Тема: Твоя інформаційна безпека в мережі Інтернет.

Мета: Розглянути можливості використання Інтернету, як мережі мереж; познайомити учнів з можливими загрозами, що чекають учнів в мережі та дати поради щодо захисту і етикету в Інтернеті. Розвивати логічне мислення учнів. Виховувати інформаційну культуру учнів.

Тип уроку: урок лекція

Обладнання: презентація «Твоя інформаційна безпека в мережі Інтернет», плакати: «Інтернет», «Сервіси Інтернету»

Хід уроку

I. Організаційний момент

Організація роботи групи:

Привітання
Перевірка присутніх
Підготовка учнів до уроку

II. Актуалізація опорних знань

За допомогою фронтальної бесіди та презентації повторити:

Що таке комп'ютерна мережа?
Що таке Інтернет?

Які сервіси Інтернету Вам відомі?

Слайд 3

III. Мотивація навчальної діяльності

Користуючись Інтернетом чи часто Ви задумувались:

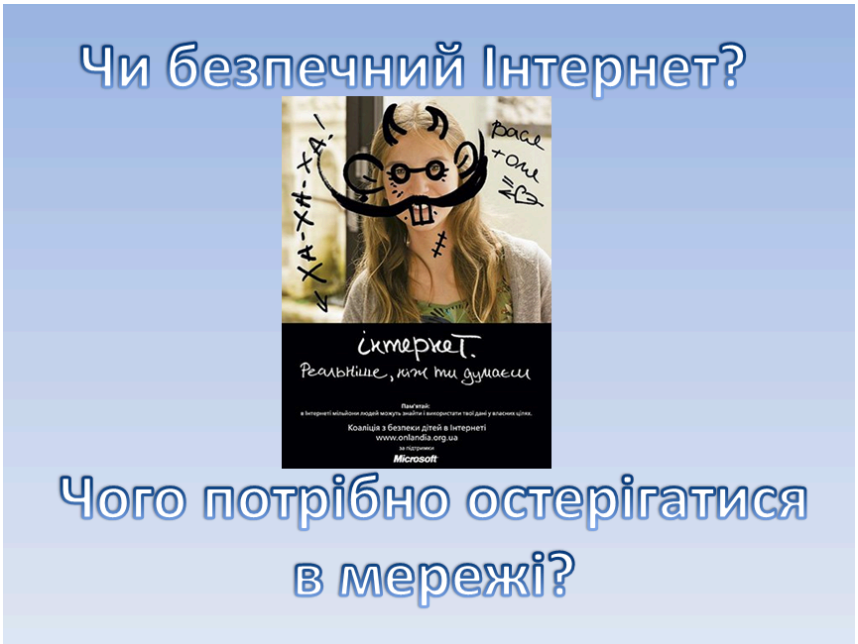
Чи безпечний Інтернет?

Які загрози приховуються в ньому?

Яким чином захиститися в мережі Інтернет?

Вивчаючи дану тему ми з’ясуємо які небезпеки приховані в Інтернеті, як захистити себе в мережі…

Слайд 4



IV. Вивчення нового матеріалу

Комп’ютерний вірус – це невелика програма, яка має здатність розмножуватися та знищувати інформацію, блокувати роботу комп’ютера. На сьогоднішній день відомо понад 50 тисяч вірусів і їх кількість зростає кожного дня. Проявляється дія вірусів на комп’ютері по різному: уповільнення роботи, затримки при виконанні програм, незрозумілі зміни у файлах, зникнення файлів, візуальні ефекти, форматування жорсткого диска, незрозумілі системні повідомлення та звукові ефекти, самовільне відкривання браузером деяких сайтів (рекламного характеру) та інше. Одним із видів вірусів є **хробаки.** Вони схожі на віруси, так як розмножуються і роблять власні копії, але на відміну від вірусів не потребують носія і передаються здебільшого через електронну пошту. Хоча спершу хробаки були не були шкідливими,

нинішні їхні різновиди спричиняють значні перезавантаження мереж і можуть руйнувати файли. Так, вірус Mellisa, перший з тих, що атакували системи електронної пошти, з моменту своєї появи в 1991 році заподіяв збитків на 80 млн. длр.

Слайд 5

Хакери та крекери.

