Первомайський будинок дитячої та юнацької творчості

Первомайської міської ради Харківської області

БЕЗПЕКА

В ІНТЕРНЕТІ

Автор: **Єфименко Владислав**, 13 років

вихованець Первомайського

будинку дитячої та юнацької творчості

гурток «Інформатика»

Керівник гуртка **Маркова Н.В**.

Первомайський - 2019

З М І С Т

ВСТУП

Кількість користувачів мобільних телефонів та інтернету щодня невпинно збільшується. Більшою їхньою частиною є молодь. Особливу небезпеку незахищений інформаційний простір приховує для дітей. Інтернет може містити інформацію агресивного чи соціально небезпечного змісту. А надання переваги віртуальному світу перед реальним справляє негативний вплив на психіку і здоров'я дитини та може погіршити не тільки зір, поставу та сон, але й викликати тривожність, дратівливість, соціальну дезадаптованість і узалежнену поведінку. Для когось інтернет може бути єдиним джерелом спілкування, але слід враховувати те, що віртуальна реальність ніколи не замінить гармонійних взаємин і повноцінного спілкування між людьми. Щоб запобігти всім тим негативним явищам та небезпекам, які очікують в Інтернеті, необхідно навчитися правильній поведінці та безпечним користуванням сучасними Інтернет – технологіями.

І Н Т Е Р Н Е Т

П Е Р Е В А Г И	**Н Е Д О Л І К И**
задовольняють інформаційні, освітні, культурні потреби, відкривають безмежний простір для спілкування та самовираження.	фінансові шахраї, хакери, різного роду дезінформатори, тенета спокус (порноіндустрія, комп'ютерні ігри тощо).

Що таке інформаційна безпека?

Під інформаційною безпекою розуміється захищеність інформації та підтримує її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктурі. [2]

Складові інформаційної безпеки

- Конфіденційність - стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на нього право.
- Цілісність - уникнення несанкціонованої модифікації інформації.
- Доступність - уникнення тимчасового або постійного захування інформації від користувачів, що отримали права доступу.

ОСНОВНА ЧАСТИНА.

Що загрожує інформаційній системі?

Хто прагне проникнути до мого комп'ютера?

Кожен користувач Інтернету повинен мати чітке уявлення про основні джерела безпеки, що йому загрожують. Це насамперед діяльність хакерів, а також віруси та 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, так звані “нігерійські листи” (листи із закликом вислати гроші, щоб отримати взамін щось набагато більше), фішинг та інше.

Фішинг - вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів 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. [1]

Кардінг - від шахрайства, при якому проводиться операція з використанням банківської картки або її реквізитів, яка не ініційована або не підтверджена її власником. Реквізити платіжних карток, як правило, беруть зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також з персональних комп'ютерів.

Скімінг – від шахрайство шляхом зчитування даних з допомогою спеціального обладнання, яке фіксує дані магнітної стрічки банківської картки і її пін-код.

Засоби захисту від Інтернет – шахрайства

- не переходити за посиланнями для оплати на неперевірених ресурсах;
- використовувати складні паролі (мінімум 8 символів у комбінації великих та малих літер, цифр та символів);
- завжди перевіряти стан банкоматів, з яких знімаються кошти;
- не проводити фінансові операції із використанням відкритих мереж Wi-Fi

Засоби захисту від спаму

- без потреби не публікуйте свою e-mail адресу будь-де.
- без потреби не реєструйтесь на сайтах, форумах чи блогах - ви також передаєте їм свою інформацію, тим більше не треба реєструватись 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.

П’ять правил використання електронної пошти:

1. Ніколи не відкривай підозрілі повідомлення. Відразу видаляй їх, вибравши відповідну команду в меню повідомлення.

2. Ніколи не відповідай на небажану пошту.

3. Використовуй фільтр спаму свого провайдера інтернет-послуг або програми електронної пошти.

4. Використовуй нову або родинну адресу електронної пошти для запитів в Інтернеті, форумів тощо.

5. Ніколи не пересилай «ланцюгові» повідомлення електронної пошти. Видаляй їх одразу після надходження.

Хакери та крекери

Хакер (від англ. to hact- рубати) – особливий тип комп'ютерних спеціалістів. Обдарований програміст, ентузіаст своєї справи, прихильник свободи та відкритості інформації, яка без дозволу проникає до чужої комп'ютерної системи з наміром викрасти або зруйнувати дані.

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

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.

Способи проникнення хакерів та крекерів до чужих систем.

Троянські коні. Це шкідливі програми, які розповсюджуються шляхом обману, які добре вміють маскувати під програмні продукти, а насамперед виконують різні дії (збирають або псують інформацію, використовують ресурси комп'ютера на власний розсуд). Так, вам може надійти електронною поштою лист, де буде сказано, що програма, яка знаходиться у вкладенні, виконує якусь корисну функцію. Якщо ви запустите її на виконання, ваш комп'ютер буде заражений. Троянські коні відкривають хакерам доступ до системи, можуть спричинити руйнування інших та виконання інших програм. Це віруси самостійно не розмножуються, вони видають себе за корисні програми, провокуючи користувача самостійно їх встановити. [4]

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

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. [3]

Віруси та хробаки

Існують програми, що мандрують Інтернетом та, потрапивши на комп'ютер чи до локальної мережі, завдають тієї чи іншої шкоди. Особливо небезпечними є два види таких програм — віруси та хробаки.

