програма успішно потрапляє в систему комп'ютера.

Як захиститися від хакерів

1. Користуйтеся складними паролями.

2. Користуйтесь антивірусним програмним забезпеченням. Обов'язкова умова - його постійне оновлення.

3. Працюйте з комп'ютером у режимі користувача. Якщо після встановлення операційної системи ви продовжуєте використовувати комп'ютер в режимі «Адміністратор», ви створюєте додаткові ризики зараження комп'ютера вірусами, які пропустила антивірусна система.

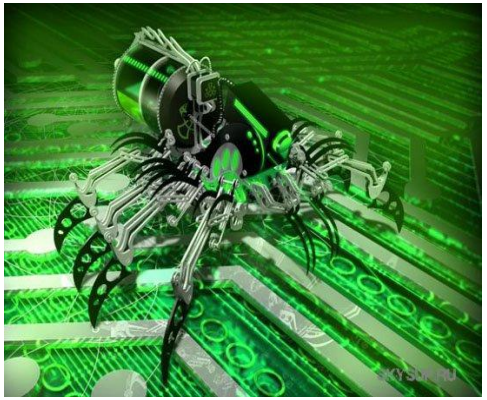
4. Виявляйте обережність при спробі підвищити власну анонімність.

Комп’ютерні віруси

Комп'ютерний вірус - це невелика програма, що написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій.

Основними джерелами вірусів є:

- Зовнішні носії інформації, на яких знаходяться заражені вірусом файли;
- комп'ютерна мережа, в тому числі система електронної пошти та Internet;
- жорсткий диск, на який потрапив вірус в результаті роботи з зараженими програмами;
- вірус, що залишився в оперативній пам'яті після попереднього користувача.



Заходи захисту від вірусів

- резервне копіювання інформації (створення копій файлів і системних областей жорстких дисків);
- уникнення користування випадковими й невідомими програмами. Найчастіше віруси розповсюджуються разом із комп'ютерними вірусами;
- перезавантаження комп'ютера перед початком роботи, зокрема, у випадку, якщо за цим комп'ютером працювали інші користувачі;
- обмеження доступу до інформації, зокрема фізичний захист дискети під час копіювання файлів із неї.

До програмних засобів захисту належать різні антивірусні програми (антивіруси). Антивірус - це програма, яка виявляє й знешкоджує комп'ютерні віруси.

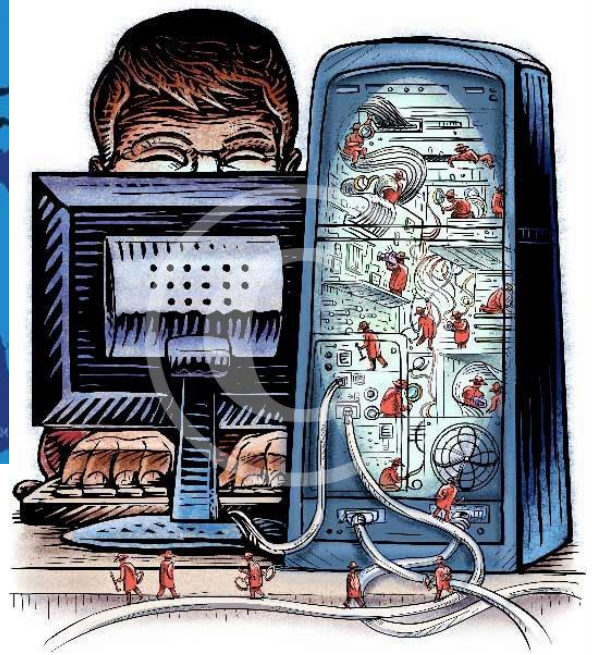
Трояни

Троянські віруси — це комп'ютерні програми, які добре вміють маскуватися під програмні продукти, а насправді виконують різні користувачем дії (збирають та пересилають, змінюють або псують інформацію, використовують ресурси комп'ютера на власний розсуд). Ці віруси самостійно не розмножуються. Вони видають себе за корисні програми, провокуючи користувача самостійно їх встановити.

Adware та Spyware

Adware (англ. Ad, Advertisement — реклама і Software — програмне забезпечення) — програмне забезпечення, яке в процесі свого використання показує користувачеві рекламу.

Spyware - шпигунське програмне забезпечення програмне забезпечення для відстежування (моніторингу) дій користувача, що вживається несанкціоновано



Дозвілля в інтернеті

Якщо у 2003 році в інтернеті проводили свій час лише 2% українців, то тепер це чи не найпопулярніший спосіб проведення вільного часу для 27% українців, грають у комп'ютерні ігри вже не 5—10%, а 15—25% молоді.

Так само активно змінює інтернет і практики спілкування. У мережі приймають і відправляють повідомлення електронною поштою, спілкуються в соціальних мережах, в чатах, на форумах, блогах, знайомляться на сайтах. Відбувається активне перенесення дозвілля молоді в інтернет-мережу. Інтернетизація життя значною мірою це життя змінює.

По-перше, людина може «лазити» в інтернеті по всьому світу, якщо знає іноземну мову. По-друге, це дає можливості об'єднуватися за інтересами, збиратися разом, створювати якісь групи. Звичайно, є і негативні наслідки — зменшення фізичної активності, а відповідно — погіршення здоров'я.

Небезпеки в Інтернеті можуть підстерігати кожного!

Важливо правильно користуватися мережею в будь-якому віці. Важливим є складання списку домашніх правил користування Інтернетом. Слід поставити обмеження на спілкування в чатах. З дітьми потрібно вести бесіди про їх спілкуванні. При цьому батьки повинні питати про це так, ніби про реальних друзів зі школи. Можна цікавитися людьми, з якими спілкується підліток за допомогою миттєвих повідомлень. Бесіда повинна бути дружньої. Інакше підліток не стане допускати батьків у свій особистий простір. Уберегти його від біди в цьому випадку буде непросто.

Правила безпечної роботи в Інтернеті

Заголовок слайда

Зараз в Україні майже 22 млн. користувачів інтернету, питання безпеки в мережі більш ніж актуальне. У цьому контексті турбота про дітей набуває більших масштабів. Якщо раніше треба було говорити з дітьми про їх безпеку поза домом тощо, то вже давно має сенс застерігати їх від негараздів під час перебування в Інтернеті.

Використані джерела:

Оригинальные шаблоны для презентаций:
https://presentation-creation.ru/powerpoint-templates.html
http://www.ukrreferat.com/index.php?referat=36222
http://kaspersky-antivirus.kiev.ua/reshenija/infosecur.html
http://pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi
http://h.ua/story/114317/
http://kaspersky-antivirus.kiev.ua/ugroz/xack.html
http://komphelp.net/Virus/Index1.htm
http://uchni.com.ua/informatika/5621/index.html
http://bibliofond.ru/view.aspx?id=439369
http://www.referatcentral.org.ua/sociology_load.php?id=255