Заняття з елементами тренінгу

**«Безпечний Інтернет» або**

**«Я вмію безпечно користуватися Інтернетом»**

**Мета:** ознайомити учнів з позитивним та негативним впливом Інтернету на людину; розвивати навички роботи в групах, вміння висловлювати свою точку зору логічно і конкретно; сприяти формуванню в учнів поняття про принципи безпечної поведінки в мережі Інтернет.

**Завдання:**

- визначити основні небезпеки, які можуть спіткати дітей у мережі Інтернет;

- сприяти формуванню навички адекватного реагування на небезпеки мережі;

- розвивати культуру поведінки в Інтернеті.

**Вікова категорія:** учні 7-11 класів

**Хід заняття**

**1.Привітання, активізація уваги, налаштування на роботу.**

**Вправа «Палець вверх».**

***Мета:*** визначити думки учасників відповідно актуального питання та викликати группу на дискусію, продемонструвати різні думки з приводу одного і того ж тверження.

***Метод:*** індивідуальна робота, обговорення.

Тренер читає твердження, яке потребує обговорення групи. Учасники стають у коло і слухають запропоноване твердження, аналізуючи чи згодні вони підтримати його чи ні. Варто наголосити, що тут не має правильних чи неправильних відповідей і цілком нормально не погоджуватись з думкою оточуючих. Коли тренер читає тверження учасники **закривають очі** і роблять свій вибір (якщо вони погоджуються з твердженням віднімають великий палець вгору, якщо ні – вниз як це показано на рис.1.) Після того, як всі зроблять вибір тренер просить групу відкрити очі і обговорити власні позиції щодо твердження.



Рис.1. Жести, які демонструють згоду або не згоду з твердженням.

**Питання для групи:**

1. Я люблю спорт.

2. Я люблю проводити свій вільний час у соціальних мережах.

3. У соціальних мережах часто вникають конфлікти.

4. У мене був неприємний випадок пов'язаний з Інтернетом.

5. Інтернет – це вільний простір, у якому можна робити все, що забажаєш.

6. Інтернет шкодить фізичному та психічному здоров’ю.

7. Я завжди розповідаю дорослим про конфлікти, які виникають зі мною в Інтернеті.

Відповідно до того, що озвучила група відбувається обговорення різних точок зору. ***Порада тренерові:***

Слідкуйте, щоб учасники закривали очі під час того, як роблять власний вибір. Це допоможе учасникам брати відповідальність за свої дій. Хваліть учасників за те, що вони висловлюють власну думку, це допоможе мотивувати учасників та сформувати простір безпеки.

**2. Знайомство. Вправа «Моє ім’я та нікнейм»**

***Мета:*** знайомство учасників, налаштування на позитивну взаємодію у групі, виявлення рівня активності у користуванні Інтернет-ресурсами.

***Хід проведення***

Учасникам пропонується по черзі назвати своє справжнє ім'я та ім'я (нік), яким би вони хотіли користуються на сьогоднішньому занятті й продовжити речення «Для мене Інтернет –це…»

***Обговорення:***

Чи в багатьох відрізняється справжнє ім'я від імені? Чи пов’язані між собою ці два імені? Як?

Чому користувачі вигадують собі імена для взаємодії в Інтернеті? Від чого вони себе убезпечують? А на які ризики можуть наразитися?

**3. Повідомлення мети та теми. Правила.**

**Вправа «Перепустка»**

***Ресурси:*** слова для складання правил роботи, роздруковані на кольорових аркушах і розрізані (кількість правил співпадає з кількістю груп).

Усі учасники заходять в аудиторію. При вході їм роздають «перепустки» - різнокольорові аркуші, на яких написані певні слова. Завдання – створити групу за кольором і зібрати всі правила.

**Приклади правил:**

1. Говорить один - всі слухають.

2. Доброзичливість

3. Поважати один одного

4. Говорити по черзі

5. Не критикувати

**Після озвучування правил, які склали учасники, ведучий повідомляє тему мету заняття.**

Сьогодні Інтернет – це невід’ємна частина нашого життя. Але не всі користувачі, особливо діти, знають всі ризики і небезпеки, які їх чатують в мережі Інтернет. Тому сьогодні ми розглянемо найнебезпечніші підводні камені Інтернету, на які може наразитись кожен з нас. Особливо серед підлітків, які проводять майже весь свій вільний час у віртуальному світі, нехтуючи навчанням, друзями, здоров’ям та навіть рідними людьми. 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: наскільки потрібен він в нашому житті та які плюси та мінуси має, а також отримаємо знання про безпечне користування Інтернетом.