Віруси. Програми названі на ім'я біологічних організмів, бо вони досить малі, розповсюджуються, роблячи копії з самих себе, та не можуть існувати без носія.

Комп'ютерний вірус - це невелика програма, що написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій.[3]

Основними джерелами вірусів є:

- дискета, на якій 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.

Хробаки розповсюджуються швидше за віруси безпосередньо з одного комп’ютера на інший. Наприклад, хробак електронної пошти може сам відправляти себе на всі адреси електронної пошти в адресній книзі користувача. Інтернет-хробаки шукають підключені до Інтернету комп’ютери, які не містять найостанніших оновлень безпеки. Хробак схожий на вірус тим, що розмножується, роблячи власні копії, але на відміну від останнього він не потребує носія й існує сам по собі. Часто хробаки передаються через електрону пошту. Хоча спершу хробаки не були шкідливими, нинішні їхні різновиди спричиняють значні перенавантаження мереж і можуть руйнувати файли.

Найкращим способом захисту комп’ютера є використання **брандмауера** та регулярне оновлення **операційної системи.**

Рекомендації:

- використовувати тільки ліцензійне програмне забезпечення;

- використовувати антивірусні програмні засоби;
- постійно слідкувати та оновлювати програмні продукти, особливо операційні системи;
- не завантажуйте, а тим паче не відкривайте додатки до листів, які отримані з недовіреної адреси;

Хто за мною спостерігає?

Крім програм, за допомогою яких певні люди намагаються проникнути до вашої системи, існують також засоби, що застосовуються для спостереження за вами. Це насамперед програмне забезпечення, яке зазвичай називають adware та spyware, шпигунські програми, програми для батьківського контролю, блокуючи програми тощо.

Ці програми можуть відстежувати ваші звички стосовно мандрування Інтернетом, надсилати комусь дані без вашого дозволу, змінювати адресу домашньої сторінки вашого браузера і навіть змінювати системні файли комп'ютера.

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 [4]

Авторське право і плагіат

Плагіат — привласнення авторства на чужий твір науки, літератури, мистецтва або на чуже відкриття, винахід чи раціоналізаторську пропозицію, а також використання у своїх працях чужого твору без посилання на автора.

Плагіатом вважається:

- крадіжка ідеї або слова іншої людини і видача їх за власні;
- використання результатів роботи іншої людини без вказання джерела, звідки вони були взяті;

- повна або часткова крадіжка мистецького, наукового або іншого твору чи роботи та видача їх за свою;
- представлення вже існуючої ідеї або продукту як новий та оригінальний .

Авторське право — набір виключних прав, які дозволяють авторам отримати соціальні блага від результатів своєї творчої діяльності. АП історично виникла внаслідок потреби захистити права авторів літературних творів та творів мистецтва.

Зі збільшенням кількості Інтернет-ЗМІ плагіат як приписування собі чужої інтелектуальної власності або її творче використання: переклад, адаптація, аранжування без отримання належного дозволу набуває все більших масштабів. Копі Пастери нехтують застереженням автора про заборону вільно використовувати його матеріал, як того вимагає ст. 21 Закону України „Про авторське право й суміжні права”

Основні «заповіді» мережевої моралі [4]

1. Пам’ятайте, що Ви спілкуєтеся з людиною. (Не роби іншим того, чого не хочеш отримати від них взамін.)

2. Дотримуйтеся тих самих правил поведінки, що і в реальному житті. (Краще дотримуватися закону як в реальному, так і у віртуальному житті.)

3. Зберігайте особистість. (Пам’ятайте, що враження про Вас скрадатиметься з Ваших висловлювань.)

4. Допомагайте іншим там, де Ви спроможні це зробити. (Обмін досвідом у мережі – захоплива справа.)

5. Не втручайтесь у конфлікти і не допускайте їх. (Флейми – емоційні висловлювання, що часто не врахують думки інших.)

6. Пам’ятайте про безпеку. (Можна легко стати мішенню для он-лайн злочинців.)

7. Поважайте право на приватне листування. (Неповага до таємниці листування – це ознака поганих манер.

8. Пам’ятайте про авторське право. (Не оголошуйте інформацію, завантажену з Інтернету, своєю власною.)

9. Не зловживайте своїми можливостями. (Деякі «нетизяни» відчувають себе професіоналами.)

10. Вчіться пробачати помилки іншим. (Не будьте зарозумілими і гордовитими.)

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.

Як убезпечити себе в Інтернеті?

В Інтернеті дійсно можна зустріти багато суб'єктів з недобрими намірами, але це не є приводом для того, щоб відмовитися від користування цією мережею. Дотримуйтесь кількох простих правил, і ви будете гарантовані, що жодна людина з нечесними намірами не отримає доступу до вашої персональної інформації.

