ТУРІЙСЬКИЙ РАЙОННИЙ МЕТОДИЧНИЙ КАБІНЕТ ПРАЦІВНИКІВ ОСВІТИ

І.М.Вознюк

МІЙ БЕЗПЕЧНИЙ ЕЛЕКТРОННИЙ СВІТ

МЕТОДИЧНА РОЗРОБКА

Турійськ - 2015

Вознюк І.М. Мій безпечний електронний світ – Турійськ – 2015. – 68 с.

Схвалено педагогічною радою Турійської загальноосвітньої школи І-ІІІ ступеня (протокол №2 27.03.2015)

Посібник розроблено для підтримки програми «Безпечний Інтернет». В посібнику пропонується зрозуміла, застосована на практиці інформація по Інтернет-безпеці, представлені матеріали для дітей, їх батьків і вчителів — інтерактивні сценарії, короткі тести, готові плани уроків, просте зведення правил і рекомендацій батькам із забезпечення безпеки дітей у Мережі — завдяки яким дорослі і діти зможуть освоїти основи безпечної роботи в Інтернеті.

Також у посібнику висвітлено способи безпечної поведінки дитини у віртуальному просторі, що убезпечать від негативного впливу на її психічне і фізичне здоров’я.

ЗМІСТ

ВСТУП 4
ЩО ТАКЕ ІНТЕРНЕТ І ЧИ БЕЗПЕЧНИЙ ВІН. Виховна година-гра для учнів 5 класу6
НАВІЩО ДІТЯМ ІНТЕРНЕТ? Бесіда для учнів 5-6 класів....11
ІНТЕРНЕТ: ЗА І ПРОТИ. Виховна година для учнів 7-8 класів....13
З ІНТЕРНЕТОМ БЕЗПЕЧНО НА ТИ. Тренінг для учнів 9-10 класів 17
ПОВЕДІНКА У ВСЕСВІТНІЙ МЕРЕЖІ. Урок-практикум для учнів 10 класу 21
БЕЗПЕЧНИЙ ІНТЕРНЕТ. Тренінг для учнів 10-11 класів 26
ДЕНЬ БЕЗПЕЧНОГО ІНТЕРНЕТУ. Позакласний захід для учнів 10-11 класів 30
ІНТЕРНЕТ. БЕЗПЕКА В ІНТЕРНЕТІ. Брейн-ринг для учнів 11 класу....35
УЧНІВСЬКА СТОРІНКА 38
Правила мережевого етикету....39
Безпека в Інтернеті....41
Реальні історії шахрайства в Інтернеті 49
ТЕСТИ 56
ПАМ'ЯТКИ ДЛЯ УЧНІВ ТА БАТЬКІВ 58
ДОБІРКА МАТЕРІАЛІВ ДО ДНЯ БЕЗПЕЧНОГО ІНТЕРНЕТУ....65
ДОДАТОК 1. Анкета «Рівень поведінки в Інтернеті» 66
ДОДАТОК 2. Анкета «Нетикет - кодекс поведінки в Інтернеті»....67
ВИКОРИСТАНА ЛІТЕРАТУРА 68

ВСТУП

Щодня зростає популярність Інтернету. І це зрозуміло, оскільки він надає багато можливостей для навчання, самоосвіти, розваг, самовдосконалення та самореалізації. Більш того, звертаючись до сучасних інформаційних технологій, людина раціонально використовує час, отже підвищує свою результативність своєї праці.

А також все більше дітей користується Інтернетом у повсякденному житті. Можливість підключитися до мережі не тільки через ПК, але й за допомогою мобільних телефонів сприяє цій тенденції. Інтернет надає дітям та молоді неймовірні можливості для здійснення відкриттів, спілкування й творчості.

Проте оскільки з самого початку Інтернет розвивався без будь-якого контролю, сьогодні він містить величезну кількість інформації, причому далеко не завжди безпечної. У зв'язку із цим виникає проблема забезпечення безпеки дітей.

Трапляються випадки, коли, навіть, дорослим людям з розвиненим критичним мисленням важко уникнути небезпеки у віртуальній спільноті. А як бути юному користувачеві з його природньою цікавістю, наївністю, романтичністю, жагою пригод, потягом до незвіданого... Традиційно, найкращий спосіб захисту у цьому випадку – знання як технічних, так і етичних норм мережі, небезпек, що можуть спіткати, способів уникнення небажаних проблем.

Також більшість українських батьків не усвідомлюють існування небезпек, на які може натрапити їх дитина, перебуваючи в мережі Інтернет.

Згідно дослідження, лише 5 % опитаних батьків цікавляться детальним змістом веб-сторінок, які переглядає їх дитина.

79 % опитаних дітей в Україні вважають, що достатньо обізнані з існуючими ризиками в мережі Інтернет. Але ця так звана «обізнаність» не виключає спілкування дітей з незнайомими людьми у соціальних мережах (27 %), пересилання особистих фотографії (28 %) та конфіденційної інформацію про родину (17 %) незнайомцям. Більш того, 7 % опитаних дітей підтвердили, що в мережі їм пропонували придбати наркотики, а 11 % із них прийняли таку пропозицію.

Враховуючи достовірність отриманої інформації про ризики Інтернету та вплив однолітків, легко помітити розбіжність між впевненістю дітей у своїй поінформованості та реальним рівнем інформування, що підтверджується також досить ризикованою поведінкою дітей в мережі Інтернет, засвідченою вищенаведеними даними.

На виклик ситуації, коли українські батьки не до кінця усвідомлюють, наскільки велику роль відіграє Інтернет у житті їхніх дітей, і недостатньо серйозно ставляться до їхньої онлайн-безпеки й захисту приватної інформації, у

лютому (другий вівторок лютого) європейська громадськість відзначає День безпечного Інтернету, введений в 2004 році організацією Insafe (Європейська мережа безпечного Інтернету).

У 2008 році понад 120 організацій у 56 країнах відзначили цей день, провівши місцеві, національні та загальні європейські заходи щодо безпеки користувачів Мережі. Основним завданням Дня безпечного Інтернету в 2009 році стало встановлення діалогу між користувачами інтернет-послуг, державними структурами, громадськими організаціями з представниками бізнес-структур, які надають ці послуги і створюють новітні технології з метою підвищення інформованості щодо безпечного та відповідального користування Інтернетом (особливо серед дітей та молоді).

Україна також у 2008 році долучилася до цього процесу. Тоді була створена Коаліція за безпеку дітей в Інтернеті.

Тому для підтримки програми «Безпечний Інтернет» розроблений цей посібник, на якому представлені матеріали для дітей, їх батьків і вчителів — інтерактивні сценарії, короткі тести, готові плани уроків, просте зведення правил і рекомендацій батькам із забезпечення безпеки дітей у Мережі — завдяки яким дорослі і діти зможуть освоїти основи безпечної роботи в Інтернеті. В посібнику пропонується зрозуміла, застосована на практиці інформація по Інтернет-безпеці, вивчивши яку, навіть починаючі користувачі зможуть ефективно використовувати ресурси мережі і захистити себе від небажаного контенту.

Також у посібнику висвітлено способи безпечної поведінки дитини у віртуальному просторі, що убезпечать від негативного впливу на її психічне і фізичне здоров’я.

Проблема існування ризиків в Інтернеті дійсно існує. Лише спільними зусиллями ми можемо зробити Інтернет більш безпечним для наших дітей. І ми це зробимо.

ЩО ТАКЕ ІНТЕРНЕТ І ЧИ БЕЗПЕЧНИЙ ВІН.
Виховна година-гра для учнів 5 класу

Мета: познайомити дітей з поняттями «мережа», «Інтернет», «послуга»; розглянути основні види мережевих послуг; з'ясувати позитивні сторони та застерегти учнів від небезпеки, яка може очікувати в мережі; розвивати логічне мислення, пам'ять.

Хід виховної години

І. Мотивація навчальної діяльності.

Вчитель: Діти, що ви знаєте про глобальну мережу Інтернет?

ІІ. Оголошення теми та мети виховної години.

Вчитель: Саме сьогодні ми і познайомимося з мережею, про яку знають всі на світі, і якою всі користуються.

Не так давно, не в одній, а в багатьох країнах оселилася маленька тваринка, яку всі називали Інтернет. Тваринка більш за все любила спілкування. Друзів та знайомих вона мала велику кількість, тому всі називали її скорочено Нет або Інет. Інет займався корисною справою – надсилав листи закоханим, листівки адресатам, приносив рахунки та повідомлення і з легкістю жонглював коротенькими повідомленнями разом зі своєю найліпшою подругою тіткою Асею. Дуже любив Інет спілкування за допомогою електронних скриньок.

- Як ви думаєте, яким же чином він спілкувався?

1. Гра «Вітання без слів»

Вчитель: Давайте з вами проведемо гру «Вітання без слів».

Учасникам пропонується протягом 2-3 хвилин вільно рухатись в класі та встигнути за цей час привітати якомога більше товаришів. Робити це треба мовчки, без слів: кивком голови, рукостисканням, обіймами і т.ін. При цьому кожен учасник має право використати кожен спосіб привітання лише один раз; для кожного наступного привітання необхідно вигадати новий спосіб.

Гра сприяє зняттю психологічної напруги, вільному спілкуванню.

Вчитель:

- Кому скільки вдалось привітати людей?
- Що складніше — вигадати нові способи або їх продемонструвати?
- Можливо хтось відчув психологічний дискомфорт?
- На якому етапі це відбулось? *(Відповіді дітей на поставлені запитання)*

Вчитель: Ви побачили, що спілкуючись в Інтернеті, люди використовують іноді зовсім незвичні форми спілкування.

2. Гра «Рухавка»

Умови гри: учасник, якій починає вправу, називає групі своє ім'я та супроводжує його якимось рухом, який виражає його емоційний стан. Його сусід справа повторює ім'я та рухи попереднього учасника, після чого називає своє ім'я та демонструє свій рух. Третій учасник повторює імена і рухи двох попередніх учасників, після чого додає свої і т.д.

Гра сприяє розвитку різноманітних способів знайомства, спілкування.

Вчитель.

- Які емоції виникли під час вправи?
- Які рухи найбільш запам'ятались?
- Чому? *(Відповіді дітей на поставлені питання)*

Вчитель: Спілкуючись в Інтернет, люди використовують іноді зовсім незвичні форми спілкування.

- Яку інформацію можна отримати від того, як люди себе презентують в Інтернет?

3. Гра «Збери привітання»

Учасникам протягом 30 секунд пропонується потиснути руки якомога більшої кількості учасників. Кожному учаснику можна тиснути руку лише 1 раз.

Вчитель:

- Кому скільки людей довелось привітати?
- Можливо хтось відчув психологічний дискомфорт?
- На яких етапах це відбулось? *(Відповіді дітей)*

Вчитель: Досить часто співрозмовника в Інтернет ми знаємо лише за його Ніком (так званим ім'ям або прізвиськом). Продовжуємо знайомство далі.

Полюбляв Інтернет колекціонувати різноманітні красивущі (та не дуже) картинки, казки, підручники, книги, пісні та шедеври сучасної і класичної музики, різноманітні фільми та веселі й безглузді мультфільми. І взагалі, в його колекціях було стільки всього!!! Одні колекції були добре упорядкованими, інші – звалені в кучу. Кількість та якість колекційного матеріалу залежала від тих, хто його надсилав. Інтернет дуже любив дружити з людьми, яких називав Юзерами.

Сам по собі Інтернет був дуже неуважним, ніколи не знав, де і що в нього лежить. Тому на допомогу йому завжди приходили роботи Великі Пошукові Системи, які наводили порядок в сховищах, складали електронні підручники з переліком матеріалу, які й зберігалися в нірці Інета.

Для того, щоб запросити Інтернет до себе в гості, треба було спочатку потоваришувати з його господарями Провайдерами. Вони проводили в кожну домівку нірку, через яку і потрапляв Інтернет до всіх бажаючих для того, щоб

поспілкуватися, пограти в різноманітні ігри, заспівати пісень або послухати улюблену мелодію.

Більшість господарів Інету задарма не хотіли товаришувати, тому брали за спілкування гроші.

Окрім цікавої інформації в сховищах Інтернету ховалися дуже дивні речі, про які не знав навіть і він сам. І коли ці речі бачили діти, то батьки дуже сварилися і іноді навіть закривали нірку.

Траплялися з Інтернетом та його друзями різноманітні пригоди та цікаві історії. Давайте разом прочитаємо цікаві історії, написані учнями 10-11 класів про мережу Інтернет.

3. Читання учнями казок про Інтернет

Королівство Інтернет

У тридев'ятому царстві, у тридесятій державі, в Королівстві під назвою Інтернет жили король Файл та королева Папка. Вони були дуже добрими та справедливими правителями, завжди уважно слухали скарги своїх жителів і з радістю допомагали мешканцям королівства у вирішенні їх проблем.

Але був у королівстві ворог – жителі країни Вірус, які намагалися захопити Інтернет. Та нічого в них не виходило, тому що інтернетівці були дружніми та сміливими, а саме королівство надійно захищеним. На чолі варти країни стояв мужній полковник Антивірус.

Одного разу з'явилася в Інтернеті папка, яка зрадила короля та королеву. І потрапили за стіни королівства злі віруси, та почали уражувати й знищувати всіх його жителів. Допомогти було нікому, полковник Антивірус у цей час перебував на завданні і не міг захистити свою країну від ворога. За полковником було направлено поштового голуба, який і повідомив про напад на Інтернет. Щойно віруси, які вже майже дісталися короля та королеви, побачили полковника Антивіруса, злякалися і почали тікати. Але не тут то було. Від Антивіруса ще ніхто ніколи не втік. Знищивши ворога, полковник приготував відвар з лікарської трави і напоїв ним усіх заражених жителів країни. Невдовзі інтернетівці одужали і зажили щасливо.

Вчитель:

- Діти, що повчального ви прочитали в цій казці? *(Відповіді дітей)*
- А як би вчинили ви? *(Відповіді дітей)*

Продовжуємо далі. Зараз ви прочитаєте історію, яка могла б трапитися будь з ким із вас.

Чудо-Інтернет

У тридев'ятому царстві, у тридесятій державі, у мальовничому куточку на лісовій галявині розкинулася Вільшанська загальноосвітня школа І-ІІІ ступенів, де навчалися розумні діти, які постійно прагнули набувати нових знань, умінь та

навичок. Вони не лише гарно вчили гуманітарні предмети, а й добре володіли комп'ютерами.

Але були в школі й такі діти, які вчилися дуже погано. Учні хворіли на хворобу – нечемність, тому під час зустрічі не віталися один з одним, на прощання ніколи не говорили «до побачення» або «до зустрічі». Тяги до навчання в них не було. Єдиним захопленням в дітей були комп'ютерні ігри. Але, на жаль, і ті були не корисними для навчання.

Довго тривало таке чи ні, але одного разу найшло на цих учнів затемнення. А виною всьому був Начальник Канцелярії Нічних Кошмарів, який жив у похмурому підземному палаці і весь час сидів перед каміном, де ледь жевріло темно-синє вогнище. Начальник любив пітьму, тому завжди ходив у чорному оксамитовому плащі з каптуром, що закривав обличчя. За це його ще називали Пан Морок. Він був увесь із темряви і боявся сонячних променів і світла, бо то була його смерть. Коли у Пана Морока був гарний настрій, він любив грати на гітарі. Але одного разу, тільки-но він набрав перший акорд …

Згори до палацу провалилися налякані та схвильовані діти Вільшанської школи. В руках вони тримали дивні пристрої – ноутбуки, на яких і грали в свої дивні ігри.

А тим часом, у школі помітили зникнення частини учнів, і всі кинулися їх розшукувати, але не знали як зробити це швидко і де саме шукати.

На допомогу прийшли відмінники. У той момент, коли сталася прикрість, у школі проходив урок інформатики, під час якого вивчалася всесвітньовідома мережа Інтернет. Саме він допоміг швидко дізнатися про місцезнаходження зниклих. Спочатку діти зайшли на пошуковий сайт «Індекс. мен» і з супутника відкрилася «джіпіес» карта підземелля. На щастя, в дітей у підземеллі були ноутбуки, які швидко зреагували на пошуковий сигнал, надісланий з Інтернету. Так з'вилась можливість врятувати друзів. Але як до них дістатись?