**4. Очікування з нікнеймами «Наш чат»**

Учасники по черзі розповідають починаючи з фрази**: «Від сьогоднішнього тренінгу я очікую…»**

**5. Вправа «Калейдоскоп запитань»**

Ведучий задає питання:

- Назвіть для чого люди використовують Інтернет;

- Для чого Інтернет використовують ваші однолітки?

- Які соціальні мережі ви знаєте?

- Чи спілкуєтесь ви з незнайомцями?

- Чи був у вас якийсь неприємний випадок в школі чи який відбувся особисто з вами, пов'язаний з Інтернетом?

***Обговорення:***

Які висновки можемо зробити, прослухавши відповіді групи?

**6. Вправа «Побажання Інкогніто»**

Всім учасникам роздаються стікери (папірці, що наклеюються) на яких вони мають написати побажання **не підписуючись**і приклеїти їх на стікери із ніками учасників (вправа очікування№4). Після того як всі виконають завдання, учасникам пропонується вгадати хто написав їм побажання. Зазвичай це важко зробити, тоді тренер говорить, що так само важко розпізнати з ким спілкуєшся в Інтернет, адже ми не знаємо хто по ту сторону екрану, тому треба бути обережними і не давати конфіденційної інформації/фото іншим людям в мережі, коли не впевнені хто це.

***Питання:***

Чи знаєте ви, від кого вони прийшли?

Чи завжди вам можуть прислати щось приємне в правдиве?

**Висновок: Як тут, так і в Інтернеті, хто реально надіслав вам повідомлення ви точно не знаєте, і це може бути людина під чужим ім’ям.**

**7. Вправа «Небезпека в Інтернеті!»**

Учнів об’єднати у дві групи. Перша команда записує негативні сторони Інтернету, друга – позитивні. Потім кожна команда представляє свою роботу.

*Питання:*

Чого більше нам приносить Інтернет: позитиву чи негативу?

Від чого залежить наша безпека в чаті?

**8.Вправа «Вчимося безпечній поведінці»**

Тренер пропонує групам (на цьому етапі склад груп можна змінити) ознайомитися з інформаційними аркушами, у яких містяться матеріали:

- про шкідливі сайти, які закликають до тероризму, екстремізму тощо;

- про комерційні сайти, розраховані на недостатньо розвинене критичне сприйняття інформації користувачами;

- про небезпеки розміщення особистої інформації, фотографій, відео;

- про небезпеки особистих контактів з незнайомими людьми.

Завдання груп – ознайомитися з матеріалами, обговорити їх і зробити свої висновки, які і представити на загал.

*Інформаційний аркуш №1*

Пропонуємо вам матеріал про те, як **захистити свої особисті дані**.

Особливо зверніть увагу на ваші дії у випадку **фішинг-атаки**.

Зробіть відповідні висновки (письмово) і представте їх на обговорення групи.

*Ознаки фішинг-атак і шахрайських повідомлень електронної пошти*

*Фішинг* – один з видів шахрайства, спрямований на викрадення цінних особистих даних користувача, таких як номери кредитних карток, паролі, дані про банківські рахунки і т.д.

Шахраї можуть розсилати безліч повідомлень, які відправлені ніби надійними веб-вузлами (наприклад, від банку) і містять запит особистих даних.

Шахраї постійно вдосконалюють свої фішинг-повідомлення і вспливаючі вікна. Вони часто використовують офіційні емблеми реальних організацій та інші дані, отриманні зі справжніх веб-вузлів. Як розпізнати шахрайське повідомлення електронної пошти?

Наводимо кілька прикладів фраз, що часто використовуються при проведенні фішинг-атак:

*«Підтвердіть свій обліковий запис»*. Представники компаній не повинні робити запит по електронній пошті про паролі, імена користувачів, номери соціального страхування та іншу особисту інформацію. Отримав повідомлення від корпорації Microsoft з проханням оновити інформацію про кредитну картку, не відповідайте – це шахрайське повідомлення;

*«Якщо ви не дасте відповідь протягом 48 годин, ваш обліковий запис буде заблокований»*. Такі повідомлення викликають відчуття терміновості, щоб змусити людину відповісти не роздумуючи;

*«Клацніть на посилання, наведене нижче, щоб отримати доступ до свого облікового запису»*. Посилання, за якими просять перейти, можуть бути повністю або частково містити реальне ім'я компанії або бути повністю замаскованими. Вони ведуть на інший веб-вузол (як правило, шахрайський).