Ха́кер (від англ. to hack — рубати) — особливий тип комп'ютерних спеціалістів. Нині так часто помилково називають комп'ютерних хуліганів, тобто тих, хто здійснює неправомірний доступ до комп'ютерів та інформації. Інколи цей термін використовують для позначення спеціалістів взагалі — у тому контексті, що вони мають дуже детальні знання в якихось питаннях, або мають достатньо нестандартне і конструктивне мислення. З моменту появи цього слова в формі комп'ютерного терміну (започаткованого в 1960-ті роки), в нього з'явилися достатньо різноманітні значення. Обдарований програміст, ентузіаст своєї справи, прихильник свободи та відкритості інформації.

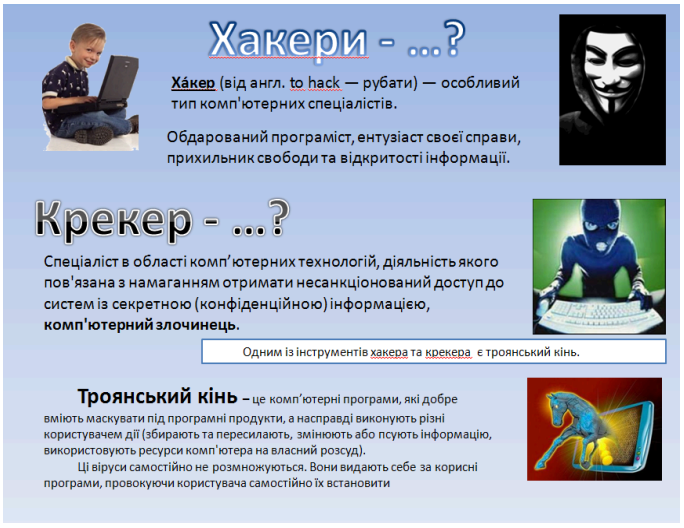
Крекер — Спеціаліст в області комп'ютерних технологій, діяльність якого пов'язана з намаганням отримати несанкціонований доступ до систем із секретною (конфіденційною) інформацією, комп'ютерний злочинець. [2]

Одним із інструментів хакера та крекера є троянський кін.

Троянський кінь – 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).[3]

Ці віруси самостійно не розмножуються. Вони видають себе за корисні програми, провокуючи користувача самостійно їх встановити.

Окремі категорії троянських вірусів здатні завдавати збитків віддаленим комп'ютерам та мережам, не порушуючи працездатності зараженого комп'ютер



Слайд 6

Одним із видів діяльності хакерів та крекерів є створення власних Ботнерів або бот мереж. В можете працювати на своєму комп'ютері і не підозрювати що є частиною групи, яка здійснює атаку на віддалений сервер, розсилає спам, краде конфіденційну інформацію.

Ботне́т (англ. botnet від robot і network) — це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп'ютері жертви і дозволяє зловмисникові виконувати певні дії з використанням ресурсів інфікованого комп'ютера. Зазвичай використовуються протиправної діяльності — розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні, отримання персональної інформації про користувачів, крадіжка номерів кредитних карт та паролів доступу.[4]

Комп'ютер може потрапити в мережу ботнету через встановлення певного програмного забезпечення, без відома користувача. Трапляється це зазвичай через:

Інфікування комп'ютера вірусом через вразливість в ПЗ (помилки в браузерах, поштових клієнтах, програмах перегляду документів, зображень, відео).

Недосвідченість або неуважність користувача — шкідливе ПЗ маскується під "корисне програмне забезпечення".

Використання санціонованого доступу до комп'ютера (рідко).

Брут адміністративного пароля до розшарених ресурсів (наприклад, до $ADMIN, що дозволяє віддалено виконати програму) - переважно в локальних мережах.[4]

віддалено виконати програму) - переважно в локальних мережах.[4]

Слайд 7.

Спам.[6]

Спам (англ. spam) — масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів. Також вважаються спамом освідчення в коханні на електронну пошту, в чатах, соціальних мережах і т.п. Найчастіше спам використовують для розсилання реклами, але є й інші сфери його застосування:

реклама незаконної продукції

нігерійські листи (ноді спам використовується для того, щоб виманити гроші в одержувача листа. Найпоширеніший спосіб одержав назву «нігерійські листи», тому що дуже багато таких листів приходило з Нігерії. Такий лист містить повідомлення про те, що одержувач листа може одержати якимось чином велику суму грошей, а відправник може йому в цьому допомогти. Потім відправник листа просить перерахувати йому трохи грошей: наприклад, для оформлення документів чи відкриття рахунку. Виманювання цієї суми і є метою шахраїв.)

фітинг

масове розсилання листів релігійного змісту

масове розсилання листів, містять комп'ютерні віруси

масове розсилання листів з метою виведення комп'ютерної системи із ладу.