На допомогу учням прийшов давній товариш усіх дітей - сонячний зайчик. Адже кожен у своєму житті, навіть дорослий, хоч раз мав можливість гратися люстерком і пускати сонячних зайчиків. Учні за допомогою мережі Інтернет показали сонячному зайчику карту підземелля із бранцями. І зайчик, не довго думаючи, взяв свій сліпучий промінь і кинув його прямо в підземелля на Пана Морока. Від такого яскравого променя він одразу загинув, а діти в ту ж мить опинилися в школі. Вони були страшенно налякані, їм було дуже соромно за свою поведінку. Але діти були вдячні Інтернету та знанням товаришів, бо якби не вони, то ще довго сиділи б бідолашні в темряві. Отже, учення – світло, а не вчення – тьма.

Вчитель: Чому з учнями сталася така пригода? Як правильно треба себе поводити? Отже, сподіваюсь, ви чинити так не будете.

- А чи є в когось з вас вдома Інтернет? *(Відповіді дітей)*

- А що цікавого ви з нього черпаєте? *(Обмін досвідом роботи з мережею)*

ІІІ. Підсумок виховної години

Вчитель. Діти, давайте пригадаємо все те, про що ми почули сьогодні і сформулюємо власні правила поведінки в мережі Інтернет.

(Учні разом з вчителем формулюють правила)

Що ж треба, і чого не слід робити в мережі:

1. Треба бути обережним, надаючи інформацію про себе.
2. Думати про сказане, тому що ми не бачимо співрозмовника і можемо його образити так само, якби дивилися в очі.
3. Пам’ятати про те, що в Інтернеті є як корисна, так і шкідлива інформація.
4. Розмістивши інформацію в Інтернеті, ми втрачаємо контроль над нею і в більшості випадків вже ніколи не зможемо видалити всі її копії.
5. В Інтернеті є речі, від яких слід захиститися.
6. Радитися з батьками з питань відвідування сайтів.
7. Якщо виникають певні проблеми, доводити про них до відома батьків.
8. Не проводити багато часу в мережі, тому що це шкідливо.

НАВІЩО ДІТЯМ ІНТЕРНЕТ?
Бесіда для учнів 5-6 класів

Мета: *пояснити недоліки та переваги мережі Internet.*

Обладнання: На дошці записана тема, мета, девіз.

«Найнебезпечніший вірус в

інтернеті – це сам інтернет!»

Вступне слово вчителя: Майже у кожного з вас вдома є компьютер та інтернет, тому в рамках Дня безпечного Інтернету сьогоднішня виховна година буде присвячена безпечному Інтернету.(Вчитель оголошує тему, мету, девіз.) (Вчитель розповідає про вади, переваги та про деякі правила користування інтернетом, діти доповнюють.)

1. Правила користування Інтернетом (час і відстань). За комп'ютером сидимо 20-25 хвилин і треба робити перерву, це техніка, нею керує людина, можна призупинити роботу і відпочити інакше зашкодите зору. (Діти доповнюють.)

2. Програми-заборони, що встановлені на комп'ютерах в школі. Такі програми «захищають» комп'ютери від сайтів, що пропагують насильство, тобто вони є «цензурою». Захист комп'ютерів від вірусів, якими «заражають» комп'ютери на деяких сайтах, а потім пропонують антивіруси за велику плату, але не завжди допомагають такі антивіруси.(Діти доповнюють.)

3. Неправдивість інформації в Інтернеті. Будь-яка інформація в інтернеті може бути змінена кожним, хто її переглядає, тому на правдивість такої інформації розраховувати не можна. Більш того в контактах, однокласниках, чатах люди, з якими випадково знайомимося, можуть бути взагалі не реальними. (Вчитель розповідає про такий випадок, почутий напередодні у новинах.) До того ж коли ви реєструєтесь на сайтах для спілкування і т. д. вводите інформацію про себе, а потім цю інформацію може будь-хто використати і, як правило, не на вашу користь. (Діти доповнюють.)

4. Ігри, що «крадуть» життя. Деякі люди так захоплюються іграми в Інтернеті, що починають плутати реальне та віртуальне життя. Вони проводять майже увесь свій час за грою, таким чином псують своє здоров'я та реальні стосунки з оточуючими їх людьми. (Діти доповнюють.)

Підсумок: Отже, Інтернет має переваги – можна знайти будь-яку корисну нам інформацію, але в той самий час він є великим «смітником». Тому треба пам’ятати про усі перераховані сьогодні вади Інтернету та не потрапляти у «пастки», що приготували нам недоброзичливі люди. Дякую за увагу.

ІНТЕРНЕТ: ЗА І ПРОТИ.
Виховна година для учнів 7-8 класів

Мета: ознайомити учнів з позитивним та негативним впливом Інтернету на людину; дати можливість учням самостійно прийняти ту позицію, до якої вони схиляються, розвивати навички роботи в групах, вміння висловлювати свою точку зору логічно і конкретно, виховувати інтерес до порушеної теми.

Обладнання: плакат «Основні правила спілкування», плакат №1 із зображенням комп'ютера, плакат №2 із зображенням комп'ютера, підключеного до мережі Інтернет; запис на дошці; малюнки учнів; пам'ятки, картки, зображення Золотої рибки, ілюстрація, мікрофон тощо.

За часів сьогодення, коли особливого значення набуває інформація, вже ніхто не заперечує, що комп'ютер увійшов до різних сфер сучасного життя, і часто-густо без нього важко обійтися. Багато хто використовує його на роботі, вдома, а деякі присвячують комп'ютеру своє дозвілля.

Хід заняття

І. Вступне слово класного керівника: Про алкогольну та наркотичну залежність часто пишуть практично усі засоби масової інформації. А ось про комп'ютерну згадують набагато рідше. Але вона існує. Особливо серед підлітків, які проводять майже весь свій вільний час у віртуальному світі, нехтуючи навчанням, друзями, здоров'ям. Можна стверджувати, що наприкінці XX століття виникла і поширилась нова форма залежності – комп'ютерна.

Тому на сьогоднішньому занятті ми будемо з вами говорити про Інтернет і спробуємо виявити: чи потрібен він в нашому житті та які плюси та мінуси має мережа. Але спочатку звернемося до епіграфу нашого заняття.

Завдання для учнів:

Прочитайте уважно епіграф і поясніть, як ви розумієте це висловлювання, чи згодні ви з цим, а якщо ні, то поясніть, чому. Але спочатку давайте звернемося до плакату «Основні правила спілкування» і будемо керуватися написаним протягом нашого заняття. *(Учні висловлюють свою точку зору, спираючись на*

«Основні правила спілкування»

- *Бути позитивним, активним.*
- *Говорити те, що думаєш.*
- *Говорити тільки за темою.*
- *Не критикувати, бути толерантним.*
- *Говорити коротко.*
- *Не перебивати.*

- *Слідкувати за часом.*

Слово класного керівника: Комп'ютер підвищує інтелектуальний рівень дитини, допомагає їй увійти у доросле життя. Діти полюбляють спілкуватися з комп'ютером: він дозволяє обрати потрібний рівень розмови, виправляє помилки, може відповідати на ті запитання, які дорослим вважаються дурницями.

Переваги комп'ютерної системи навчання безумовні, але попередження несприятливих факторів має особливе значення для учнів. Чому саме? Зараз спробуємо з'ясувати.

Завдання для учнів:

Зверніть увагу на плакат №1 і плакат №2, скажіть, чим схожі зображення на даних плакатах і чим вони відрізняються.

(учні відповідають, що комп'ютер, зображений на плакаті №2 підключений до мережі Інтернет, і в нього більше можливостей ніж у комп'ютера на плакаті №1)

Інтерактивна вправа «Займи позицію» або «Кути»

Спробуйте визначитися, з яким комп'ютером, №1 чи №2, вам цікавіше і доцільніше працювати, об'єднайтеся у відповідні групи і займіть відповідну позицію. Доведіть свою точку зору, користуючись правилами спілкування.

(учні працюють в групах, намагаються переконати своїх опонентів таким чином, щоб ті зайняли іншу позицію. Класний керівник може допомогти учням у виявленні позитивних і негативних рис користуванням комп'ютером в мережі та домашнім комп'ютером взагалі, використовуючи картки виду:

Позитивні аспекти
• Активізація пізнавальної діяльності. • Розвиток уваги та просторової орієнтації. • Збільшення обсягу інформації за одиницю навчального часу. • Систематизація мислення. • Розвиток навичок пізнавальної діяльності та особистісний зріст.

Негативні аспекти
• Розумова втома та перевтомлення. • Емоційне, психічне та зорове навантаження.

- Несприятлива дія на навколишнє середовище.
- Поява синдрому залежності від Інтернету.
- Соціальна ізоляція.
- Серйозні особистісні проблеми, суїцид.

Слово класного керівника: Без комп'ютерів цивілізоване суспільство не можна вважати повноцінним, і застосування комп'ютерів поширюється кожного дня і буде поширюватися у майбутньому. Як і будь – який інший винахід, комп'ютер в умілих руках – це благо, а у безладних – покарання. Його шкідлива дія на здоров'я людини головним чином залежить від порушення правил, які ми з вами встановимо пізніше. Слід користуватися комп'ютером так, щоб можна було зберігати фізичне, психічне та духовне здоров'я.

Інтерактивна вправа «Карусель»

Учні об'єднуються в 4 групи (за принципом: зима, весна, літо, осінь). Кожна група отримує картку з фразами, які необхідно закінчити. За певний відрізок часу члени кожної групи повинні виконати завдання і за сигналом передати свою картку сусідній групі. Ті, отримавши нову картку, читають завдання і відповіді, що внесли учні попередньої групи, та доповнюють відповіді своїми. Вправа продовжується до тих пір, поки до групи не повернеться її картка, яку учні отримали попередньо. Після цього командир кожної групи оголошує написане з урахуванням версій інших груп.

Картка №1

1. Якщо ви отримали по Інтернету невихований грубий лист..?
2. Нікому без дозволу батьків не давати…

Картка №2

1. Якщо ви знайшли в Інтернеті інформацію, що стурбувала вас..?
2. Ви познайомилися за допомогою Інтернету з людиною, і вона вас запросила на побачення…

Картка №3

1. Вам дуже потрібно зустрітися з вашим другом з Інтернету, хоча ви його раніше не бачили…
2. ви несподівано для себе зайшли до забороненого сайту…

Картка №4

1. Ваш друг виклав в Інтернет ваші фото, які ви не хотіли оприлюднювати…
2. Вам дуже хочеться поспілкуватися з другом з Інтернету, але на ваші електронні листи він відповідає мовчанням…

Слово класного керівника: Ви самі вивели правила користуванням Інтернетом. Чи погодитесь ви прийняти їх за правила, які допоможуть уберегти

вас в мережі?

Слово класного керівника: Перед початком наступної вправи хочу наголосити на тому, що в Інтернеті вас підстерігають небезпеки, про які ви навіть не здогадуєтесь. Тому наступна вправа дасть можливість переконати тих, хто вважає себе непідступним.

Тренінг «Зіпсований телефон» або «Брехня»

З числа учнів класу вибираються 3 – 5 бажаючих взяти участь в тренінгу. Один з них залишається в класі, а ті виходять за двері в коридор. Учневі, що залишився, показують ілюстрацію. Він її запам'ятовує, а потім описує побачене одному з тих, хто зайшов до класу з коридору. Другий уважно слухає пояснення першого і передає почуте третьому. Коли останній учень, що вийшов до коридору, пояснить те, про що йому розкаже попередній, і за його розповіддю на дошці схематично учитель зобразить це, учасникам тренінгу покажуть справжню ілюстрацію. І тоді кожен зможе побачити наскільки співпадає почуте з побаченим.

Слово класного керівника: Потрапити у залежність можна від чого завгодно, і комп'ютер не є винятком. Така пристрасть може стати серйозною проблемою, коли людина реалізує біля комп'ютера весь вільний час, забуваючи про їжу, нехтуючи своїми щоденними обов'язками. Якщо людині, у якої сформувалася залежність від Інтернету, з якоїсь причини не вдається сісти до екрана монітору, вона стає нервовою, дратівливою, агресивною. Часто-густо у таких людей виникають складності з іншими людьми, їм важко заводити друзів і підтримувати стосунки з близькими. І тут багато що залежить від батьків. Тому наступна наша вправа буде стосуватися саме їх.

Інтерактивна вправа «Золота рибка»

Кожен учень отримує зображення золотої рибки, яка може виконати 3 бажання, але тільки ті, що стосуються батьків, Інтернету та безпечного знаходження в мережі. Учні на зворотному боці Золотої рибки пишуть побажання – правила для батьків стосовно користування Інтернетом, а потім презентують їх усім учням. Після оголошення усіх робіт учасники заходу повинні отримати правила для батьків.

Підсумок заняття

Інтерактивна вправа «Мікрофон»

Учні отримують по черзі мікрофон і відповідають на питання:

- Які нові знання ви сьогодні отримали?
- Як ці знання ви будете використовувати в реальному житті?
- Що вас найбільше вразило із почутого?

З ІНТЕРНЕТОМ БЕЗПЕЧНО НА ТИ.
Тренінг для учнів 9-10 класів

Мета: сформувати розуміння правильного користування Інтернетом та виявити всі плюси та мінуси бездумного та грайливого ставлення до ресурсів глобальної мережі. Виявити фактори ризику для дітей у цій сфері та навчити учасників, як себе убезпечити в кіберпросторі. Формувати принципи групової роботи та налаштувати на плідну й цікаву співпрацю.

Цільова група: категорія учасників: діти 14-16 років.

Обладнання: заготовка «Ваза», квіти, вирізані з паперу для гри «Знайомство», фрукти, вирізані з паперу для гри «Дерево знань», портрети, маркери, клубок.

Хід тренінгу

Вчитель: Сьогодні ми проведемо з Вами тренінг, щоб ще пригадати правила користування мережею Інтернет".

Вправа «Правила групи»

Вчитель: В житті кожної людини є правила, які допомагають регулювати взаємовідносини в суспільстві. Для того щоб група працювала продуктивно, щоб кожен учасник почувався комфортно і міг ефективно взаємодіяти, потрібно прийняти правила групи. Давайте разом обговоримо і запишемо на плакаті правила роботи.

Пропозиції обговорюються, корегуються і записуються на окремий плакат, який буде розміщено на видному місці до кінця тренінгу.

Основні правила:

- бути позитивним;
- бути активним;
- говорити те, що думаєш;
- говорити тільки за темою;
- не критикувати, бути толерантним;
- говорити коротко, не перебивати виступаючого;
- дотримуватись регламенту.

Зупинка 1. Інтернет можливості і ТИ

Вчитель: Діти, як і дорослі, використовують Інтернет з різною метою: щоб поспілкуватися з друзями, пограти в ігри, послухати та записати музику, відео, підготуватися до уроків, знайти та прочитати цікаву інформацію або придбати певні товари. Для цього вони використовують різні послуги в мережі Інтернет. А чим користуєтесь Ви в мережі Інтернет і навіщо?

Учні записують можливості Інтернет на стікерах-будиночках та наклеюють на плакат з зображенням павутиння, яке буде символізувати мережу Інтернет.

Мозковий штурм «Що я повинен знати про Інтернет»

(для актуалізації знання і досвіду учнів)

Зупинка 2. Інтерактивне спілкування

Вчитель: Для того щоб людина користувалася мережею Інтернет, спілкувалася з іншими в мережі Інтернет, їй треба зареєструватися. Що таке реєстрація? Людина вигадує собі ім‘я (нікнейм) під яким вона буде блукати по мережі. Ми також з Вами створили свою мережу.

Зараз ми з Вами спробуємо теж зареєструватися в цій мережі. Гра «Ваза з квітами».

Кожний учень пише на квітці своє вигадане ім‘я, з яким він буде подорожувати мережею Інтернет. Виходить з квіткою та наклеює її на вазу, так щоб утворився букет. Аркуш з вазою розміщується на дошці.

Висновок

Не всі люди в мережі реєструються під власним ім‘ям, зазвичай вони вигадані, і дуже важко дізнатися, що за людина знаходиться за екраном.

Вчитель: Ви зареєструвалися. а тепер може поспілкуватися в мережі Інтернет.

Гра «Хто надіслав тобі листа».