Фішинг-повідомлення зазвичай розсилаються масово і не містять ані імені, ані прізвища отримувача.

*Дії у випадку фішинг-атаки*

1. Повідомте компанію, чиє ім'я було використано. Для цього створіть нове повідомлення у вашій поштовій скриньці, вкладіть у нього шахрайське повідомлення і відправте на адреси відповідних організацій.

2. Терміново змініть паролі для всіх облікових записів, якими ви користуєтесь у мережі.

3. Регулярно перевіряйте стан своїх рахунків.

4. Встановіть на свій комп’ютер антивірусні та антишпіонські програми, постійно їх оновлюйте.

*Інформаційний аркуш №2*

Пропонуємо вам матеріал про те, як **безпечно спілкуватися в мережі.**

Зробіть відповідні висновки (письмово) і представте їх на обговорення групи.

*Соціальні мережі*

Соціальні мережі сприяють вашій творчості, дозволяють постійно контактувати з друзями, надають багато можливостей – обмінюватися і переглядати відео, фото, слухати музику. І все це в одному місці. Але як уникнути небезпек і отримати користь і задоволення від відвідування соціальних мереж?

Дехто дуже любить дивитися фільми і відеоролики, використовуючи, наприклад, YouTube, переглядаючи своє улюблене відео та спілкуються з тими, кому це теж подобається. Але пам’ятайте, що на подібних сайтах немає обмежувальної класифікації за віком (як у кінотеатрах) й інколи можна знайти фільм, що не підходить вам за віком. Якщо фільм тривожить вас, викликає почуття страху, роздратування, відчаю, сорому – не потрібно його дивитись. Можна поділитися своєю думкою з дорослими, які можуть звернутися зі скаргою до адміністрації сайту.

*Зображення*

Фотографії і фільми – важлива частина мережевого простору. Завжди гарно подумайте, перш ніж завантажити свої фотографії чи відео. Зображення залишаються на сайтах надовго (інколи навіть після того, як ви їх видалили). Вони можуть бути скопійовані, відредаговані і використані де завгодно. Подумайте, чи хочете ви цього. Пам’ятайте, коли ви викладаєте щось у мережі, це стає доступним мільйонам людей в світі. Про що ви маєте подумати у першу чергу, коли оновлюєте свої сторінки у соціальних мережах? Про власну безпеку. Захистіть сторінки налаштуваннями приватності – так ви зможете контролювати тих, хто має доступ до вашої інформації.

*Персональний профіль*

Це джерело інформації про вас. Додавання деталей – цікавий і веселий процес, але краще утриматися від додавання деякої інформації. Дату народження, адресу, номер мобільного краще не публікувати.

Мільйони людей в усьому світі спілкуються у соціальних мережах. Переконайтесь, що ніхто не має доступу до персональних налаштувань ваших сторінок і сайтів.

І ще декілька порад:

- частіше перевіряйте персональні налаштування ваших сторінок, щоб захистити себе від небажаних контактів;

- попросіть друзів і членів родини повідомити вам, якщо вони помітили, що ви розмістили надто багато особистої інформації або неналежні фото, відео. Зі сторони це може бути більш помітно. Зберігайте паролі у таємниці;

- поважайте себе та інших у мережі;

- якщо відбулась якась неприємна ситуація, повідомте про це дорослих.

Пам’ятайте, що кіберзапугування і погрози з мережі неприпустимі! На це обов’язкового необхідно реагувати:

- повідомити адміністраторам сайту;

- зберегти повідомлення-погрозу як доказ;

- обов’язково поставити до відома дорослих.

*Спілкування он-лайн*

Розмови з друзями завжди дозволять вам дізнатися останні новини. Електронна пошта, Skype, Qip – що вам більше до вподоби?

Ваше ім'я в сервісах для он-лайн спілкування має легко запам’ятовуватися, але це не повинно бути вашим реальним, повним іменем.

*Повідомлення*

Ви колись отримували від друзів неочікувані файли невідомого вам змісту? Двічі подумайте, перш ніж відкрити їх, вони можуть містити віруси. Якщо не впевнені, краще перепитайте друга про них по телефону або особисто.

У своїй електронній скриньці відкривайте лише повідомлення від тих людей, яких ви знаєте і яким довіряєте. Не забувайте прочитувати тему повідомлення. Якщо тема викликає підозри і не схожа на те, про що ви могли б поговорити з друзями, **не** **відкривайте** ніякі вкладення. Це можуть бути віруси.