Слайд 8

Інтернет шахрайство. [5]

Сказати що в Інтернеті існує шахрайство – це не сказати нічого. Інтернет– це рай для шахрайства.

1. Фальшиві товари на аукціонах

На онлайн-аукціонах типу eBay досить часто попадаються фальшиві товари. І незважаючи на те, що в того ж eBay є комісія для відстеження шахраїв, однаково ймовірність купити підробку існує, навіть якщо надані сертифікати, котрі підтверджують справжність.

Ще на інтернет-аукціонах бувають випадки накручування ціни за допомогою спільників. Продавець з іншого акаунту або його друзі підвищують ставку, щоб ви заплатили більше. Тому якщо якийсь користувач часто трапляється у списку тих, що зробили ставки в одного продавця, можливо, він просто накручує ціну. І ще одне: ніколи не

переказуєте гроші за товар напряму. Якщо вам нічого не надішлють, повернути гроші в такому випадку буде практично неможливо.

2. Банківська афера, або фішинг

Якщо ви отримали електронного листа від свого банку, в якому сказано, що хтось намагався скористатись вашим рахунком, і для розблокування рахунку вам необхідно передати банку інформацію, що підтверджує особу, у жодному разі не слід цього робити. Банки ніколи не запитують таку інформацію через е-мейли. Аферисти (фішери), отримавши вашу особисту інформацію, скористаються нею для одержання доступу до вашого ж банківського рахунку.

3. Афера «Ви виграли безкоштовний Xbox!»

Щоразу, коли вам в Інтернеті безкоштовно пропонують те, за що зазвичай треба платити, варто бути вкрай обережним. Виробники товарів, які ви «виграли, отримавши е-мейл» – комерційні організації, і в їхні плани не входить роздавати тисячі Xbox'ів, Ipod'ів чи інших гаджетів безкоштовно. У таких аферах звичайно просять оплатити тільки доставку, якої, природно, не буде.

4. Благодійна афера

Як тільки трапляється трагедія, що вимагає доброчинності, активізуються не тільки благодійні фонди, але й аферисти. Якщо вам приходить е-мейл із проханням про внесок, не варто зразу пересилати гроші. Впевніться на 100%, що ці кошти підуть куди треба. А взагалі в таких випадках краще довіряти великим благодійним організаціям, таким як Червоний Хрест або Міжнародна амністія.

5. Шантаж

Іноді трапляється, що «жертві» приходить лист із погрозами викрадення кого-небудь із близьких і вимогами перерахувати енну сумі грошей на рахунок відправника листа. Звичайно ж, це афера. Навіть

якщо ви відчуваєте, що хтось справді може викрасти ваших родичів або має у розпорядженні компромат, найкраще звернутися в правоохоронні органи.

Буває й зворотна ситуація: вам приходить лист від сищиків, які знайшли ваші контакти в затриманого злочинця, і просять допомогти в розслідуванні. Насправді аферисти просто виманюють у вас особисту інформацію.

Слайд 9

Online-хижаки[7]

Використання таких інструментів комунікації в Інтернеті, як чат-кімнати, електронна пошта та обмін миттєвими повідомленнями, може поставити дитину під потенційну загрозу зустрічі з он-лайн-хижаками. Анонімність Інтернету означає, що довіра та тісний зв’язок в он-лайні можуть виникати досить швидко. Хижаки користуються цією анонімністю, щоб будувати свої взаємовідносини з недосвідченими молодими людьми. Батьки можуть захистити своїх дітей, якщо вони будуть обізнані з ризиками он-лайн-спілкування та цікавитимуться діяльністю своїх дітей у мережі Інтернет. Батькам потрібно бути добре

поінформованими, щоб отримати відповіді на свої запитання про те, як діють он-лайн-хижаки, хто ризикує стати їхньою жертвою та як знизити для своєї дитини ризик стати мішенню інформаційних атак.

Як діють он-лайн-хижаки?