Для цієї вправи використовує «Ваза» з попередньої вправи. Учень пише позитивне побажання а бо просто хороші слова на квітці. А потім наклеїти їх поряд з будь -якою квіткою. Кожен учень має наклеїти побажання до чужого нікнейму так щоб власники нікнеймів не бачили хто надає їм побажання. Учасники отримають побажання до свого нікнейму і намагаються вгадати, хто надіслав їм це «повідомлення».

Висновок

Так само відбувається і зі спілкуванням в Інтернет просторі. Дуже складно перевірити, хто саме пише тобі листи, спілкується з тобою. Якщо учасники групи добре знайомі між собою, вони можуть вгадувати відправника. Але в Інтернет просторі ти ніколи не знаєш хто знаходиться по той бік комп'ютера або мобільного телефону.

Зупинка 3. Розміщення приватної інформації

Гра «Фоторобот»

Діти поділяються на 2 групи. Кожній групі дається фото, яке потрібно розмалювати.

Висновок

Фото, яке розміщується в Інтернеті, теж може бути розмальованим, домальованим. Тому перш ніж розміщувати приватну інформацію, треба добре подумати, як її інші можуть використати проти вас.

Вправи на формування навичок безпечної поведінки під час обміну фотографіями та особистою інформацією.

Вправа "Таємниця"

Всі учасники сідають на стільці. Кожен отримує аркуш паперу та олівець.

Вчитель: Кожен із учасників має певні таємниці і не хоче, щоб вони стали відомі іншим. Напишіть на папері одну таку подію.

Після того, як учасники напишуть, вчитель просить дуже щільно скласти цей папірець, перегнувши декілька разів, щоб не було видно, що саме написано, і покласти його під стілець. Після цього всім учасникам пропонується пересісти на два стільці вправо, потім на п'ять стільців вліво та ще на три стільці вліво.

Обговорення

Що Ви зараз відчуваєте? Чи можете ви визначити, під яким стільцем знаходиться ваша таємниця?

Вчитель просить взяти чужий папірець під стільцем, на якому він зараз опинився. Не треба його розгортати! Учасники лише беруть у руки папірці з чужими таємницями.

Обговорення

Що ви відчуваєте тепер? Чи хотіли б ви, щоб зараз хтось прочитав зміст того, що написано на папері, який він тримає у руках? Звісно, ніхто цього не бажає.

Висновок

Досить часто ми розміщуємо у мережі Інтернет інформацію, яка може нас компрометувати або навіть ідентифікувати: повне ім'я, домашню адресу, телефон, фінансовий статок, місце роботи батьків та інше. Цього не варто робити, інакше ми не будемо почувати себе так, як під час цієї вправи.

Вправа "Мішечок знань" або «Дерево знань»

Вчитель: Напишіть на монетках або фруктах, які правила безпеки з сьогоднішнього тренінгу Ви взяли для себе.

Учні пишуть правила на монетах і наклеюють на "Мішечок знань".

Учні пишуть правила на фруктах і наклеюють на «Дереві знань».

10 золотих правил безпеки в Інтернеті для дітей

1. Нікому без дозволу батьків не давати особисту інформацію: домашню адресу, номер домашнього телефону, робочу адресу батьків, їхній номер телефону, назву й адресу школи.

2. Якщо знайдете якусь інформацію, що турбує вас, негайно сповістіть про це батьків.

3. Ніколи не погоджуватися на зустріч з людиною, з якою ви познайомилися в Інтернеті. Якщо все ж таки це необхідно, то спочатку потрібно спитати дозволу батьків, а зустріч повинна відбутися в громадському місці й у присутності батьків.

4. Не посилати свої фотографії чи іншу інформацію без дозволу батьків.

5. Не відповідати на невиховані і грубі листи. Якщо одержите такі листи не з вашої вини, то сповістіть про це батьків, нехай вони зв'яжуться з компанією, що надає послуги Інтернет.

6. Розробити з батьками правила користування Інтернетом. Особливо домовитися з ними про прийнятний час роботи в Інтернеті і сайти, до яких ви збираєтесь заходити.

7. Не заходити на аморальні сайти і не порушувати без згоди батьків ці правила.

8. Не давати нікому крім батьків свої паролі, навіть найближчим друзям.

9. Не робити протизаконних вчинків і речей в Інтернеті.

10. Не шкодити і не заважати іншим користувачам.

Вчитель: Ми сьогодні повторили ще раз, які небезпеки існують в мережі Інтернет. Але насправді їх багато. Кожний ваш крок має бути обдуманим і заздалегідь Ви маєте прогнозувати результат своїх дій. Пам'ятайте: Інтернет – це як азартна гра, чим більше ти ним користуєшся, тим сильніше він тебе затягує.

ПОВЕДІНКА У ВСЕСВІТНІЙ МЕРЕЖІ.
Урок-практикум для учнів 10 класу

Тема. Поведінка в Інтернеті.

Мета: під час вивчення теми «Служби Інтернету» систематизувати, узагальнити та закріпити на практиці знання учнів про значення Інтернету в суспільстві, про те, що собою являє глобальна мережа, про сервіси Інтернету; надати інформацію про небезпеку роботи в Інтернеті; прививати етичні погляди; виховувати почуття відповідальності під час роботи в мережі.

Тип: урок-практикум.

Хід уроку

І. Теоретична частина

Вчитель: Наприкінці двадцятого століття особливо важливого значення набуває інформація. Усе більшої необхідності набуває володіння швидкими й точними даними про предмет діяльності. Практично одночасно з появою комп'ютерів виникла проблема передачі інформації між ними. Можна передавати інформацію за допомогою так званих носіїв інформації: дискет, дисків тощо. Але цей спосіб досить складний для інформаційного самообміну, без участі людини. Причому їхня своєчасність стає надзвичайно важливою. У цей час найбільш зручним способом одержання й передачі різноманітної інформації є використання всесвітньої комп'ютерної мережі Інтернет.

Ближче познайомитися із поняттям Інтернету та визначити його значення в житті суспільства нам допоможе фахівці з інформаційних технологій.

Виступ першого фахівця з інформаційних технологій

Інтернет являє собою всесвітню інформаційну комп'ютерну мережу, що поєднує в єдине ціле безліч комп'ютерних мереж, що працюють за єдиними правилами. Інтернет не є комерційною організацією й нікому не належить. Користувачі Інтернету є практично у всіх країнах світу. Комп'ютери зв'язуються за допомогою ліній зв'язку. Для підключення лінії зв'язку до комп'ютерів використовуються спеціальні електронні пристрої (модеми), установлюються програми для спільної роботи. Тобто комп'ютерна мережа - це об'єднання комп'ютерів, ліній зв'язку між ними й програм, що забезпечують обмін інформацією.

До Інтернету мають доступ десятки мільйонів користувачів. Ріст і розвиток Інтернету триває, і з кожним роком значно збільшується роль Інтернету у всіх інформаційних технологіях.

Однією з переваг Інтернету є корисність. Обсяг інформації набагато більший. Подання й зручність її сприйняття поки не можуть зрівнятися із книгами або телебаченням, але кількість і доступність інформації в мережі порівняно вища. Інтернет - джерело найбільш свіжої інформації. Проте з розширенням глобальної комп'ютерної мережі кількості доступної інформації й послуг виникає проблема перевірки та достовірності.

Електронна пошта (e-mail) - перший із сервісів Інтернет, найпоширеніший і ефективний з них. Електронна пошта - типовий сервіс відкладеного читання (off-line). Ви посилаєте Ваше повідомлення, як правило у вигляді звичайного тексту, адресат одержує його на свій комп'ютер через якийсь, можливо досить тривалий проміжок часу, і читає Ваше повідомлення тоді, коли йому буде зручно.

До інтерактивних сервісів, що служать спілкуванню людей через Інтернет, ставиться ICQ, розмови через Інтернет. Користувачі установлюючи одну програму можуть спілкуватися в реальному режимі (on line). Також дуже популярні чати. Користувачі приєднуються до одному з каналів - тематичних груп і беруть участь у розмові, що ведеться не голосом, але текстом.

Виступ другого фахівця з інформаційних технологій

В Інтернет є, звичайно ж, своя небезпека. Сьогодні немає засобів впізнання особи, з якою спілкуєшся, тому важко перевірити інформацію щодо співрозмовника. Є дуже багато випадків, коли себе видають за інших, приписуючи собі гарну зовнішність, риси характеру, захоплення тощо. Подумайте чи хотіли б спілкуватися з нещирою людиною?

Існують випадки потрапляння в рабство через мережу Інтернет. Дівчата та хлопці переписуються з особами, які пропонують роботу за кордоном або одруження. Також існують випадки, коли за допомогою спілкування просять надіслати фотокартки, а потім використовуючи монтаж, створюють фотокартки і розміщують на порносайтах.

З поширенням використанням Інтернету з'явилося таке явище як spam. Це коли на поштову адресу приходять листи з рекламними пропозиціями. Іноді за день їх може надійти від одного до 50. Вберегтися від цього дуже важко. Також Інтернет може використовуватися шахраями, які можуть вимагати гроші організацію допомоги. Як правило, дається тільки рахунок для перерахування грошей, немає ні координат організації, ні інформації, якою діяльністю вони займаються, як довго існують тощо. Або надсилається інформація про виграш грошей або якоїсь речі. Для того щоб отримати приз, треба зателефонувати за номером телефону, який є платним. А потім приходить великий рахунок за телефон.

Вчитель: Звісно, на сьогоднішній день великої актуальності набуло питання безпеки даних. Комп'ютери, підключені до глобальної мережі, стають набагато більше уразливими. І не має гарантії, що дані не використовують інші. Що ж треба для цього робити? Як себе вберегти від мереженого шахрайства? Про це нам розповість експерт в галузі мереженого етикету.

Виступ експерту в галузі мереженого етикету

Варто пам'ятати п'ять основних правил, які допоможуть безпечно працювати в Інтернеті:

1. Пам'ятайте, що Ви говорите з людиною.

Поставте себе на місце людини, з якою говорите. Відстоюйте свою точку зору, але не ображайте Ваших співрозмовників. Коли ви використаєте телекомунікації, то маєте справу з екраном комп'ютера. Ви не можете жестикулювати, змінювати тон, і вираз обличчя тощо. Вашої особи не має ніякого значення. Слова, тільки слова - це все, що бачить Ваш співрозмовник. Коли ви спілкуєтесь по Інтернету можна дуже легко помилитися в тлумаченні слів Вашого співрозмовника. Коли Ви зв'язуєтеся з ким-небудь, пам'ятайте, що Ваші слова фіксуються.

2. Дотримуйтесь етики спілкування.

Поважайте час і можливості інших. Існує стереотип, що сьогодні в людей залишається усе менше часу і створення нових пристроїв дозволяє заощадити час. Коли Ви посилаєте електронну пошту або спілкуєтесь в Інтернеті Ви фактично претендуєте на чийсь час. І тоді Ви відповідаєте за те, щоб адресат не витратив цей час марно.

4. Не давайте ніякої особистої інформації.

В жодному разі не можна в мережі надавати інформації особистого характеру, такої як: домашню адресу, номер телефону, номер школи, місце роботи батьків, опис квартири тощо.

5. Не надсилайте свої фотокартки незнайомим особам.

Отримавши інформацію, яка змусить почуватися некомфортно необхідно негайно припинити спілкування та повідомити про це батьків або тим кому ви довіряєте.

Пам'ятайте! Спілкування через Інтернет, ніколи не замінить живого спілкування з друзями.

ІІ. Практична частина

Вчитель: А тепер, щоб повторити і закріпити поради наших експертів, я пропоную вам виконати декілька завдань. Ви отримали один на парту аркуш паперу з текстом на ньому.

Завдання 1

Уважно прочитайте листи. Яку відповідь ви дасте на них? Обґрунтуйте.

Лист 1

Привіт! Мене звати Сашко. Мені 15 років. Я живу в Києві. Шукаю друзів по переписці. Я полюбляю комп'ютерні ігри, читати книги, дивитися телевізор. Я мрію подорожувати. Хочу побувати в Лондоні ....

Лист 2

Привіт! Мене звати С. Я хочу з тобою познайомитися. Мені 30 років. Я живу в Сполучених Штатах Америки. Я маю власну фірму. У мене свій двохповерховий будинок. Я збираюся відвідати Україну. Може ми зустрінемося? Пришли мені свою фотокартку та домашню адресу.

Лист 3

Всім!!!

Наша організація займається збиранням коштів для потерпілих від повені в N. Ми купуємо їжу, теплі речі для тих, хто втратив домівки. Не будьте байдужими до чужого горя! Хто скільки може. Наш рахунок № 123456789.

Вдячні діти Вас ніколи не забудуть.

Дякуємо.

(Діти відповідають на листи, обґрунтовуючи свої відповіді)

Вчитель: Молодці. Добре засвоїли прослуханий матеріал. А зараз проведемо невеличке анкетування, щоб визначити рівень вашої поведінки в мережі.

Завдання 2

Анкета «Рівень поведінки в Інтернеті» (додаток 1).

Виберіть, будь ласка, один із двох варіантів відповідей (А або Б) той, котрий найкраще підходить для опису вашої поведінки в Інтернеті й відзначте його галочкою. У цій анкеті немає правильних або неправильних відповідей.

Вчитель: Думаю, цей коротенький тес допоміг вам визначитися з рівнем поведінки та подумати над тим, добре це чи погано.

Завдання 3

Прочитайте уважно листа. Подумайте, які дії допомогли уникнути ситуації. Чому?

В січні цього року я познайомилась по ICQ з кіпріотом, який виступав ініціатором листування. Він був досить наполегливим у продовженні контактів. Написав, що він є 49-річним директором великого підприємства і вислав навіть адресу сайту підприємства. Майже зразу ж після нашого знайомства він почав говорити про те, що має намір приїхати в Київ, і попросив підібрати для нього найдорожчий готель та ресторани. Потім, нібито, з поїздкою в нього не вийшло і він активно почав запрошувати мене на Кіпр. Пропонував покрити всі витрати, пов'язані з проїздом та проживанням. Від такої пропозиції я відмовилась, оскільки вона здалась мені підозрілою, але листуватися з ним продовжувала, так

як він писав цікаві та приємні листи. Тоді він запропонував поїхати з ним на конференцію дилерів „Вольво” в Стамбул. Я зайшла на сайт компанії „Вольво” і не знайшла ніякої інформації щодо проведення конференції, тому від поїздки знову відмовилась. Через декілька днів я розмовляла з своєю однокласницею, котра розповіла мені про кіпріота, з яким вона почала листуватися в Інтернеті. Виявилося, що це був той самий кіпріот, котрий писав і мені, оскільки писав він все те ж саме, що й мені – який він значний бізнесмен, яка в нього велика фірма, як він хоче, щоб вона приїхала до нього в гості. Він також надсилав ті ж самі компліменти та чарівні слова.

(Відповіді дітей)

Вчитель: Отже, сьогодні на уроці ми з’ясували, що під час спілкування в мережі Інтернет, як і будь-де, існують свої правила етикету і, щоб не потрапити в халепу, треба обов’язково їх дотримуватися.

ІІІ. Домашнє завдання

Схематично або у вигляді малюнку зобразити правила безпечної поведінки в Інтернеті.

БЕЗПЕЧНИЙ ІНТЕРНЕТ.
Тренінг для учнів 10-11 класів

Мета: ознайомити дітей з правилами спілкування в Інтернет, з небезпечними кібертехнологіями, з якими можуть зустрітися діти, працюючи в Інтернеті. Розвивати вміння спілкуватись в соціальних мережах та чатах. Провести психологічний тренінг «Інтернет-дерево» та «Хто більше» з метою виховання культури спілкування. Визначити правила безпечного використання Інтернету. Перевірити якість засвоєння отриманих знань.

Хід тренінгу

Вступне слово вчителя (ознайомлення з темою заходу, метою)

Цей тренінг проводиться в рамках всеукраїнської програми «Безпека дітей в Інтернеті». Також для підтримки програми розроблений веб-ресурс «Онляндія» (www.onlandia.org.ua), на якому представлені матеріали для дітей, їх батьків і вчителів — інтерактивні сценарії, короткі тести, готові плани уроків, — завдяки яким діти зможуть освоїти основи безпечної роботи в Інтернеті. На сайті пропонується зрозуміла, застосована на практиці інформація по Інтернет-безпеці, вивчивши яку, навіть починаючі користувачі зможуть ефективно використовувати ресурси мережі і захистити себе від небажаного контенту.