*Chain mails* – повідомлення-ланцюжки, у яких просять переслати їх десятьом друзям, а інакше відбудеться щось неприємне, жахливе. Домовтесь з друзями не пересилати подібний спам. Якщо в таких повідомленнях міститься реальна загроза, поговоріть з дорослими.

*Чати*

Вони відкриті для всіх, ви можете говорити з кожним. Якщо ви спілкуєтесь в чатах, переконайтесь, що в них є модератори – люди, які слідкують за змістом спілкування. Будьте обережними і не повідомляйте особисту інформацію. Уникайте безпосередніх контактів з невідомими партнерами по спілкуванню. Якщо ви домовились з кимось про реальну зустріч, обов’язково повідомте про це дорослих.

Пам’ятайте: щоб ви не використовували для спілкування – мобільний телефон, комп’ютер тощо – правила безпеки завжди однакові.

*Інформаційний аркуш №3*

Пропонуємо вам матеріал про те, як **безпечно спілкуватися за допомогою мобільного телефону, як не потрапити на вудку реклами і що робити зі спамом.**

Зробіть відповідні висновки (письмово) і представте їх на обговорення групи.

*Мобільне спілкування*

*Premium Rate Numbers – платні номери*

Що це таке? Це можливість витрати багато грошей, навіть не усвідомлюючи цього. Пропонуються різні послуги, придбання цікавих речей, акції і для цього вам потрібно подзвонити на певний номер або надіслати повідомлення. Всі дзвінки і повідомлення можуть бути дуже дорогими. Якщо ви хочете здійснити покупку онлайн, завжди уважно читайте всю надану інформацію, особливо написану дрібним шрифтом. Якщо у вас виникли труднощі із цим питанням, попросіть батьків зв’язатися з цим сайтом.

*IMEI номер*

Персональний ідентифікаційний код телефону (англ. International Mobile Equipment Identity), який встановлюється на заводі при виготовленні, слугує для ідентифікації пристрою в мережі. Зберігається у прошивці апарату, як правило, написаний на упаковці, в гарантійному талоні, а також під батареєю мобільного телефону. Відіграє роль серійного номеру апарату. Передається в ефір при авторизації у мережі. IMEI номер використовується для відстеження апаратів, для їх блокування на рівні оператора мобільного зв’язку при крадіжці.

Запишіть цей номер і зберігайте у надійному місці.

*Погрози*

Якщо ви стали отримувати неприємні чи грубі повідомлення з невідомих номерів, пам’ятайте – на них *не потрібно відповідати*, але необхідно зберегти у якості доказів. Якщо вас таким чином турбують, зверніться до дорослих, ким довіряєте, в школу або до мобільного оператора.

Декілька порад:

- завжди замислюйтесь, кому ви повідомляєте свій мобільний номер – ви не знаєте, чим це може закінчитися;

- будьте пильними, не розмовляйте голосно у публічних місцях, а також не слухайте голосно музику;

- будьте обережні з тим, що завантажуєте у свій телефон – кількість вірусів постійно зростає;

- якщо ви отримуєте смс-спам з різних номерів, повідомте про це вашого оператора.

*Реклама*

Деякі сайти містять багато реклами, яка привертає увагу, відволікаючи від мети, з якою ви зайшли в Інтернет. Якщо у вас весь час з’являються вспливаючі вікна, ви можете позбутися них, клацнувши мишкою «закрити», або натиснувши комбінацію клавіш Alt F4.

*Зауважте:*

- коли вас зацікавив якійсь рекламований продукт і ви вводите свої дані, щоб придбати його або дізнатися більше, завжди читайте інформацію про політику конфіденційності, щоб знати, куди інформація уходить від вас;

- не вірте всьому підряд. Якщо інформація (або рекламна пропозиція) надто приваблива – це може бути пастка шахраїв;

- поговоріть зі своєю родиною і заведіть окрему сімейну електронну скриньку для онлайн покупок і онлайн підписки. Залиште свою особисту скриньку для листування з друзями;

- інколи важко відрізнити рекламу від просто якогось розважального контенту. Читайте посилання уважно і перевірте безпеку свого комп’ютера і персональних даних, якщо ви помилково не туди натиснули.