Завжди звертайтеся до батьків чи учителів з будь-яких питань, пов'язаних із користуванням Інтернетом. Візьміть за звичку не надавати свою персональну інформацію в кімнатах чату та системах обміну миттєвими повідомленнями. Ніколи не погоджуйтеся на зустріч із людиною, з якою ви познайомилися через

Інтернет. Не надсилайте своє фото інтернет-знайомим. Ніколи не давайте незнайомим людям таку інформацію, як повне ім'я, адреса, номер школи, розклад занять або відомості про родину. [4]

ВИСНОВКИ

З початком широкого використання міжнародних мереж передачі даних загального користування темпи росту мережної злочинності зростають в геометричної прогресії. За оцінками експертів Міжнародного центру безпеки Інтернет (CERT) кількість інцидентів пов'язаних з порушенням мережної безпеки зросла в порівнянні з 2000 роком майже у 10 разів. Наше завдання - навчити дітей використовувати інтернет правильно. Так само, як вчимо дітей безпеки в реальному житті - на вулиці та дорозі, нам необхідно навчити їх безпечній поведінці у віртуальному житті - в інтернеті.

Інтернет-технології стали природною частиною життя дітей і сучасної молоді. Невміння працювати з комп'ютером і орієнтуватися в інтернет-просторі в сучасному суспільстві можна порівняти з невмінням писати й читати. Комп'ютер є не тільки розвагою, але й засобом спілкування, самовираження та розвитку. У кіберпросторі існує велика кількість спеціальних сайтів, адресованих дітям різного віку. Самостійне пізнання інформаційного світу дозволяє розширити коло інтересів дитини і сприяє її додатковій освіті, спонукає до кмітливості, привчає до самостійного розв'язання задач. Всесвітня мережа також задовольняє потребу підлітків у лідерстві. Діти, які добре знають комп'ютер та інтернет більш адекватно оцінюють свої здібності та можливості, вони більш цілеспрямовані та кмітливі. Щоб повноцінно орієнтуватись у віртуальному просторі дитині треба вчитися структурувати великі потоки інформації, дотримуючись основних правил безпеки в мережі Велике значення також має дотримання користувачами правил безпеки під час роботи в Інтернеті. Для отримання персональної інформації, небезпечні особи використовують чати, системи обліку миттєвими повідомленнями та сайти знайомств. Дотримання простих правил в спілкуванні через мережу Інтернет, дозволить захистити користувача від недобрих намірів зловмисників.

Шість правил розумних користувачів інтернету :

1. Чемним і толерантним у спілкуванні будь! Не ображай нікого,
   Про бумеранг у стосунках не забуть!
2. Якщо веб-сайт негарний закрій його негайно!
3. Свій пароль, як таємницю зберігай у власній скриньці!
   Правила розумних користувачів Інтернету пам'ятай і всім про них розповідай!
4. Цікаві веб-сайти ти шукай, друзям своїм про них розповідай.
   Разом з ними нове пізнавати і в віртуальному просторі безпечно крокувати.
5. Розкажи батькам, що не можеш вирішити сам.
   Всі проблеми вирішуй в сім'ї, бо батьки найкращі друзі твої!
6. Реальну адресу телефон і ім'я нехай знає тільки твоя сім'я.
   Нікому його не повідомляй в Інтернеті, бо можуть обманути, затягнути в тенет. [4]

З метою запобігання небезпеки у Всесвітній мережі діє портал для дітей, батьків та вчителів «Безпечна країна On- ляндія». Саме тут можна познайомитися з видами інтернет-небезпеки, отримати поради, як уникнути інтернет-залежності, взяти участь у різноманітних тренінгах, опитуваннях та конкурсах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Алексєєнко Т.Ф. Явища мобінгу та булінгу в стосунках групи і особистості// Шлях освіти.- 2012 - №2. - с.12-16.
2. Войскунский А.Е. Зависимость от Интернета: актуальная проблема // Мир Интернета. – М., 2000. – №3. – С. 76 – 81.
3. Навч.-метод. посібник. / К.Б. Левченко, О.А. Удалова, І.М. , Трубавіна та ін.; Заг. ред. К.Б. Левченко та О.А. Удалової. К.: „Міленіум”, 2004. – 180с.
4. Інтернет-ресурси:

- сайт Онляндія - http://www.onlandia.org.ua/
- 6 правил для батьків - розумних користувачів Інтернету: http://www.onlandia.org.ua/pages/v_turvallisesti_6rules
- Правила використання Інтернету вдома: http://www.onlandia.org.ua/pages/v_...sti_pelisaannot
- Засоби батьківського контролю: http://www.onlandia.org.ua/pages/pct
- Безпечне використання інтернету дітьми різного віку: http://www.onlandia.org.ua/pages/v_...s_ja_lapsen_ika
- Права дітей у мережі: http://www.onlandia.org.ua/pages/v_lapsen_oikeudet
- Безпечна електронна пошта: http://www.onlandia.org.ua/pages/e-mail