Вправа 1

Правила

Мета: забезпечити конструктивну атмосферу для роботи групи.

Метод: обговорення в групі.

Теоретична інформація: Перший крок в організації роботи тренінгової групи у відповідності з принципами проведення тренінгів – прийняття та засвоєння правил роботи. На початку тренінгу рекомендується разом з учасниками самостійно визначити та обґрунтувати правила і протягом усієї роботи їх дотримуватися.

Існує багато можливостей для розробки правил або визначення рамок роботи для групи. Це гарна можливість знайти шляхи до продуктивної співпраці та пізнати одне одного. Під час роботи над правилами створюються умови для кращого визнання власних потреб та особистих відмінностей.

Правила можуть бути такими:

- приходити вчасно;
- вимкнути мобільні телефони;
- правило «тут і зараз»;
- правило «піднятої руки»;
- правило добровільної активності;

- говорити по черзі й коротко;
- не критикувати;
- бути толерантними;
- дотримуватись конфіденційності;
- правило «вільної ноги».

Вправа 2

Знайомство (гра «Інтернет - дерево»)

Мета: знайомство учасників для створення комфортної атмосфери для роботи.

Метод: індивідуальна робота.

Теоретична інформація

На ватмані малюється дерево. Учасникам тренінгу пропонується придумати собі «нікнейм» та написати його на отриманих стікерах. Після чого кожен з учасників виходить і наклеює свій стікер з «нікнеймом» на дерево та розповідає про себе: своє реальне ім'я, рід заняття, хобі, та чому він придумав такий «нікнейм». Ці «нікнейми» можна використовувати під час спілкування на тренінгу.

Після виконання вправи порівняти отримане дерево з мережею інтернет: так само як багато гілочок на дереві, так багато і користувачів у мережі інтернет.

Вправа 3

Гра «Хто більше?»

Яку Інтернет-термінологію ви знаєте?

- Тренер пропонує учасникам назвати два улюблених фрукта, наприклад, *апельсин, яблуко,* або щось інше.
- По черзі „через одного" діти поділяються на дві групи:

«Апельсини» знаходяться в одній стороні, а «Яблука» - в іншій.

- Кожній з команд видається маркер та лист ватману.
- Тренер пропонує командам написати за 3 хвилини якомога більше Інтернет-термінологій, тобто все, що пов'язано з Інтернетом. Але назви сайтів писати не можна.

Наприклад: *спам, комунікації, вірус, друзі, сайт, пошта та інші.*

- Далі кожна з команд називає одне слово по черзі. Якщо в іншій команді воно є, обидві групи закреслюють слово.
- Перемагає той, в кого найбільша кількість незакреслених слів.

Вправа 4

«Ситуації»

А тепер давайте з вами розберем декілька життєвих ситуацій, що можуть трапитись з вами в інтернеті, та з'ясуємо що ж треба робити в таких ситуаціях.

Уважно прочитайте листи. Яку відповідь ви дасте на них? Обґрунтуйте.

Лист 1

Привіт! Мене звати Сашко. Мені 15 років. Я живу в Києві. Шукаю друзів по переписці. Я полюбляю комп'ютерні ігри, читати книги, дивитися телевізор. Я мрію подорожувати. Хочу побувати в Лондоні ....

Лист 2

Привіт! Мене звати С. Я хочу з тобою познайомитися. Мені 30 років. Я живу в Сполучених Штатах Америки. Я маю власну фірму. У мене свій двохповерховий будинок. Я збираюся відвідати Україну. Може ми зустрінемося? Пришли мені свою фотокартку та домашню адресу.

Лист 3

Всім!!!

Наша організація займається збиранням коштів для потерпілих від повені в N. Ми купуємо їжу, теплі речі для тих, хто втратив домівки. Не будьте байдужими до чужого горя! Хто скільки може. Наш рахунок № 123456789.

Вдячні діти Вас ніколи не забудуть.

Дякуємо.

(Діти відповідають на листи, обґрунтовуючи).

Вправа 5

Гра «Флешка»

Учасники передають один одному флефку та розповідають будь-яку історію пов'язану з використанням Інтернету, що трапилась із ними.

Вправа 6

Робота з журналами, газетами – «Колаж»

Мета: виявити, наскільки тема безпеки в Інтернеті висвітлюється в ЗМІ та довести корисність розповсюдження інформації.

Учасникам пропонують зробити колаж за темою: «Інтернет – «ЗА» і «ПРОТИ».

Вправа 7

Анкета «Рівень поведінки в Інтернеті» (додаток 1)

Виберіть, будь ласка, один із двох варіантів відповідей (А або Б) той, котрий найкраще підходить для опису вашої поведінки в Інтернеті й відзначте його галочкою. У цій анкеті немає правильних або неправильних відповідей.

Вчитель: Думаю, цей коротенький тест допоміг вам визначитися з рівнем поведінки та подумати над тим, добре це чи погано.

Вправа 8

Правила розумного користувача Інтернету

Мета: визначити правила безпечного використання Інтернету

Метод: обговорення в групі

Пропонуємо учасникам тренінгу відповісти на питання:

- Чи вивчаєте ви правила поведінки на дорогах?

- Так. Інтернет – це теж автострада, тільки інформаційна. Давайте розробимо свої правила безпечного користування Інтернетом, які починатимуться зі слова «Я».

***Шість правил розумного користувача Інтернету*:**

1. Я буду поводитись в Інтернеті чемно і не ображати інших.
2. Я буду залишати негарні веб-сайти.
3. Я буду зберігати свій пароль в таємниці.
4. Я буду розповідати своїм батькам про проблеми й користуватися їхньою підтримкою.
5. Я буду шукати цікаві веб-сайти й ділитися посиланнями зі своїми друзями.
6. Я знаю, що можна бути легко обманутим і не буду повідомляти реальні імена, адреси й номери телефонів.

Вправа 8

Гра «Пакуємо валізи»

Наш тренінг дійшов логічного завершення. Подумайте, друзі, щоб ви взяли із собою з тренінга. Давайте запакуємо наші валізи. Що ви в них покладете?

(Учні висловлюють свої думки, що їм запам’яталось з проведенного тренінгу, що стане їм корисним у житті).

ДЕНЬ БЕЗПЕЧНОГО ІНТЕРНЕТУ.
Позакласний захід для учнів 10-11 класів

Мета: навчити дітей безпечно користуватись Інтернетом.

Хід заходу

Ведучий 1: В Україні цей день відзначається вже п’ятий рік поспіль завдяки ініціативи компанії «Майкрософт Україна». З моменту заснування були проведені сотні активностей, спрямованих на захист дітей в Інтернеті. Основні серед них – це запуск освітнього сайту «Онляндія –безпечна веб-країна», на якому всі бажаючі можуть отримати необхідну інформацію, приєднатися до руху й зробити свій посильний внесок у вирішення проблеми.

Ведучий 2: Починаючі з 2008 року проведено 4 000 тренінгів для 161 000 учасників!

За підтримки Міністерства освіти і науки, молоді та спорту України, члена Коаліції за безпеку дітей в Інтернеті 14 лютого 2012 року в навчальних закладах Вільнянського району проводять виховні заходи на тему безпеки дітей в Інтернеті.

Ведучий 3: Загрози, пов'язані з використанням Інтернету

Важко переоцінити переваги й величезний освітній потенціал Інтернету, але водночас з цією мережею пов'язані певні ризики та загрози, про які необхідно знати. Аналіз статистичних даних свідчить про важливість питання захисту молоді та дітей під час роботи в режимі онлайн. Так, за даними Європейської Комісії, 44 % дітей, які використовують Інтернет, стикалися з матеріалами «дорослого» змісту, і про це здогадуються лише 15 % батьків. Перебуваючи в Інтернеті, 40% дітей спілкувались із людьми, які пропонували їм зустрітись особисто, 14 % з цих дітей дійсно намагались зустрітись. 75 % дітей, що працюють у мережі Інтернет, згодні поділи¬тися персональною інформацією про себе або свою родину в обмін на подарунки. Лише 25% підлітків, що зустрічалися з сексуальними домаганнями в мережі Інтернет, повідомили про це батькам.

Ведучий 4: Так! — безпечному Інтернету для дітей в Україні

Проблема безпеки дітей в Інтернеті вже не здається Україні такою далекою. Ніхто не може заперечити, що на сьогоднішній день вона постала особливо гостро. Кожного року аудиторія користувачів всесвітньої мережі дедалі розширюється і її переважну частину становить молоде покоління — діти та підлітки, які повністю не усвідомлюють загрозу, що може чекати на них у віртуальному просторі.

Ведучий 4: Що робити, якщо Ви отримали Scam?

Основний принцип шахрайства - ввести жертву в оману, встановивши з нею довірчі стосунки, і, скориставшись цією довірою, спонукати її під тим або іншим приводом добровільно передати шахраю гроші, майно, права на що-небудь. Для цього існує безліч як психологічних, так і технічних прийомів. З метою шахрайства в останні роки все частіше стали використовуватися можливості Інтернет.

Ведучий 5: Такий вид шахрайства, як «Emergency Scam» чи інакше званий «Scam» - явище вже відоме в світі. Не так давно це стало актуально і для України.

Шахрайство «Scam» полягає в тому, що шахрай, використовуючи ресурси Інтернету (електронна пошта, соціальні мережі тощо), входить в довіру до людини і, отримавши від нього необхідну інформацію, скоює злочин.

Ведучий 6: Варіантів Scam зустрічається дуже багато. Найбільш поширеним є метод, коли шахрай повідомляє потенційній жертві інформацію про великий виграш у лотереї. І для отримання великої суми просить всього лише повідомити наступну інформацію: прізвище та ім'я, домашню адресу, контактний телефон та банківську інформацію.

Ведучий 1: Також поширеним є розсилання листів з інформацією про допомогу потерпілим у катастрофі. Шахрай повідомляє про те, що його онук чи внучка, або член сім'ї, або сусід, потрапили в біду. Далі йде барвистий опис події. Шахрай повідомляє, що він терміново потребує грошей. Жертви дізнаються про шахрайство лише після того, як вже позбулися своїх грошей, переведених на рахунок незнайомців. Шахрай попереджає про те, що «ніхто з родичів нічого не повинен про це знати». Це звучить приблизно так: «Don't tell Dad. He would be very upset with me if he found out. Please send the money ASAP. I'm scared ». (Не говори батькові. Він буде дуже турбуватися, якщо дізнається, що трапилося зі мною. Будь ласка, присилай гроші якомога швидше. Я хвилююся.)

Ведучий 2: **Що потрібно знати?**

Слід пам'ятати, що для доступу до банківського рахунку не обов'язково мати на руках саму платіжну картку - в більшості випадків достатньо знати її дані (номер картки, термін дії та код безпеки). Саме на цій інформації сфокусовані шахраї, відправляючи листи потенційним жертвам.

Слід також знати й те, що при купівлі товарів чи послуг через Інтернет, відомості про вчинені Вами операціях і дані картки після покупки зберігаються в тих же Інтернет-магазинах і, потенційно, можуть дістатися зловмисникам.

Ведучий 3: Дуже часто крадіжці грошей з карт звичайно передує тривала підготовка. По електронній пошті засилається вірус, наприклад, відомий вірус типу Trojan, що запам'ятовує всі уведені паролі та логіни і відправляє їх шахраям. Після того як дані незаконно отримані, шахраї можуть купувати товари та

послуги на Інтернет-сайтах. Адже останніх цифр номера картки (CVV2) достатньо для того, щоб розплачуватися картою в Мережі.

Ведучий 4: Реальні історії...

Ми починаємо публікацію реальних історій, які демонструють витонченість шахраїв. Надсилайте свої історії, питання і наші експерти на цій сторінці підготують відповідь і нададуть практичні поради. Експерти Онляндії та WebMoney, члена Коаліції за безпеку дітей в Інтернеті, постаралися не тільки надати відповідь на питання «чому так сталося?», а й розповісти про заходи безпеки, які необхідно дотримуватися, щоб цього уникнути. Не дозволяйте шахраям обдурити Вас!

Мені на пошту прийшов лист з таким змістом «Шановний Олег Миколайович! Як і домовлялися, я вислав на ваш рахунок 10 800 грн. Відсканована копія платежу в додатку. Перевірте, будь ласка, чи надійшли гроші на ваш рахунок. З повагою, директор компанії DFS Олександр Кочин». Мене дійсно звуть Олег Миколайович, але що робити з цим листом я не знаю.

Олег, 20 років

Як правило, у вкладенні виявляється зовсім не сканована копія якогось документа. Тому слід добре подумати, перш ніж відкривати листи від незнайомого вам користувача. Особливо ті, які містять будь-які вкладення, адже ці вкладення вбільшості випадків виявляються троянськими програмами, а інформація про відправника грошей вигадана.

Ведучий 5: *Одного разу в Інтернеті я потрапила на сайт з інформацією про фотоконкурс для дівчат. Щобвзяти участь, потрібно було відправити 3 своїх фотографії: портрет, фото в повний ріст і фото в купальнику. Три переможниці конкурсу повинні були отримати цінні призи. Я теж вислала свої фотографії на цей конкурс, але не виграла. Через кілька місяців мені зателефонувала подруга і сказала, що бачила моїфотографії на сайті міжнародних знайомств ...Що тепер робити?*

Вікторія, 18 років

Ніколи не можна бути впевненим в тому, що люди, які пропонують вам вислати фотографії, насправді є тими, за кого себе видають. При розміщенні своїх фотографій в Інтернетіви не можете бути застрахованими від ситуацій шахрайства. Якщо ви публікуєте фото або відео в Інтернеті, потрібно розуміти, що подивитися їх зможе кожен. Якщо ви надсилаєте незнайомим людям свої фотографії то потрібно розуміти, що вони можуть передати або продати їх третім особам і т.п.

Ви можете звернутися в міліцію для захисту своїх прав.

Ведучий 6: *На мою електронну адресу прийшов лист, в якому повідомлялося, що я виграла в лотереї 2 тисячі доларів. Щоб отримати виграш треба заплатити 50 доларів банківською карткоюабо через WebMoney: 20 доларів за оформлення документів і 30 доларів податок на виграш. Як правильно вчинити?*

Ольга, 18 років

Звісно, ніякої лотереї немає, а отриманий лист це ще один спосіб обдурити довірливих користувачів Інтернету. Подібна шахрайська схема, використовувана не тільки в мережі, але й у реальному житті. Не висилайте ніякої нформації відправнику листа. Позначте лист «СПАМ» і занесіть його вчорний список.

Ведучий 1: У випадках, якщо Вас обдурили шахраї, використовуючи систему WebMoney, обов'язково звертайтеся до Арбітражної системи! Це постійно діючий сервіс, який розглядає і приймає рішення по претензіях. Тобто, Арбітраж розглядає будь-які претензії до людей, які проводять протиправну, незаконну чи аморальну діяльність в Мережі з використанням WebMoney-реквізитів (шахрайство, розсилка спаму, порушення авторських прав і т.п). Потім щодо шахраїв приймаються відповідні заходи: блокування WM-ідентифікатора, закриття сайту, на який надійшла претензія, передача інформації в правоохоронні органи і т.п.

Ведучий 2: Основи безпеки в Інтернеті для підлітків 15 — 18 років

Для підлітків є розповсюдженим той факт, що інколи вони переживають періоди низької самооцінки, шукають підтримки від своїх друзів та менше бажають виправдовувати очікування своїх батьків. Старші підлітки мають потребу ототожнювати себе з якоюсь групою, та бажають незалежності, й вони схильні порівнювати цінності своєї сім'ї та своїх товаришів. У старшому підлітковому віці діти є більш зрілими та готові взаємодіяти зі світом на інтелектуальному рівні. Загалом підлітки відкриті новим ідеям, але їм бракує життєвого досвіду для того, щоб оцінювати себе. Важливо, щоб батьки продовжували відігравати активну роль у контролі використання дітьми Internet.

Ведучий 3: Що роблять в онлайні підлітки

Підлітки завантажують музику, використовують обмін миттєвими повідомленнями (EN), електронну пошту та грають в онлайнові ігри. Вони активно використовують пошукові сервери для знаходження інформації в Internet. Більшість підлітків відвідувала чат-кімнати (EN), і багато з них брали участь у дорослих або приватних чатах. Хлопці в цьому віці скоріше за все виходять за межі, шукаючи грубий гумор, насильство, азартні ігри та відверті сайти для дорослих. Дівчата, скоріш за все, схильні до розмов в **онлайні** й більш піддані сексуальним домаганням.