Скористайтесь нижченаведеними порадами, щоб уникнути небажаного спаму, реклами у своїй поштовій скриньці та убезпечити себе при користуванні Інтернет-ресурсами для спілкування:

- ставтесь з повагою до свого Інтернет-простору – дозволяйте тільки друзям і близьким людям спілкуватися з вами. Якщо ви не зустрічали когось у реальному житті, намагайтесь уникати таких контактів;

- використовуйте нікнейм, а не своє справжнє ім'я. Нікнейм має бути таким, щоб не привертати небажаної уваги;

- завжди звертайте увагу на особисті налаштування тих сайтів, де ви публікуєте особисту інформацію. Переконайтесь, що ви особисто знаєте тих, хто бачить і може скопіювати дану інформацію;

- спостерігайте за поведінкою своїх друзів у мережі і робіть щось (поговоріть з ними, зверніться до дорослих), якщо вважаєте, що вони потрапили у ризиковану ситуацію;

- видаляйте листи-ланцюги (наприклад, «перешли це 10 друзям…»), не читаючи їх.

*Інформаційний аркуш №4*

Пропонуємо вам матеріал про те, як **безпечно слухати і завантажувати музику та як уникнути небезпеки, граючи в онлайн ігри.**

Зробіть відповідні висновки (письмово) і представте їх на обговорення групи.

*Музика*

Музика – одна з ваших найулюбленіших розваг у вільний час. Не забудьте про правила безпеки, коли ви працюєте з музичними файлами в Інтернеті:

- завжди читайте інформацію, написану в оголошенням дрібним шрифтом, перш ніж програти чи завантажити якусь мелодію чи ринг тон;

- перш ніж завантажити пісню, прочитайте відгуки інших користувачів;

- якщо ви використовуєте якісь програми обміну файлами, переконайтесь, що вони встановлені вірно і не дозволяють стороннім особам отримувати доступ до всіх файлів вашого комп’ютера;

- поважайте авторське право. Якщо автор пісні не виклав її на своєму офіційному сайті для вільного завантажування, ви можете опинитися у категорії порушників авторських прав.

*Ігри*

Ігри бувають найрізноманітнішими – від коротких і простих, до складних, у яких беруть участь багато гравців. Усі вони дуже різні, але якою б гра не була і на чому б ви не грали (комп’ютер, телефон, ігрова консоль), правила безпеки залишаються однаковими:

- треба створити сімейну електронну адресу для реєстрації у грі;  
- вивчіть спеціальну мову ігор;

- якщо у процесі гри хтось почне використовувати нецензурні вирази у вашу адресу, ви можете зробити скріншот і надіслати скаргу адміністрації сайту, використавши скріншот як доказ;

- не забувайте про мережевий етикет. Флеймінг і тролінг – приклади безвідповідальної поведінки і не варто витрачати свій час на таких користувачів. Завжди будьте ввічливими у спілкуванні;

- переконайся, що при реєстрації у грі ти не видав особистої інформації.

І ще кілька корисних порад:

- вивчіть рейтинг гри, переконайтесь, що вона підходить вашому віку;

- прочитайте терміни гри й умови використання даних сайтів, перевірте, чи є спеціальні функції безпеки для дітей;

- заповніть свій профіль гравця таким чином, щоб це дозволило вам знайти інших гравців вашого віку;

- нехай ваші батьки знають ваш псевдонім, як перевірити ваш онлайн акант на предмет безпеки, якщо раптом щось піде не так;

- встановіть часові обмеження для себе. Використайте, наприклад, будильник у мобільному телефоні, щоб слідкувати за часом.

**9. Узагальнення, висновок. Складання пам’ятки**

Учасники розробляють у підгрупах правила розумного користувача у мережі Інтернет, використовуючи опорні слова:

- пам’ятай про

- піклуйся про

- ніколи не

- завжди

- думай про

- зверни увагу на

- намагайся

- порадься з

- узнай про

- не забудь

- ні в якому разі не

- зроби

- відповідай за

Після представлення правил, учасники висловлюють свої враження від заняття, висновки, які для себе зробили.

**10.Очікування. Підведення підсумків: «Кастрюля. Кошик. Сміттєвий бак»**

**Мета:** визначити наскільки збулися очікування учасників від заняття.

**Метод:** індивідуальна робота.

На стікерах учасникам потрібно написати такі позиції:

 те, що потрібно переварити/переосмислити



те, що забирають з собою в життя.



те, що є непотрібним.

Ці стікери учасники наклеюють на відповідні малюнки, які у формати А-3 розвішені на стінах.

те, що потрібно переварити/переосмислити.

те, що забирають з собою в життя.

те, що є непотрібним.

**11. Прощання.Подаруй усмішку сусідові.**