Хижаки встановлюють контакт із дітьми шляхом розмов у чат-кімнатах, обміну миттєвими повідомленнями, завдяки електронній пошті або дошкам повідомлень. Багато підлітків користуються он-лайн-форумами підтримки ровесників для розв'язання своїх проблем. Хижаки часто відвідують такі зони в он-лайні для пошуку вразливих жертв. Он-лайн-хижаки намагаються поступово спокусити своїх жертв, виявляючи по відношенню до них увагу, доброту або навіть пропонуючи подарунки. Як правило, не шкодують ні часу, ні грошей, ні енергії. Вони в курсі найостанніших музичних новинок і все знають про хобі, які цікавлять дітей. Вони вислуховують дітей і співчувають їхнім проблемам, намагаються «послабити комплекси» молодих людей, поступово вводячи у свої розмови сексуальний контекст або показуючи їм відверто сексуальні матеріали. Деякі он-лайн-хижаки намагаються одразу ж втягнути дітей у відверто сексуальні розмови. Цей більш прямолінійний підхід може включати і сексуальне домагання. Хижаки також можуть запрошувати дітей, з якими вони знайомляться в он-лайні, до контакту віч-на-віч.

Хто ризикує стати жертвою он-лайн-хижаків?

Юнаки та дівчата є найбільш вразливою категорією, яка знаходиться під загрозою контактів з он-лайн-хижаками. Молодь досліджує свою сексуальність, виходить з-під батьківського контролю й шукає нових стосунків за межами сім'ї. Виходячи в Інтернет під маскою анонімності, вони, скоріш за все, ризикують стати чиїмись жертвами в он-лайні,

цілком не розуміючи до кінця можливих наслідків. Молоді люди, які є найбільш вразливими для он-лайнових хижаків, мають наступні риси:

• Вони новачки в он-лайні й незнайомі з «мережевим етикетом».

•Завзяті користувачі комп'ютера.

• Хочуть спробувати щось нове, авантюрне у житті.

• Активно шукають уваги та теплих стосунків.

• Бунтівні.

• Ізольовані або самотні.

• Допитливі.

• Збентежені в плані статевої приналежності.

• Занадто довірливі, яких можна легко ошукати.

• Їх приваблюють субкультури, що існують за межами їхнього контрольованого батьками світу.

Діти вважають, що вони знають про всю небезпеку хижаків, але насправді вони наївні, коли мова йде про он-лайн-стосунки.

Слайд 9

Перегляд відео-фрагменту «Фільм про правила безпеки в Інтернеті»

ПРАВИЛА Інтернет-БЕЗПЕКИ І Інтернет-ЕТИКИ ДЛЯ ДІТЕЙ І ПІДЛІТТКІВ[8]

Ніколи не давайте приватної інформації про себе (прізвище, номер телефону, адресу, номер школи) без дозволу батьків.

Якщо хтось говорить вам, надсилає вам, або ви самі віднайшли у мережі щось, що бентежить вас, не намагайтеся розібратися в цьому самостійно. Зверніться до батьків або вчителів - вони знають, що треба робити.

Зустрічі у реальному житті із знайомими по Інтернет-спілкуванню не є дуже гарною ідеєю, оскільки люди можуть бути дуже різними у електронному спілкуванні і при реальній зустрічі. Якщо ж ви все ж хочете зустрітися з ними, повідомте про це батьків, і нехай вони підуть на першу зустріч разом з вами

Не відкривайте листи електронної пошти, файли або Web-сторінки, отримані від людей, яких ви реально не знаєте або не довіряєте.

Нікому не давайте свій пароль, за виключенням дорослих вашої родини.

Завжди дотримуйтесь сімейних правил Інтернет-безпеки: вони розроблені для того, щоб ви почували себе комфортно і безпечно у мережі.

Ніколи не робіть того, що може коштувати грошей вашій родині, окрім випадків, коли поруч з вами батьки.

Завжди будьте ввічливими у електронному листуванні, і ваші кореспонденти будуть ввічливими з вами.

У електронних листах не застосовуйте текст, набраний у ВЕРХНЬОМУ РЕГІСТРІ - це сприймається у мережі як крик, і може прикро вразити вашого співрозмовника.

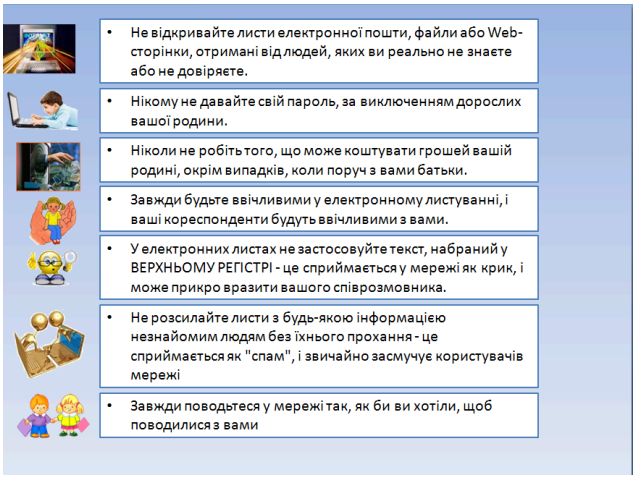
Не надсилайте у листі інформації великого обсягу (картинки, фотографії тощо) без попередньої домовленості з вашим співрозмовником.