Ніколи не відомо хто твій співрозмовник

Ведучий 4: ПРАВИЛА ІНТЕРНЕТ-БЕЗПЕКИ І ІНТЕРНЕТ-ЕТИКИ ДЛЯ ДІТЕЙ І ПІДЛІТТКІВ

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

Ведучий 5: 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.

Ведучий 6: 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.

Ведучий 1: Не відкривайте листи електронної пошти, файли або Web-сторінки, отримані від людей, яких ви реально не знаєте або не довіряєте.

Ведучий 2: Нікому не давайте свій пароль, за виключенням дорослих вашої родини.

Ведучий 3: 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.

Ведучий 4: Завжди будьте ввічливими у електронному листуванні, і ваші кореспонденти будуть ввічливими з вами.

Ведучий 5: У електронних листах не застосовуйте текст, набраний у ВЕРХНЬОМУ РЕГІСТРІ - це сприймається у мережі як крик, і може прикро вразити вашого співрозмовника.

Ведучий 6: Не надсилайте у листі інформації великого обсягу (картинки, фотографії тощо) без попередньої домовленості з вашим співрозмовником.

Ведучий 1: Не розсилайте листи з будь-якою інформацією незнайомим людям без їхнього прохання - це сприймається як "спам", і звичайно засмучує користувачів мережі.

Ведучий 2: Завжди поводьтеся у мережі так, як би ви хотіли, щоб поводилися з вами!

Використані матеріали з Веб-сайту «Он-ляндія».

ІНТЕРНЕТ. БЕЗПЕКА В ІНТЕРНЕТІ.
Брейн-ринг для учнів 11 класу

1. Як називається сукупність веб-сторінок, доступних в Інтернеті, які об'єднані як за змістом, так і навігаційно? (сайт)
2. Як називається масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати? (спам)
3. Алфавітно-цифровий набір символів, що ідентифікує користувача комп'ютерної мережі і разом із паролем використовується операційною системою для надання йому дозволу на з'єднання з комп'ютерною системою та визначення його прав доступу до ресурсів мережі. (логін)
4. Комп'ютерна програма, яка має здатність до прихованого само розмноження. (вірус)
5. Службовий комп'ютер у локальній чи глобальній мережі, що забезпечує функціонування мережі, всі або частину її функцій (сервер)
6. Програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом (Антивірусна програма)
7. Заснований на стандартах набір правил, що визначає принципи взаємодії комп'ютерів в мережі (протокол)
8. Засіб для швидкого обміну текстовими повідомленнями між користувачами інтернету у режимі реального часу (чат)
9. Популярний сервіс в інтернеті, що робить можливим обмін даними будь-якого змісту за допомогою листування.(електронна пошта)
10. Як називається служба IP-телефонії, що забезпечує миттєве відправлення та отримання текстових повідомлень? (ICQ)
11. Програмне забезпечення для комп'ютера під'єднаного до Інтернету, що дає можливість користувачеві взаємодіяти з текстом, малюнками або іншою інформацією на гіпертекстовій веб-сторінці(браузер)
12. Веб-сайт або інша служба у Веб, яка дозволяє користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок та переглядати власний список зв'яків і списки інших користувачів (соціальна мережа)
13. Всесвітня система взаємосполучених комп'ютерних мереж, що базуються на комплекті Інтернет-протоколів.(Інтернет)
14. Назвіть рік виникнення Інтернет (1969)
15. Як звучить на англійській мові вислів «всесвітня паутина»? (WWW)

16. Користувач, який має ширші права порівняно із звичайними користувачами на суспільних інтернет-ресурсах (чатах, форумах). (модератор)

17. Організація, яка надає послуги доступу та передачі (інформації) в Інтернеті (провайдер)

18. В Інтернеті означає прізвисько, псевдонім (нік)

19. Секретне слово або символьна послідовність, призначена для підтвердження особи або прав. (пароль)

20. Коли відзначається Всесвітній день Інтернету? (4 квітня)

21. Що означає вислів «блю туз»?

22. Комп'ютерний хуліган, тобто той, хто здійснює неправомірний доступ до комп'ютерів та інформації. (хакер)

23. Сайт, або програмне забезпечення для спілкування в оф-лайн режимі (форум)

24. Комп'ютерні системи, які забезпечують візуальні і звукові ефекти, що занурюють глядача в уявний світ за екраном монітора. (віртуальна реальність)

25. Протокол передачі файлів (FTP)

26. Що означає вислів юзер? (користувач)

27. Зараз спам – це масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати, а в 1936 році – це …? (гострий ковбасний фарш)

28. Як називається текст для перегляду на комп'ютері, який містить зв'язки з іншими документами? (гіпертекст)

29. Як звучить на комп’ютерному сленгу мережений протокол ICQ? (аська)

30. Веб-сайт, головний зміст якого — записи, зображення чи мультимедіа, що регулярно додаються, що є журналом чи щоденником подій (Блог)

31. Комп'ютерна мережа для обмеженого кола користувачів, що об'єднує комп'ютери в одному приміщенні або в рамках одного підприємства (локальна)

32. Працівник, посадові обов’язки якого передбачають забезпечення роботи комп’ютерної техніки, комп’ютерної мережі і програмного забезпечення в організації (системний адміністратор)

33. Який має колір тло екрана монітора на якому з’являється назва повідомлення про критичну помилку операційної системи Microsoft Windows? (синій)

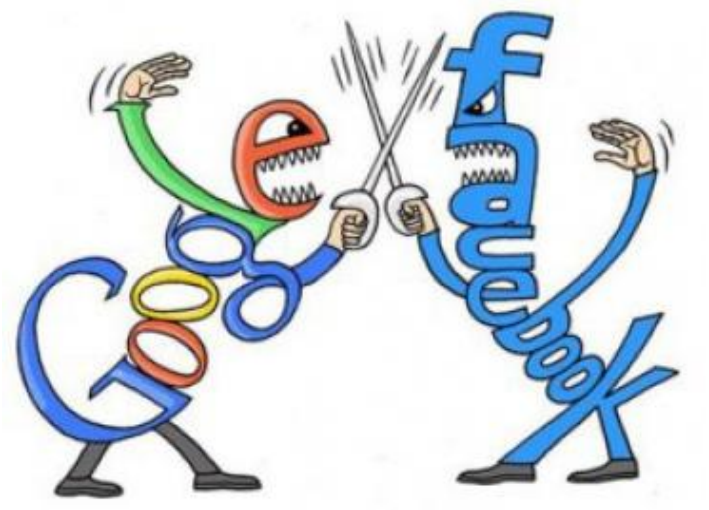
34. Що означає на комп'ютерному сленгу гектар? (1Гб)

35. Людина, що займається програмуванням, виконує розробку програмного забезпечення (програміст)

36. Як юзери називають клавіатуру? (клава)

37. Як записується домен в доменному імені Запорізької області?(zp)

38. Дія групи людей направлена на блокування роботи певного інтернет-ресурсу. (хакерська атака)



УЧНІВСЬКА СТОРІНКА

Ви, звичайно, вже мали змогу переконатися в тому, що Інтернет — це феноменальний за своїми можливостями засіб. Зараз мова піде про небезпеки пов’язані з його використанням.

Інтернет охоплює майже весь світ, а отже ця мережа доступна і для тих людей, які мають далеко не найкращі наміри.

Проблема збільшується ще й тому, що після підключення комп'ютера до Інтернету, виникає ризик вторгнення зловмисника до цього комп’ютера та подальшого використання його для атак на інші комп’ютерні системи.

Злочинці послуговуються чужими комп’ютерами, щоб уникнути відповідальності за свої дії, бо в такому в такому разі визначити справжнє джерело нападу буває дуже складно. Тому захист від зловмисників став одною з основних проблем користувачів Інтернету. Існують й інші види небезпек, наприклад стеження через Інтернет за діяльністю людини чи організації.

І тому постають питання:

- Хто прагне проникнути до мого комп'ютера?
- Хто за мною спостерігає?

Як уберегтися від непроханих візитерів?

Як саме й навіщо люди здобувають інформацію про мене?

Як уберегти персональну інформацію від викрадення?

Хто і як може завдати мені шкоди?

Як убезпечити себе в Інтернеті?

Саме тому в Україні день безпеки в інтернеті відзначається вже четвертий рік поспіль завдяки ініціативи компанії «Майкрософт Україна».

Світовій спільноті слід разом вирішувати проблему кіберзлочинності, сказав прем`єр-міністр Великобританії Девід Кемерон на *міжнародній конференції* з інтернет-безпеки. Кемерон зазначив, що в спробі забезпечити інтернет-безпеку влада країн не повинна піддавати цензурі той чи інший контент. Британський прем`єр назвав хакерство однією з головних проблем сьогоднішнього інтернет-простору.

Правила мережевого етикету

Мережевий етикет (нетикет) - це порядок поведінки, прийнятий у певних соціальних групах. У мережі Інтернет, яка теж є суспільною групою, також сформувалися свої загальновизнані правила, на базі яких будується спілкування в мережі.

Спілкуючись в мережі, не забувайте - Ви маєте справу з живими людьми. Правила хорошого тону для звичайного світу і для віртуального єдині. Не пишіть і не робіть нічого такого, чого не хотіли почути або побачити самі. Навчіться доводити свою позицію, не принижуючи опонента.

Пам'ятайте, людина, з якою ви спілкуєтеся за допомогою клавіатури, не бачить ваших емоцій, не чує вашого голосу. Постарайтеся представити себе на місці цієї людини і правильно формуйте свої думки, для того, щоб уникнути невірного трактування вашої думки.

Є і ще одна причина, по якій слід уважно стежити за тим, що пишеш в мережі. "Слово не горобець, вилетить - не впіймаєш" - ця приказка особливо справедлива для кіберпростору, адже все що ви пишете, зберігається в мережевих сховищах, а значить, зможе спливти в майбутньому і заподіяти багато неприємностей.

Підсумовуючи все вищесказане, можна сказати, що головний і основоположний принцип мережевого етикету - це відношення до віртуальних опонентів, як до реальних людей.

Не робіть нічого такого, чого б ви не зробили в реальному житті, де всі ми, усвідомлено чи ні, підкоряємося негласним правилам. Порушники яких караються законами і людьми. У мережевому суспільстві це зробити порівняно складно. Тому люди відчувають безкарність і поводяться неналежним чином, виправдовуючи себе тим, що мережа - це "зовсім не те, що в житті".

Як би себе люди не намагалися виправдати, але це у будь-якому випадку буде неправильно. Стандарти поведінки більш менш, відрізняються, але в цілому, вони поблажливіші, ніж в звичайному житті.

Прагніть зберігати етику спілкування на належному рівні, ігноруючи думки тих, хто стверджує "тут свобода - хто що хоче, то і говорить". Не вірте цьому. Якщо трапиться побувати в складній етичній ситуації, то поставте себе на це місце в реальному житті і Ви швидко знайдете правильне рішення.

Ще один важливий пункт мережевого етикету. Якщо ви користуєтеся не безкоштовним програмним забезпеченням - заплатіть за нього, ваш внесок сприятиме розвитку програмного ринку. Порушники законів віртуального простору, зазвичай, порушують їх і в реальному житті.

Не забувайте, що ви знаходитеся у віртуальному інформаційному просторі і норми поведінки прийняті на одному сайті, можуть відрізнятися від норм іншого. Наприклад, якщо на одному форумі прийнято круто відходити від основної теми обговорення і це нормально, то на другому це буде сприйнято як поганий тон. Щоб уникнути неприємних ситуацій, перш ніж вступити в дискусію, рекомендуємо придивитися до правил і порядків. Після цього можна спілкуватися.

Поважайте час і можливості інших, адже не всі користувачі мережі Інтернет мають в своєму розпорядженні високошвидкісні канали передачі даних. Для людини, яка підключилася до мережі за допомогою модемного з'єднання, буде вельми скрутно закачати ваш лист, з прикріпленою фотографією (вашої улюбленої кішечки) розміром 20 мегабайт. Зменшивши розмір фотографії, ви заощадите час іншої людини.

Бережіть особу - у мережі, якщо ви побажаєте залишитися інкогніто, ніхто не дізнається ваш вік, колір шкіри, манеру говорити, сімейні подробиці і інші особисті речі. Тому, ваші співбесідники в мережі формуватимуть думку про вас, лише на підставі манери висловлювати думки.

Стежте за тим, що пишете і як пишете. Не припускайтеся орфографічної помилки, адже для більшості людей правила орфографії грають важливу роль. Про людину, яка хронічно здійснює помилки, користувачі мережі можуть думати лише негативно - дурний підліток.

Невірно подана, наперед помилкова інформація може накликати шквал емоцій від ваших співбесідників. Якщо це повториться неодноразово, то може відбутися ситуація як в грі "зіпсований телефон" - ваші слова перекрутяться до невпізнання, а ваша репутація постраждає назавжди.

Зверніть увагу на зміст ваших повідомлень. Вони повинні бути логічні, послідовні і витримані. Можна написати сторінку тексту, але зрозуміти, щось з цього, буде вельми непросто. Це часто буває, коли людина, не дуже розбираючись в темі, хоче переконати співбесідника і використовує для цього багатоскладову термінологію, в якій сам слабкий.

Ніколи не кривдьте віртуальних опонентів, будьте терплячі і ввічливі, не користуйтеся ненормативною лексикою і не влаштовуйте конфлікт не маючи на те підстав.

Допомагайте людям в тих питаннях, в яких ви достатньо компетентні.

Якщо ви самі ставите питання - зробіть його максимально осмисленим і коректним. Так ви швидше отримаєте правильну відповідь. Завдяки вашим відповідям і відповідям інших людей збільшується об'єм знань в мережі, який може стати в нагоді багатьом іншим людям.

Якщо ви одержуєте інформацію від іншої людини за системою коротких повідомлень, що містить велику кількість дрібних реплік, резюмуйте одержані дані і відправте їх на форум - інформація буде в зручному вигляді підготовлена до сприйняття.

Обмін знаннями - це те, для чого глобальна мережа була створена, не відходьте від цих традицій, обмінюйтеся інформацією. Якщо ви володієте цікавою інформацією, яка може зацікавити інших людей, відішліть її на форум. Цим ви зробите свій внесок в світовий інформаційний простір.

Не вплутуйтеся в конфлікти і попереджайте їх.

Флейм - це емоції, виражені текстом, які робляться, не враховуючи думку інших учасників розмови. Чи заборонений мережевим етикетом флейм? І так і ні. Флейм відноситися до старовинних мережевих традицій. У якісному вигляді він може принести приємні емоції для всіх учасників розмови. Але флейм, що переростає в численні злісні повідомлення, якими обмінюються декілька чоловік, заборонений мережевим етикетом. Такі "спалахи" можуть захлеснути всю розмову і втопити корисну інформацію в смітті, знищивши всю позитивну атмосферу.

Поважайте право людини на особисту інформацію.

Не допускайте зловживання своїми можливостями

Завдяки навикам, одержаним в професійній сфері, деякі люди одержують значну перевагу в порівнянні з іншими користувачами мережі. Прикладів цьому маса - системні адміністратори, програмісти, фахівці з кодування інформації. Завдяки своїм широким знанням вони можуть одержати перевагу і скористатися нею проти вас. Наприклад, читати ваше особисте листування. Але такого бути не повинно! Не зловживайте своїми можливостями!

Прощайте помилки інших людей і допоможіть їх виправити, адже і ви теж були колись новачком. Якщо ви побачите, як якась людина робить банальні помилки, наприклад - ставлячи дурні питання або неправильним чином відповідаючи, будьте терпимі до нього. Але допомагаючи людині не треба поводитися гордовито. Скромність прикрашає. Підкажіть про помилку не при всіх, а при особистому спілкуванні.

Безпека в Інтернеті

Інтернет — це феноменальний за своїми можливостями засіб. Зараз мова піде про небезпеки пов'язані з його використанням.

Інтернет охоплює майже весь світ, а отже ця мережа доступна і для тих людей, які мають далеко не найкращі наміри. Проблема збільшується ще й тому, що після підключення комп'ютера до мережі,

а особливо до Інтернету, виникає ризик вторгнення зловмисника до цього комп’ютера та подальшого використання його для атак на інші комп’ютерні системи.

Злочинці послуговуються чужими комп’ютерами, щоб уникнути відповідальності за свої дії, бо в такому в такому разі визначити справжнє джерело нападу буває дуже складно. Тому захист від зловмисників став одною з основних проблем користувачів Інтернету. Існують й інші види небезпек, наприклад стеження через Інтернет за діяльністю людини чи організації.

Як захистити комп'ютер від атак зловмисників?

Існують різні види небезпек, пов'язаних із користуванням Інтернетом. Одні зловмисники прагнуть отримати вашу персональну інформацію та скориставшись нею, зашкодити вам. Інші вибирають об'єктом атак вашу комп'ютерну систему та намагаються вивести її з ладу або використати для приховування своїх шкідливих дій.

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.

Хакери

Спочатку слово хакер було сленговою назвою комп'ютерного ентузіаста. Однак з часом воно набуло негативного значення, й тепер так називають людину, яка без дозволу проникає до чужої комп'ютерної системи з наміром викрасти або зруйнувати дані. Більшість подібних хакерів воліють, щоб їх називали кракерами — від англійського слова «crack», тобто злом.

Існує багато способів, за допомогою яких Хакери проникають до чужих систем.

Найбільш поширеними є такі :

- **Троянські коні**. Це шкідливі програми, які розповсюджуються шляхом обману. 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.
- **Перевантаження сайту або мережі.** Генеруючи багато запитів довільного змісту до сайту або мережі, хакер збільшує їхнє робоче навантаження внаслідок чого цей сайт або мережа не можуть нормально функціонувати.
- **Підміна адрес**. Хакер підмінює адреси сайтів у такий спосіб, що коли користувач зводить у браузері адресу якогось сайту, його спрямовують до зовсім

іншого сайту. Іноді на такому альтернативному сайті міститься негативна інформація про власника того сайту, який збирався відвідати користувач.

- **Соціотехніка.** Цей термін використовується для позначення шахрайських дій, спрямованих на отримання інформації, яка дає змогу проникнути до певної системи та даних, що в ній знаходяться. Соціотехніка зазвичай є грою хакера на довірі людини.
- **Підміна веб-сторінки.** Хакер дістається сайту та змінює на ньому певну веб-сторінку, після чого на ній відображається інша інформація.

УВАГА

Отримавши електронного листа з проханням повідомити персональну інформацію, ніколи не надавайте цю інформацію.

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. Такий вірус потрапляє до комп'ютерної системи, власник якої про це й гадки не має. До того ж іноді вірус якийсь час залишається затаєним, жодним чином себе не викриваючи, і лише після настання певної дати чи події активізується та завдає шкоди комп'ютерній системі.
- **Хробаки.** 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. Найбільш нищівний з усіх хробаків на ім'я I LOVE YOU завдав збитків на 7 млрд. доларів.

УВАГА

Нові віруси та інші методи вторгнення до вашої комп’ютерної системи виникають майже щодня. Тому регулярно перевіряйте наявність оновлень на сайті своєї антивірусної програми. Повідомлення про нові віруси та інші небезпеки з’являються в Інтернеті постійно.

Спам

Спамом називають небажану електронну пошту, тобто пошту, що надходить без вашої згоди.

Люди отримують спам з різних причин. Проте часто вони самі є винуватцями того, що їхня електронна адреса потрапляє до спамерів. Щоб з вами такого не сталося, треба знати, як відбувається полювання за адресами. Зазвичай спамери використовують спеціальні програми-павуки, які обстежують Веб і

відшукують всі адреси електронної пошти, що там з'являються. Тому пам'ятайте: як тільки ви вкажете де-небудь адресу своєї електронної пошти, чекайте надходження спаму.

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. Таке програмне забезпечення має багато функцій. Воно може 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.

Інформацію про відвідувані веб-сторінки також можна отримати із cookie-файлів.

Adware і spyware

Термін adware не має перекладу українською мовою, так називають програми, які під час своєї роботи виводять на екран рекламні стрічки — банери. Подібні програми сповільнюють роботу вашої системи.

Програми типу spyware без вашого дозволу надсилають комусь інформацію про те, що ви робите в Інтернеті. Зазвичай це здійснюється в рекламних цілях. Програмне забезпечення типу spyware також сповільнює роботу системи і навіть призводить до її збоїв. Програми цього типу можуть також збирати без вашого дозволу інформацію з комп'ютера.

Шпигунські програми

Існує безліч причин, з яких певні особи застосовують шпигунські програми, що стежать за вашими діями, аналізують вашу електронну пошту та фіксують адреси відвідуваних вами веб-сторінок. Існує багато засобів, які утруднюють несанкціоноване отримання персональної інформації. Серед них — програми батьківського контролю, що є дуже популярними. Ними користуються не лише батьки, щоб вберегти своїх дітей від відвідування сайтів з небажаним вмістом, а й керівники корпорацій та навчальних закладів, з аналогічною метою. Мандруючи мережею Веб, учні у такому разі стикаються з блокуванням у випадках, коли сторінка, яку вони намагаються відкрити, містить слова, розцінені блокуючою програмою як образливі чи неприйнятні для дитячої або підліткової аудиторії.

На деяких інтернет-порталах, зокрема на MSN, також є засоби блокування доступу до подібних інтернет-ресурсів. Існує багато програм, які містять функції блокування. Крім того, у більшість браузерів вбудовано функції, що дозволяють користувачеві підключатися до певних сайтів лише після введення паролю.

Усі такі програми діють майже однаково. Програма встановлюється на комп'ютер. Коли користувач вводить адресу сайту, програма її перевіряє, звертаючись до бази даних заборонених сайтів. Якщо ця адреса є в базі даних, програма блокує доступ до сайту, і користувач не зможе до нього підключитися, доки не введе пароль. Якщо ж адреси в базі даних немає, програма сканує сам сайт у пошуку певних заборонених слів і тільки після цього надає користувачеві доступ до сайту. Більшість подібних програм щомісяця оновлюють свою базу даних, завдяки чому ця інформація завжди актуальна, незважаючи на швидке зростання кількості інтернет-ресурсів.

Як уберегтися від непроханих візитерів?

Отже, ви мали змогу впевнитись, що є багато людей, які намагаються отримати доступ до чужих комп'ютерів. Проте існують засоби, що утруднюють цей процес або навіть унеможливлюють його. Найпоширеніші з них — брандмауери, а також антивірусне та антиспамове програмне забезпечення. Велике значення має також дотримання користувачами правил безпеки під час роботи в Інтернеті.

Брандмауери

В комп'ютерній мережі брандмауером називати програмне та апаратне забезпечення, яке захищає локальну мережу від небезпек. Брандмауер розташовують між локальною мережею та Інтернетом або між окремими ланками локальної мережі. Він відстежує й аналізує весь потік пакетів з даними що надходить до нього, і пропускає лише дозволені пакети. Таким чином, небезпечний код з Інтернету не може потрапити до локальної мережі. Принцип дії Брандмауера ілюструє.

Антивірусне програмне забезпечення

Однією з найбільших загроз для комп'ютерних систем є віруси. Для боротьби з ними можна придбати програмне забезпечення, що називається антивірусним. Воно працюватиме у вашій системі й перевірятиме на вміст вірусів усі файли, які ви отримуєте електронною поштою, завантажуєте з Інтернету, переписуєте на жорсткий диск або запускаєте на виконання з компакт-дисках чи флешки.

Центр забезпечення безпеки Windows

Основними нововведеннями цього пакету є Центр забезпечення безпеки, за допомогою якого користувач може встановити бажаний рівень захисту комп'ютера, а також вбудований засіб блокування спливаючих вікон у браузері Microsoft Internet Explorer.

Центр забезпечення безпеки складається з трьох компонентів: брандмауера, засобу автоматичного оновлення системи та засобу антивірусного

захисту. Центр регулярно виконує перевірку комп’ютера й нагадує користувачеві, що певна важлива функція вимкнена чи застаріла. Для доступу до Центру забезпечення безпеки потрібно з меню Пуск визвати команду Панель керування та вибрати посилання Центр обеспечения безопасности (Центр забезпечення безпеки).

Блокування спливаючих вікон

Спливаючі вікна з'являються під час перегляду багатьох сайтів. Деякі такі вікна містять лише рекламу, проте є вікна, разом з якими без вашого відома може завантажуватися та встановлюватися програмне забезпечення типу Spyware.

Як зазначалося вище, операційна система Windows XP має засіб блокування спливаючих вікон, який вбудований в Internet Explorer. Користувач може обрати потрібний варіант: блокувати всі такі вікна, блокувати лише ті, що належать до безпечних сайтів, або ж не блокувати жодні.

Антиспамове програмне забезпечення

Програми даного типу застосовуються для фільтрації електронної пошти, вони аналізують усі повідомлення, які надходять до вашого комп'ютера, з метою виявлення та видалення спаму. Зазвичай у таких програмах є можливість задавати правила, за якими бажана пошта буде відокремлюватися від небажаної. Існує також програмне забезпечення, яке розширює антиспамові можливості поштового клієнта. Воно буває різним: одні програми просто ізолюють підозрілі повідомлення, а інші відокремлюють усі повідомлення із зворотними адресами, яких немає у сформованому вами списку.

Запобігання зараженню вірусами

Немає й не може бути стовідсоткової гарантії того, що ви ніколи не підхопите в Інтернеті вірус, не зазнаєте вторгнення чи не отримаєте спам, — певний ризик завжди існує. Для запобігання цьому потрібно використовувати відповідні програмні засоби, завжди керуватися здоровим глуздом та дотримуватися правил безпечної поведінки в Інтернеті. Ось деякі з цих правил.

- На комп'ютері завжди має функціонувати антивірусне програмне забезпечення. Стежте за його актуальністю. Настройте програму в такий спосіб, щоб вона автоматично сканувала систему, коли ви не працюєте, скажімо, по неділях чи вночі.
- Не відкривайте файли-вкладення, які надходять разом із повідомленнями електронної пошти, якщо ви не впевнені, що вони містять саме ті дані, на які ви чекаєте.
- Використовуйте лише те програмне забезпечення, яке надійшло з перевірених джерел.
- Своєчасно встановлюйте оновлення операційної системи.

Як захиститися від тих, хто хоче використати мою персональну інформацію?

Крім хакерів, які намагаються завдати шкоди вашому комп'ютеру, існують зловмисники, що прагнуть отримати вашу персональну і конфіденційну інформацію та, використовуючи її, завдати вам шкоди.

Як саме й навіщо люди здобувають інформацію про мене?

Ми вже розповідали про існування певної категорії людей, що здійснюють атаки на чужі комп'ютери задля отримання персональної інформації. Зазвичай їхніми об'єктами стають бази даних великих корпорацій, де зберігаються такі відомості, як персональні ідентифікаційні номери, номери банківських рахунків та кредитних карток клієнтів. Проте відомо багато випадків, коли жертвами зловмисників стають приватні особи, особливо якщо вони передають конфіденційну інформацію через Інтернет без належного захисту. Часом зловмисники намагаються викрасти персональну інформацію для того, щоб від імені іншої людини відкривати рахунки, купувати товари тощо. Найчастіше викрадають дані про банківські картки. Анонімність і величезні розміри Інтернету роблять його «землею обітованою» для шахраїв усіх ґатунків.

Як уберегти персональну інформацію від викрадення?

Незважаючи на всі пов'язані з Інтернетом загрози, ним можна безпечно користуватися за умови дотримання певних правил. Аналогічні правила та надійні й безпечні методи передавання даних Інтернетом розроблені і для персональної інформації.

Захищені сайти та шифрування

Ніколи не надсилайте персональну інформацію незнайомим людям. Це основне правило безпеки. Проте ми можемо визначити ситуації, коли це робити безпечно. Головне, в кожному випадку треба бути впевненим, що одержувач інформації надійний. Не завадить також переконатися, що сайт захищений і на ньому використовуються технології шифрування.

Захищена веб-сторінка

Зверніть увагу на значок замка у правій частині рядка стану браузера. Значок замка показує, що сайт зашифрований. Він підтримується всіма браузерами та застосовується для безпечного передавання інформації.

Правила безпеки, яких слід дотримуватися під час передавання інформації Інтернетом

Коли ви працюєте із захищеними сайтами, дотримуйтесь наведених нижче правил, які стосуються надання вами будь-якої інформації. Це гарантуватиме, що вона не потрапить до чужих рук. Навіть якщо у вас поки немає власної картки чи банківського рахунку, краще заздалегідь виробити звичку дотримуватись правил, наведених у цьому розділі.

- Не надавайте більше інформації, ніж потрібно.
- Захищені сайти зазвичай вимагають введення імені користувача та пароля. Робіть його довжиною щонайменше вісім символів, комбінуючи букви та числа. І головне, паролем не повинно бути щось очевидне, якісь слова чи дати.

ПРИМІТКА

Зручно мати два пароля: один для так званих розважальних сайтів, тобто ігор, чатів тощо, а інший для більш важливих дій, наприклад для придбання товарів. Тоді зменшиться ймовірність, що ваші важливі дії піддаватимуться ризику. І ніколи не використовуйте для паролів такі дані, як дата народження, номер телефону чи ім'я.

- Користуйтеся останньою версією браузера. У новіших браузерах реалізовані останні досягнення в галузі шифрування та інших технологій захисту й безпеки.
- Уважно читайте правила безпеки сайту. Адже навряд чи вам сподобається, коли інформацію, що ви надасте про себе, організація згодом продасть власникам розсилок.
- Занотовуйте інформацію про дії, пов'язані з купівлею або замовленням товарів через Інтернет.

Як захиститися від людей, які прагнуть завдати мені шкоди?

Коли зловмисник, вкравши ідентифікаційні дані, знімає гроші з чужого рахунку, це дуже неприємно, але значно гірше, коли він отримає персональну інформацію і це стане загрозою безпеці чи життю людини.

Хто і як може завдати мені шкоди?

Існують особи, які через Інтернет знайомляться з молодими людьми, здобувають їхню довіру, випитують особисті дані й призначають зустріч.

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.

Настроїти свою програму обміну миттєвими повідомленнями можна так, що «бачити» вас і надсилати вам повідомлення зможуть лише люди зі складеного

вами списку знайомих. Можна навіть відкрити кімнату чату зі своїми друзями, але треба уважно стежити, щоб до неї не потрапили сторонні особи.

- 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, навчальний заклад, розклад занять або відомості про родину.

Виконуйте три наведені нижче рекомендації, і використання Інтернету буде для вас безпечним:

Захистіть свій комп'ютер

- Завжди оновлюйте операційну систему.
- Використовуйте антивірусну програму.
- Використовуйте брандмауер.
- Робіть резервні копії важливих файлів.
- Будьте обережними, завантажуючи вміст.

Захистіть себе в онлайні

- Будьте обережними, надаючи особисту інформацію.
- Думайте про те, з ким ви розмовляєте.
- Пам'ятайте, що в Інтернеті не все є надійним і не всі є чесними.

Дотримуйтесь правил

- Ви маєте дотримуватися законів навіть в Інтернеті.
- Пам'ятайте, що в Інтернеті ви повинні піклуватися про інших так само, як про себе.

Реальні історії шахрайства в Інтернеті

Основний принцип шахрайства - ввести жертву в оману, встановивши з нею довірчі стосунки, і, скориставшись цією довірою, спонукати її під тим або іншим приводом добровільно передати шахраю гроші, майно, права на що-небудь. Для цього існує безліч як психологічних, так і технічних прийомів. З метою шахрайства в останні роки все частіше стали використовуватися можливості Інтернет.

Такий вид шахрайства, як «Emergency Scam» чи інакше званий «Scam» - явище вже відоме в світі. Не так давно це стало актуально і для України.

Шахрайство «Scam» полягає в тому, що шахрай, використовуючи ресурси Інтернету (електронна пошта, соціальні мережі тощо), входить в довіру до людини і, отримавши від нього необхідну інформацію, скоює злочин.

Варіантів Scam зустрічається дуже багато. Найбільш поширеним є метод, коли шахрай повідомляє потенційній жертві інформацію про великий виграш у лотереї. І для отримання великої суми просить всього лише повідомити наступну інформацію: прізвище та ім'я, домашню адресу, контактний телефон та банківську інформацію.