Не розсилайте листи з будь-якою інформацією незнайомим людям без їхнього прохання - це сприймається як "спам", і звичайно засмучує користувачів мережі

Завжди поводьтеся у мережі так, як би ви хотіли, щоб поводилися з вами!

Слайд 12

Слайд 13



Слайд 14

V. Закріплення нового матеріалу

VI. Підведення підсумків

Фронтальна бесіда з учнями за запитаннями:

Інтернет – що це?

Які небезпеки підстерігають Вас в Інтернеті?

Хакери – добро, чи зло? Крекери -…?

Яких правил потрібно дотримуватися, щоб забезпечити собі безпеку в мережі?

VII. Домашнє завдання

Вивчити матеріал конспекту

Створити малюнок на тему «Твоя інформаційна безпека в мережі Інтернет» (для учнів 8 класів)

Словник

Інтернет – це всесвітня комп'ютерна мережа, що об'єднує різні мережі та окремі комп'ютери (вони називаються хост-комп'ютерами, від англ. Host – хазяїн)

Протокол - це сукупність правил обміну інформацією між комп'ютерами, встановлених зав взаємною угодою.

Комп'ютери - маршрутизатори – визначають шлях, яким повинні проходити пакети від одного комп'ютера до другого, користуючись таблицями й алгоритмами маршрутизації.

Доменні адреси – унікальні імена комп'ютерів в Інтернет.

IP – адреса (або цифрова адреса) – запис, який точно визначає місцезнаходження комп'ютера в Інтернеті і є записом чотирьох чисел у діапазоні від 0 до 255, відділених крапками, наприклад, 220.15.68.33

TCP/IP – основний транспортний протокол передавання даних в Інтернеті. Абревіатура TCP/IP складається з двох частин: TCP(Transmition Control Protocol протокол керування передаванням) і IP(Internet Protocol –протокл Інтернет)

Ха́кер (від англ. to hack — рубати) — особливий тип комп'ютерних спеціалістів. Нині так часто помилково називають комп'ютерних хуліганів, тобто тих, хто здійснює неправомірний доступ до комп'ютерів та інформації. Інколи цей термін використовують для позначення спеціалістів взагалі — у тому контексті, що вони мають дуже детальні знання в якихось питаннях, або мають достатньо нестандартне і конструктивне мислення. З моменту появи цього слова в формі комп'ютерного терміну (започаткованого в 1960-ті роки), в нього з'явилися достатньо різноманітні значення

Шахрайство — заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою.

Фі́шинг (англ. phishing МФА: ['fiʃiŋ] від fishing — рибальство) — вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтівонлайнових аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів.

Спам (англ. spam) — масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів.

Список використаних джерел

http://uk.wikipedia.org/wiki/Комп'ютернийвірус

http://uk.wikipedia.org/wiki/хакер

http://uk.wikipedia.org/wiki/Троянськийвірус

http://uk.wikipedia.org/wiki/Ботнер

http://www.rate1.com.ua/ua/ekonomika/tekhnologiji/1538/

http://uk.wikipedia.org/wiki/Спам

http://informaiklern.blogspot.com/2012/02/online.html

http://chl.kiev.ua/default.aspx?id=88

www.onlandia.org.ua

Гаєвський О.Ю. Інформатика: 7-11 кл. Навч. посіб. - К.: Видавництво А.С.К., 2003. – 512с.: іл.

Руденко В.Д., Макарчик О.М., Патланжоглу М. О. Практичний курс інформатики / За ред. Мадзігона В.М. – К.: Фенікс, 1997. – 304 с.

Інформатика: Підручник для 10-11 кл. загальноосвіт. навч. закладів / І.Т. Зарецька, А.М. Гурій, О.Ю.Соколов. У 2-х част.- К.: Форум, 2004. – 288 с.: іл.

Верлань А.Ф., Апатова Н.В. Інформатика: Підруч. для учнів 10-11 кл. серед. загальноосв. шк. – К.: Форум, 2000 – 223 с.

Александр Левин Самоучитель работы на компьютере (6-е издание, исправленное и дополненное) Москва, издательство «Нолидж», 2001 – 624 с.