Також поширеним є розсилання листів з інформацією про допомогу потерпілим у катастрофі. Шахрай повідомляє про те, що його онук чи внучка, або член сім'ї, або сусід, потрапили в біду. Далі йде барвистий опис події. Шахрай повідомляє, що він терміново потребує грошей. Жертви дізнаються про шахрайство лише після того, як вже позбулися своїх грошей, переведених на рахунок незнайомців. Шахрай попереджає про те, що «ніхто з родичів нічого не повинен про це знати». Це звучить приблизно так: «Don't tell Dad. He would be very upset with me if he found out. Please send the money ASAP. I'm scared ». (Не говори батькові. Він буде дуже турбуватися, якщо дізнається, що трапилося зі мною. Будь ласка, присилай гроші якомога швидше. Я хвилююся.)

Шахраї вигадали новий спосіб підзаробити на юзерах “ВКонтакте”

Компанія “Доктор Веб” повідомила про поширення чергової схеми шахрайства, спрямованої проти учасників соціальної мережі “ВКонтакте”.

Користувачі "ВКонтакте" знову потрапили під приціл зловмисників

В першу чергу це стосується користувачів, які заходять в інтернет через мобільний телефон з підтримкою платформи Java ME.Суть використовуваної зловмисниками техніки полягає в розсилці ICQ спам-повідомлень, які закликають інтернет-користувачів скачати мобільний Java-додаток, який нібито є зручним і функціональним клієнтом для соціальної мережі “ВКонтакте”.В процесі установки програма відсилає SMS на один з платних номерів і просить власника пристрою ввести у відповідній формі на сайті кіберзлочинців отриманий у повідомленні код. Таким чином користувач погоджується стати передплатником певної послуги, за використання якої з його рахунку мобільного оператора буде щомісяця списуватися певна сума. Програма представляє собою файл у форматі. Jar, здатний запуститися практично на будь-якому портативному пристрої, що підтримує Java ME.Фахівці з інформаційної безпеки рекомендують користувачам бути дуже пильними та обережними під час роботи у мережі.

Реальні історії...

Мені на пошту прийшов лист з таким змістом «Шановний Олег Миколайович! Як і домовлялися, я вислав на ваш рахунок 10 800 грн. Відсканована копія платежу в додатку. Перевірте, будь ласка, чи надійшли гроші на ваш рахунок. З повагою, директор компанії DFS Олександр Кочин». Мене дійсно звуть Олег Миколайович, але що робити з цим листом я не знаю.

Олег, 20 років

Як правило, у вкладенні виявляється зовсім не сканована копія якогось документа. Тому слід добре подумати, перш ніж відкривати листи від незнайомого вам користувача. Особливо ті, які містять будь-які вкладення, адже ці вкладення в більшості випадків виявляються троянськими програмами, а інформація про відправника грошей вигадана.

Одного разу в Інтернеті я потрапила на сайт з інформацією про фотоконкурс для дівчат. Щоб взяти участь, потрібно було відправити 3 своїх фотографії: портрет, фото в повний ріст і фото в купальнику. Три переможниці конкурсу повинні були отримати цінні призи. Я теж вислала свої фотографії на цей конкурс, але не виграла. Через кілька місяців мені зателефонувала подруга і сказала, що бачила мої фотографії на сайті міжнародних знайомств ... Що тепер робити?

Вікторія, 18 років

Ніколи не можна бути впевненим в тому, що люди, які пропонують вам вислати фотографії, насправді є тими, за кого себе видають. При розміщенні своїх фотографій в Інтернеті ви не можете бути застрахованими від ситуацій шахрайства. Якщо ви публікуєте фото або відео в Інтернеті, потрібно розуміти, що подивитися їх зможе кожен. Якщо ви надсилаєте незнайомим людям свої фотографії то потрібно розуміти, що вони можуть передати або продати їх третім особам і т.п.

Ви можете звернутися в міліцію для захисту своїх прав.

На мою електронну адресу прийшов лист, в якому повідомлялося, що я виграла в лотереї 2 тисячі доларів. Щоб отримати виграш треба заплатити 50 доларів банківською карткою або через WebMoney: 20 доларів за оформлення документів і 30 доларів податок на виграш. Як правильно вчинити?

Ольга, 18 років

Звісно, ніякої лотереї немає, а отриманий лист це ще один спосіб обдурити довірливих користувачів Інтернету. Подібна шахрайська схема, використовувана не тільки в мережі, але й у реальному житті. Не висилайте ніякої інформації відправнику листа. Позначте лист «СПАМ» і занесіть його в чорний список.

У випадках, якщо Вас обдурили шахраї, використовуючи систему WebMoney, обов'язково звертайтеся до Арбітражної системи! Це постійно діючий сервіс, який розглядає і приймає рішення по претензіях. Тобто, Арбітраж розглядає будь-які претензії до людей, які проводять протиправну,

незаконну чи аморальну діяльність в Мережі з використанням WebMoney-реквізитів (шахрайство, розсилка спаму, порушення авторських прав і т.п). Потім щодо шахраїв приймаються відповідні заходи: блокування WM-ідентифікатора, закриття сайту, на який надійшла претензія, передача інформації в правоохоронні органи і т.п.

Як вкрасти мільйон

За даними Національної Ліги Споживачів (National Consumers League), в 2002 році в США найбільш часто використовувалися такі види шахрайства:

Крадіжка інформації про кредитні картки

Шахраї, що отримали інформацію про особисті дані власника кредитної картки, можуть розплачуватися нею в інтернет-магазинах, брати банківські кредити, орендувати житло, претендувати на допомогу і т.д.

Інтернет-магазини й аукціони

Схема: покупець платить гроші за покупку в інтернет-магазині, але, або не одержує її, або одержує товар у меншій кількості або гіршої якості. Найбільш популярний вид шахрайства в Інтернеті. За даними Центру аналізу інтернет-шахрайства, подібні злочини в 2002 році склали 27% від числа зафіксованих злочинів у всесвітній Мережі.

Інвестиції

Компанія пропонує купити її акції або зробити приватні інвестиції, обіцяючи значний прибуток. Зазвичай для залучення жертв, шахраї оперують фальшивою статистикою і повідомляють завідомо неправдиві відомості про історію або власників компанії.

Збір пожертвувань

Збір пожертвувань широко поширений в США. 90% американців жертвують великі або менші суми на різні благодійні цілі. Цим користуються шахраї. Вони просто створюють фальшиву благодійну організацію, яка спеціалізується на якому-небудь добру справу, і абсолютно відкрито збирають пожертви. Єдина відмінність від звичайних благодійних фондів полягає в тому, що гроші привласнюють шахраї.

Відновлення кредитної історії

Практично кожен житель США і кожна компанія володіють своєю кредитною історією - хронікою отримання та погашення кредитів. У США існує декілька незалежних кредитних бюро, які відстежують кредитну історію американців, обмінюються інформацією і діють абсолютно незалежно як один від одного, так і від сторонніх фірм і організацій. Вплинути на їх дії неможливо. Багато американців виявляються не в змозі нести кредитне тягар, і їх кредитна історія погіршується, що робить неможливим покупку будинку, машини і т.д.,

оскільки банки не хочуть зв'язуватися з ненадійним позичальником. Шахраї пропонують за скромну плату «поліпшити» кредитну історію - природно, ці обіцянки не виконуються, оскільки не можуть бути виконані в принципі.

Погашення боргів

Вчасно неповернені кредити і неоплачені рахунки вважаються особистим обов'язком жителя США. Досить часто людина виявляється не в змозі оплачувати всі свої рахунки. Цим користуються шахраї: вони пропонують наступну схему: їхня компанія самостійно оплачує рахунки жителя США і домагається серйозних знижок від кредиторів, а жертва компенсує витрати компанії. У реальності, шахраї лише отримують гроші від своїх жертв.

Пропозиція роботи

Шахраї пропонують вигідну роботу вдома. Проте жертві припадає по грабіжницьким цінам оплачувати надані витратні матеріали, робити гарантійний або вступний внесок або частину часу працювати безкоштовно, в якості випробувального терміну.

Страховка

«Страхова» компанія пропонує рекордно низькі розцінки за свої послуги. У дійсності, або ця компанія існує лише на папері, або вона закладає в договір з клієнтом такі умови, які роблять неможливим отримати страхове відшкодування.

Пільгові кредити

Фізичним особам часто пропонують пільгові кредити. Однак для отримання такого кредиту шахраї вимагають зробити якийсь вступний внесок (наприклад, щоб отримати кредит в 100 $, жертва платить 150 $) або закладають у договір грабіжницькі відсотки.

«Нігерійські листи»

Одержувачу листа пропонується взяти участь у перекладі з нігерійського (ганського, лівійського, конголезького, мозамбіцького і т.д.) банку в банк США декількох мільйонів доларів, що належать спадкоємцям африканських президентів, міністрів, диктаторів, королів і т.д. За свою допомогу, одержувач повинен отримати чверть або третина переведеної суми. Однак, для демонстрації чистоти намірів, жертві пропонується перевести кілька тисяч доларів на рахунок шахраїв. Ще в 2001 році «нігерійським листів» повірили 15,5% жертв онлайн-шахраїв, в 2002 році кількість потерпілих різко впала - до 1%.

Фінансові «піраміди»

Дана схема широко відома і вперше була використана кілька сот років тому. Проте до цих пір фінансові «піраміди» приваблюють жертв. Остання з звалилися в США «пірамід» залучила кошти 7 тис. осіб, кожен з яких втратив близько 3 тис. дол

Податки

Іноді жителі США не встигають вчасно подати податкову декларацію. Шахраї пропонують підтасувати дані про час доставки декларації в податкові служби і, таким чином, уникнути неприємностей.

Телефонний зв'язок

Жертві пропонується зателефонувати за телефонним номером, де хвилина розмови коштує величезні гроші. Дрібні телефонні компанії також вдаються до шахрайства: вони виставляють своїм клієнтам рахунки, куди включені сервіси (наприклад, голосова пошта), яку клієнт не замовляв.

Туризм \

Шахраї або недобросовісні бізнесмени продають своїм жертвам тури або квитки в готелі, реальні умови в яких значно поступаються рекламі. Наприклад, замість п'ятизіркового готелю жертва шахраїв опиняється в тризірковому.

Революційний метод позбавлення від зайвої ваги

Реклама обіцяє рятування від зайвої ваги протягом днів або тижнів при використанні нового чудодійного препарату або дієти. У кращому випадку, жертва стане володарем непотрібного продукту, в гіршому - здоров'я опиниться під загрозою.

Як не стати жертвою шахраїв

Експерти ФБР пропонують ряд простих рекомендацій, виконання яких може зробити зусилля шахраїв безрезультатними.

- Якщо щось звучить дуже заманливо, щоб бути правдою - це неправда.

- Реклама може обманювати. Ніколи не довіряйте рекламі.

- Уважно читайте всі пункти договору. Не підписуйте нічого, поки не переконаєтеся в тому, що всі положення угоди зрозумілі і влаштовують вас. Вимагайте пояснень, якщо вам щось незрозуміло.

- Якщо якийсь пункт договору не зафіксовано у письмовій формі, а обговорювалося лише на словах, це означає, що вас намагаються ввести в оману.

- Завжди дізнавайтеся адресу, телефон та інші координати компанії і спробуйте навести про неї довідки (у США це робиться через особливу організацію Better Business Bureau, яка виступає в ролі захисника прав постраждалих споживачів).

- Не довіряйте фірмам, що базується не у вашому регіоні.

- Купуйте товари та послуги у компаній, які базуються у вашому регіоні. В іншому випадку, ви не маєте можливості заздалегідь перевірити їх реальну якість.

- Якщо вам роблять комерційні пропозиції по телефону, завжди вимагайте надання вам повної інформації у письмовій формі.

- Відмовляйтеся від усіх «конфіденційних» пропозицій.

Хакери мережі анонімус

Хакери міжнародної мережі «Анонімус» продовжили атаки по всьому світі.

У Сполучених Штатах – виведений з ладу сайт ЦРУ, в Ірані – зламана електронна пошта помічників президента Башара Асада. В Росії дії хакерів спричинили скандали, які зачепили і Україну. Здається, несподівано для всіх, у світі з'явилася нова глобальна та потужна сила.

Приватне листування, ймовірно, Кремлівських чиновників і їхніх помічників, спричинив ефект бомби, що розірвалася. Росіяни дізналися імена людей, що за свої коментарі в мережі отримували гроші із Кремля. Електронну пошту російського чиновника зламали хакери з відомої міжнародної групи «Анонімус».

В інтернеті з'явилося відео про хакерів з «Анонімус». Воно швидко стало лідером переглядів.

Невідомі хакери загрожують чиновникам. Єдиний спосіб зберегтися від скандалів – не порушувати законів, не брехати та не брати хабарів.

«Анонімуси» представляють новий вид хакер – інтернет активістів. Ефектні, активні,публічні, із власними політичними ідеями. Але хакери існували і до «Анонімусів», і більшість далеко не Робін Гуди.

Український хакер із групи «Анонімус», який минулого тижня атакував державні сайти, підтвердив існування в Україні цілого ринку чорних хакерських груп. Він сказав: «Нажаль це правда. Хакерів дуже багато. Вони діють групами або поодинці. Деякі групи хакерів пропонують свої послуги за гроші. Більшість їх клієнтів – це великі корпорації, банки, фінансові установи. Вони на замовлення зламують клієнтські бази, а компанії використовують інформацію проти суперників у своєму бізнесі.»

За інформацією ТСН тижня, день роботи чорного хакера розпочинається від 100 дол. , але залежно від складності роботи може сягати до 1500 дол. на добу. Робота, яку підкидають звичайні українці – дрібніша: зламати електронну пошту або акаунт у соціальній мережі. Такі прохання часто надходять від людей, занепокоєних у подружній зраді.

Американське ФБР називає українських хакерів найнебезпечнішими у світі. Потужна школа математики та інформатики виростила в Україні першокласних комп'ютерних фахівців. Одні розробляють комп'ютерні іграшки, які стають бесселерами, інші створюють спец ефекти до російських та голівудських блокбастерів. Треті взламують системи безпеки, аби знайти їх слабкі місця і щоб зробити інтернет безпечнішим. А хтось навпаки - пише віруси, що крадуть паролі, номера рахунків кредитних карток.

Хакери – це люди, які можуть повністю замінити зовнішню розвідку. Не виходячи з кімнати, вони отримують надсекретну інформацію.

ТЕСТИ

1. Як розповсюджуються комп'ютерні віруси?
   - ☐ Через повідомлення електронної пошти.
   - ☐ Через подорожування по мережі.
   - ☐ Через вашу квартиру.
   - ☐ Вони можуть розповсюджуватися лише злочинцями.
2. Що робить брандмауер?
   - ☐ Не дозволяє зловмисникам проникнути у ваш комп'ютер і дивитися ваші файли та документи.
   - ☐ Захищає ваш комп'ютер від вірусів.
   - ☐ Захищає конфіденційні документи, збережені на вашому комп'ютері.
   - ☐ Захищає ваш комп'ютер від пожежі.
3. Чи завжди відправник повідомлення електронної пошти є тією особою, якою здається?
   - ☐ Так.
   - ☐ Так, якщо ви знаєте відправника.
   - ☐ Ні, не завжди, оскільки інформацію про відправника можна легко підробити.
   - ☐ Лише в Україні.
4. На екрані вашого комп'ютера висвітлюється повідомлення, якого ви не розумієте. Ви повинні:
   - ☐ Продовжувати так, як ніби нічого не трапилося.
   - ☐ Натиснути «Ок» або «Так».
   - ☐ Звернутися за порадою до свого вчителя, батьків або опікуна.
   - ☐ Повністю припинити використання Інтернету.
5. Отримавши підозріле повідомлення електронної пошти, потрібно:
   - ☐ Не відкриваючи, видалити його.
   - ☐ Відкрити повідомлення і подивитися, чи не містить воно чогось важливого.
   - ☐ Відкрити вкладення до повідомлення (якщо воно є).
6. Ви отримуєте ланцюговий лист у вашій скриньці електронної пошти. У цьому повідомленні йдеться, що ви повинні відправити його своїм друзям. Ви повинні:
   - ☐ Відправити його п'яти друзям.
   - ☐ Відправити його не п'яти, а десяти друзям.
   - ☐ Не відправляти ніяких ланцюгових листів.
   - ☐ Відповісти відправнику, що більше не хочете отримувати від нього ніяких повідомлень.

7. Коли ви можете безпечно повідомити іншим ваш телефонний номер, або домашню адресу в Інтернеті?

- ☐ Завжди.
- ☐ Якщо це спеціально просять.
- ☐ У чат-кімнатах, коли ваш друг по чату хоче це знати.
- ☐ З обережністю, людям, яким ви довіряєте.

8. Ви випадково прочитали пароль, який ваш друг залишив записаним на шматку паперу. Що ви маєте зробити?

- ☐ Запам’ятати його.
- ☐ Спробувати забути пароль.
- ☐ Сказати своєму другові, що ви прочитали пароль і сказати йому/їй змінити його та порадити більше ніколи не записувати ніде свої паролі.
- ☐ Повідомити пароль своїм батькам.

9. Що таке «мережний етикет»?

- ☐ Правила поводження за обіднім столом.
- ☐ Правила дорожнього руху.
- ☐ Поради щодо того, як поводитися в Інтернеті.
- ☐ Закон, який стосується Інтернету.

10.Чого ви не повинні робити в Інтернеті?

- ☐ Ображати інших.
- ☐ Шукати інформацію.
- ☐ Грати в ігри.
- ☐ Спілкуватися зі своїми друзями.

ПАМ’ЯТКИ ДЛЯ УЧНІВ ТА БАТЬКІВ

Безпека дітей в Інтернеті

Пам’ятка учням

- Нікому без дозволу батьків не давати особисту інформацію: домашню адресу, номер домашнього телефону, робочу адресу батьків, їхній номер телефону, назву й адресу школи.
- Якщо знайдете якусь інформацію, що турбує вас, негайно сповістіть про це батьків.

- Ніколи не погоджуватися на зустріч з людиною, з якою ви познайомилися в Інтернеті. Якщо все ж таки це необхідно, то спочатку потрібно спитати дозволу батьків, а зустріч повинна відбутися в громадському місці й у присутності батьків.
- Не посилати свої фотографії чи іншу інформацію без дозволу батьків.
- Не відповідати на невиховані і грубі листи. Якщо одержите такі листи не з вашої вини, то сповістіть про це батьків, нехай вони зв'яжуться з компанією, що надає послуги Інтернет.
- Розробити з батьками правила користування Інтернетом. Особливо домовитися з ними про прийнятний час роботи в Інтернеті і сайти, до яких ви збираєтесь заходити.
- Не заходити на аморальні сайти і не порушувати без згоди батьків ці правила.
- Не давати свої паролі нікому, крім батьків, навіть найближчим друзям.
- Не робити протизаконних вчинків і речей в Інтернеті.
- Не шкодити і не заважати іншим користувачам.

Небажаний вміст в Інтернеті

Небажана маса електронних повідомлень відома як небажана пошта, або спам. Вона перенавантажує системи електронної пошти і може заблокувати поштові скриньки. Як інструмент для відправки небажаної пошти інколи використовують хробаків електронної пошти.

П’ять правил використання електронної пошти:

1. Ніколи не відкривайте підозрілі повідомлення або вкладення електронної пошти, що надійшли від людей, яких ви не знаєте. Натомість відразу видаляйте їх, вибравши відповідну команду в меню повідомлення.

2. Ніколи не відповідайте на небажану пошту.

3. Використовуйте фільтр спаму свого провайдера інтернет-послуг або програми електронної пошти (якщо він є).

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

5. Ніколи не пересилайте «ланцюгові» повідомлення електронної пошти. Видаляйте їх одразу після надходження.

Якщо ваша дитина отримує зловмисні повідомлення електронною поштою або sms:

- Скажіть дитині, що вона не повинна відкривати такі повідомлення або інші повідомлення від незнайомої людини.
- Не слід відповідати на такі повідомлення. Однак варто зберегти їх на випадок, якщо ситуацію необхідно буде розв'язувати з іншою людиною.
- Якщо ви виявите, що відправник ходить до тієї самої школи, що й ваша дитина, зв'яжіться зі школою.
- Якщо образи продовжуються, необхідно змінити адресу електронної пошти або номер телефону дитини.

Пам'ятайте:

- Зловмисні повідомлення можна зберегти для подальших дій.
- Можна скоригувати настройки програми електронної пошти, щоб вона направляла повідомлення від певного відправника до окремої папки. У такому випадку вашій дитині не потрібно буде їх читати.
- Якщо ви знаєте адресу електронної пошти відправника, можете відправити копію зловмисного повідомлення постачальнику інтернет-послуг з проханням скасувати зазначену адресу електронної пошти.
- Якщо ви не знаєте адреси відправника, попросіть вашого постачальника інтернет-послуг надати вам допомогу.

Додаткові правила

Закривайте сумнівні спливаючі вікна

Спливаючі вікна — це невеликі вікна з повідомленнями, які закликають вас клацнути у вікні. Якщо таке вікно з'являється на вашому екрані, то найбезпечніша річ, яку можна зробити, — це закрити вікно, клацнувши значок X (зазвичай його розміщено у верхньому правому куті). Ніколи не можна передбачити, які дії зробить програма, навіть якщо ви клацнете кнопку «Ні».

Не допускайте того, щоб вас ошукали

Приховати свою особу в Інтернеті легко. Рекомендується перевірити особу людини, з якою ви спілкуєтеся (наприклад, у групах обговорення). Не повідомляйте особисту інформацію через Інтернет нікому, крім людей, яких ви знаєте і яким довіряєте. Якщо вас просять надати персональну інформацію на веб-сайті, завжди перевіряйте розділ «Умови використання» або «Політика захисту конфіденційної інформації», щоб пересвідчитися, що оператор веб-сайту пояснив, для чого буде використовуватись інформація і чи буде вона передаватись іншим особам.

Обговоріть з дітьми правила використання Інтернету

Багато матеріалів, доступних в Інтернеті, не підходять для неповнолітніх. Обговоріть зі своїми дітьми, як правильно та безпечно використовувати Інтернет.

Про інформаційну безпеку

Пам'ятайте

Розмістивши інформацію в Інтернеті, ви втрачаєте контроль над нею і в більшості випадків вже ніколи не зможете видалити всі її копії.

Перевіряйте

Завжди слід переконатися, що ви знаєте людину, якій надаєте інформацію, і знаєте, для чого її буде використано.

Думайте

Чи безпечно розміщувати особисту інформацію на своєму веб-сайті, якщо ви не впевнені в тому, для чого вона використовуватиметься?

Зазначте

Імена учнів, їхні фотографії та іншу особисту інформацію, що міститься у шкільному журналі, можна публікувати на шкільному веб-сайті лише зі згоди учнів та їхніх батьків.

Закони Інтернету

Що дозволено і що не дозволено в Інтернеті

Інтернет є публічним місцем. Працюючи в онлайні, слід дотримуватися основних правил так само, як ви дотримуєтеся правил дорожнього руху, перебуваючи за кермом.

Закони стосуються й Інтернету

Хоча більшість законів було створено до того, як Інтернет набув широкого розповсюдження, дія законів розповсюджується і на Інтернет. Все, що є незаконним у повсякденному житті, є незаконним і в онлайні.

Надаючи безпрецедентні можливості для вільного спілкування, Інтернет водночас накладає й відповідальність. Зокрема, ви несете відповідальність за вміст і законність свого веб-сайту.

Авторське право

Авторське право захищає спосіб, в який ви втілюєте ідею в життя, але не саму ідею. Копіювати матеріали з Інтернету для використання в особистих цілях дозволено, але передавати та подавати такий матеріал як власний не можна. Наприклад, якщо ви використовуєте матеріал для своєї презентації, то маєте посилатися на джерело.

Передавання недозволеного матеріалу (зокрема, незаконних копій фільмів або музичних творів, доступних у однорангових (P2P) мережах) є незаконним.

Копіювання програмного забезпечення та баз даних, для використання яких потрібні ліцензії, є незаконним, навіть якщо це робиться з метою застосування в особистих цілях.

Незаконне використання матеріалів може призвести до позовів за спричинені збитки і мати інші наслідки, передбачені законодавством.

Коротка пам’ятка для батьків

- Підвищуйте власну комп’ютерну та інтернет-обізнаність.
- Станьте для своєї дитини другом і порадником, опануйте інтернет разом.
- Оберіть найбільш прийнятний спосіб технічного захисту: від регулярно поновлюваного антивірусу до спеціального програмного забезпечення, що забезпечує батьківський контроль на комп’ютері та мобільному телефоні дитини.
- Створіть територію безпечного інтернету. Запропонуйте дітям пізнавальні, цікаві та захоплюючі інтернет-ресурси

Сімейна онлайн-безпека – відповідальність кожного

Навчіть дитину правилам безпечної роботи у Мережі:

1. *Роз’ясніть дитині важливість захисту своєї та чужої конфіденційної інформації:*

- не можна викладати в інтернет інформацію про сім’ю та її фінансові справи, адреси проживання та навчання, номери телефонів, кредитної картки та банківські дані;
- нікому, крім батьків, не можна називати власні паролі до інтернет-сервісів (навіть найкращім друзям).

2. *Навчіть дітей поводитися в інтернеті так само, як у реальному житті.*

У всесвітній Мережі дитина має поводитися ввічливо, не робити нічого, що може образити інших людей або суперечить закону. Поясніть дітям, що в інтернеті також слід із повагою ставитися до людей та їх авторських прав. Незаконне копіювання та розповсюдження матеріалів, що є чиєюсь власністю, вважається крадіжкою.

3. *Віртуальний співрозмовник може видавати себе за іншого.*

Навчіть дитину не надто довіряти незнайомим людям у Мережі. Дитина повинна знати, що не можна призначати зустріч з віртуальними знайомими без

дозволу батьків.

4. *Віртуальний світ іноді коштує реальних грошей.*

Завжди потрібно з'ясовувати, скільки коштують спеціальні інтернет-сервіси: наприклад, якою є повна вартість SMS в онлайн-грі. Якщо така інформація не очевидна для дитини, вона має звертатися за порадою до Вас. Допомагайте дітям розібратися, скільки насправді коштують такі SMS-послуги та чи дійсно необхідно їх надсилати.

5. *Звертатися за порадою – необхідно.*

Повідомте дитині, що вона може звернутися до Вас у будь-якій ситуації. Якщо в інтернеті (повідомленні електронної пошти, на сайті, форумі, чаті) щось не зрозуміло, хвилює або загрожує, дитина завжди має звертатися по допомогу до Вас. Інформація та послуги в інтернеті не завжди безпечні, тому перш ніж завантажувати, копіювати чи встановлювати будь-що з інтернету, дитина має отримати Ваш дозвіл. Навчіть перевіряти інформацію з Мережі за допомогою додаткових запитів і звернення до перевірених джерел.

ДОБІРКА МАТЕРІАЛІВ ДО ДНЯ БЕЗПЕЧНОГО ІНТЕРНЕТУ

1. Відеоролик «Я – за безпечний Інтернет!» (http://www.youtube.com/watch?v=hjo8lOi8VNE&feature=related)
2. Відеоролик «Фільм про правила безпеки в Інтернеті» (http://www.youtube.com/watch?v=TIyyrGAxdZk&feature=related)
3. Відеоролик «Остерігайся шахрайства в Інтернеті» (http://www.youtube.com/watch?v=AMCsvZXCd9w&feature=related)
4. Відеоролик «Як виявити брехню і залишатись правдивим в Інтернеті?» (http://www.youtube.com/watch?v=5YhdS7rrxt8&feature=relmfu).
5. Інтернет-етикет. Відеоролик «Розваги і безпека в Інтернеті». (http://www.youtube.com/watch?v=3Ap1rKr0RCE&feature=relmfu).
6. Соціальний ролик "Безпечний Інтернет - дітям" (https://www.youtube.com/watch?v=789j0eDglZQ#t=43)
7. Правила Інтернет-безпеки для батьків (https://www.youtube.com/watch?v=eg3aM5pdT_8)
8. Правила Інтернет-безпеки для дому (https://www.youtube.com/watch?v=MfTGJJmDP50)
9. Основні правила безпечного Інтернету (https://www.youtube.com/watch?v=cn3YVBOP03Q)
10. Безпека в Інтернеті (https://www.youtube.com/watch?v=l5RUBiw-IIY)
11. Сайт "Ліга безпечного інтернету" (http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=639)
12. Ресурс від Google (http://www.google.ru/safetycenter/families/start/)
13. Мультфільм із серії Почемучка "Як поводитись у соціальних мережах" (https://www.youtube.com/watch?v=yZIdEW7dmTY)

ДОДАТОК 1. Анкета «Рівень поведінки в Інтернеті»

1.А. Коли мені смутно або самотньо, я звичайно виходжу в Інтернет.

1.Б. Я не почуваю необхідності вийти в Інтернет тоді, коли в мене поганий настрій.

2.А. Коли я проводжу в Інтернеті менше часу, чим звичайно, я почуваю себе подавлено.

2.Б. Мій емоційний стан не залежить від того, скільки часу я проводжу в Інтернеті.

3.А. Я почуваю, що моє захоплення Інтернетом заважає моєму навчанню, роботі або відносинам з людьми поза Інтернетом.

3.Б. Використання Інтернету не заважає моїм відносинам з людьми, навчанню або роботі.

4.А. Багато моїх знайомих не знають, скільки часу я насправді проводжу в Інтернеті.

4.Б. Більшість моїх знайомих знає, скільки часу я проводжу в Інтернеті.

5.А. Я часто намагаюся зменшити кількість часу, що я проводжу в Інтернеті.

5.Б. Я не намагаюся зменшити кількість часу, що я проводжу в Інтернеті.

6.А. Коли я не в Інтернеті, я часто думаю про те, що там відбувається.

6.Б. Коли я не в Інтернеті, я рідко думаю про нього.

7.А. Я волію спілкуватися з людьми або шукати інформацію через Інтернет, а не в реальному житті.

7.Б. Я далеко не завжди вдаюся до допомоги Інтернету, коли мені потрібно знайти інформацію або поспілкуватися.

Ключі.

Вибір варіанта "А" оцінюється в 1 бал, вибір варіанта "Б" - 0 балів.

Від 0 до 3 балів - не зловживаєте Інтернетом.

Від 3 до 5 балів - звичайний користувач, але інколи забагато часу проводити в Інтернеті.

Від 6 і вище Ви занадто багато часу проводити в Інтернеті. Озирніться навколо - на світі є стільки цікавого, поспілкуйтесь з друзями.

ДОДАТОК 2. Анкета «Нетикет - кодекс поведінки в Інтернеті»

1. Щоб сісти за комп’ютер треба

   _____.

2. Тримай свій пароль в

   _____.

3. Не можна відкривати повідомлення від

   _____.

4. Про проблеми повідомляй

   _____.

5. В Інтернеті ніколи не повідомляй

   _____.

6. Розміщувати в Інтернеті чужі малюнки без дозволу

   _____.

7. З батьками обговорюй, які веб-сайти

   _____.

8. За цілий день біля комп’ютера можна знаходитись

   _____.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Бартків А.Б. та ін. Мережа Інтернет: сьогодні і вчора. -К.: Вища школа, 1996.
2. Гуржій, А.М. Інформатика та Інформаційні Технології. - Х.: Компанія СМІТ, 2003. - 352 с.
3. Щербатенко Т. Як не заблукати в Інтернеті. – Л.: Видавництво Старого Лева, 2013. – 104 с.
4. Гаєвський О.Ю. Інформатика: 7-11 кл. Навч. посіб. - К.: Видавництво А.С.К., 2003. – 512с.
5. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: Монографія. - Запоріжжя: ГУ "ЗІДМУ", 2003 - 250 с.
6. Кавун С. В. Інформаційна безпека. - Харків : Вид. ХНЕУ, 2009. - 368 с.
7. Вишняков В. М. Захист даних в інформаційних системах. - К.: КНУБА, 2010. - 128 с.
8. Ковальчук В. Н. Система інформаційної безпеки навчального комп'ютерного комплексу. - Житомир: Вид-во ЖДУ ім. І. Франка, 2009. - 84 с.
9. http://frichx.pp.ua/2011/08/24/shahrajstvo-v-interneti/
10. http://www.onlandia.org.ua/
11. http://online-bezpeka.kyivstar.ua/
12. http://bezpeka.kyivstar.ua/materials/articles/