

ԱՊԱՀՈՎ ՀԱՄԱՑԱՆՑ

Հ. 154 հիմնական դպրոցի ծնողական ժողով

Ապահով համացանց 2014 (Slide 1)

Միասին ավելի ապահով և արդյունավետ օգտագործենք համացանցը: (Slide 2)

Ծնողական ժողովի նկարագրություն

1. Բարև ձեզ հարգելի ծնողներ, այսօրվա մեր ծնողական ժողովի նպատակն է ներկայացնել համացանցում առկա վտանգները և տրամադրել ձեզ դրանցից խուսափելու գործիքների մասին գիտելիքներ: (Slide 3)

2. ԱՊԱՀՈՎ ՀԱՄԱՑԱՆՑ ԾՐԱԳԻՐ

Ավելի քան 90 երկրներում փետրվարի 11-ը նշվում է որպես ապահով համացանցի օր: Երրորդ տարին անընդմեջ ապահով համացանցի օրվա առթիվ Orange-ը «Մեդիակրթության կենտրոն» և «Ինտերնետ Հանրություն» կազմակերպությունների հետ համատեղ նախաձեռնում է «Ապահով համացանց Հայաստան» լայնածավալ ծրագիրը: Մեր ծնողական ժողովը անցկացնում ենք այդ ծրագրի շրջանակներում: (Slide 4,5,6)

3. Նախ ցանկանում եմ ներկայացնել, թե ինչպես պետք է կազմակերպել երեխայի համակարգչային աշխատատեղը:

Ցուցադրել պաստառը, որտեղ ցուցադրված է համակարգչի մոտ նստելու ճիշտ կեցվածքը, սենյակի լուսավորությունը: (Slide 7)

Ցուցադրել 2-րդ պաստառը, որտեղ ներկայացված է համակարգչի մոտ նստելու տարիքային և ժամանակային սահմանափակումները: (Slide 8)

4. Համացանցը այսօր դարձել է մեր առօրյա կյանքի մի մասը: Այն օգտագործում ենք աշխատանքում, ուսման մեջ և զվարճանքի համար:

Այժմ ներկայացնեմ համացանցի հնարավորությունները.

5. Ինչ է համացանցը- այն տեղեկատվության հսկայական շտեմարան է, որից անհրաժեշտ է գրագետ օգտվել: (Slide 10)

Համացանցը միմյանց հետ կապակցված համակարգչային ցանցերի ամբողջություն է: (Slide 8)

6. Ինչ է համաշխարհային ուստայնը – դա փոխկապակցված փաստաթղթերի ամբողջություն է, որոնք կապված են գերհղումներով (Slide 11)

Համացանցի հնարավորությունները. (Slide 12)

1. Ինֆորմացիայի արագ փոխանցում և ստացում
2. Տեղեկությունների շտեմարաններ
3. Սիրելի ֆիլմերի, երգերի, տեսահոլովակների ներբեռնում
4. Շփում արտերկրում գտնվող բարեկամների և հարազատների հետ
5. Ցանցային ուսուցում և այլ...

Համացանցին մենք միանում ենք հատուկ ծրագրերի միջոցով, որոնք կոչվում են զննարկիչներ կամ բրաուզերներ: Ներկայում առավել շատ են օգտագործվում հետևյալ բրաուզերները. Google chrome, Internet Explorer, Opera, Mozilla Firefox.. (Slide 13)

7. Համացանցային վիճակագրություն (Slide 14)

Օգտվելով «ՀՀ-ում ինտերնետի թափանցումն ու կիրառումը» հետազոտությունից - http://isoc.am/publ/penetration_am.pdf, կարող ենք բերել հետևյալ վիճակագրական տվյալները.

Աշխարհի բնակչության մոտ 30 տոկոսը՝ ավելի քան 2.1 մլրդ մարդ միացել է համացանցին: Հայաստանի բնակչության արդեն կեսից ավելին մոտ՝ 1,7 մլն մարդ միացել է համացանցին՝ նրանցից 670 հազարը գրանցված է facebook.com, իսկ ավելի քան մեկ միլիոնը այլ սոցիալական ցանցերում:

ՄԱԿ-ի տվյալներով համացանցում մոտ 800 հազար մանկապիղծ կա:

8. Գրադարաններ(Slide 15)

Համացանցի ստեղծման հիմքում ընկած էր էլեկտրոնային գրադարանի մշակման գաղափարը՝ տեղեկատվությունը դյուրամատչելի դարձնելու և այն հեշտությամբ տարածելու նպատակով : Ներկայումս համացանցում առկա են 18 հազարից ավելի գրադարաններ, որոնք ներկայացված են <<http://www.libdex.com/>> կայքում:

Հարկավոր է տարբերել համացանցում ներկայացված գրադարանները թվային (էլեկտրոնային) գրադարաններից: Առցանց գրադարաններն ունեն պարզ կառուցվածքով վեբ էջ, որի միջոցով օգտվողները կարող են ստանալ հիմնական տեղեկություններ ծրագրերի, գործունեության, հավաքածուների և կոնտակտային տվյալների վերաբերյալ: Առցանց գրադարանները կարող են առաջարկել կատալոգներում թվարկված ֆիզիկական գրքերի վարձույթը, այդ գրքերը կարելի է նաև պատվիրել համացանցով: (Slide 16)

Թվային գրադարաններն (Slide 17) առաջարկում են գրքերից առցանց օգտվելու հնարավորություն: Գրքերը սովորաբար թվայնացված են կամ որպես վեբ էջ, կամ որպես պարզ տեքստային փաստաթուղթ. MS Word կամ Adobe PDF փաստաթղթեր, որոնք հնարավոր է ներբեռնել կայքերից:

9. Երաժշտությունն ու պատկերները համացանցում: (Slide 18)

Համացանցը, որպես մուլտիմեդիա միջավայր, առաջարկում է հաղորդակցման բազմապիսի եղանակներ՝ ներառյալ աուդիո ֆայլերի, տեսանյութերի և թվային լուսանկարների փոխանակում: Ժամանակակից կիրառական ծրագրերը զգալիորեն հեշտացրել են նման բովանդակության ստեղծումը և տարածումը՝ հաղթահարելով լեզվական, մշակութային և ազգային խոչընդոտները, ինչպես նաև վերհանելով ոչ միայն անձնական տվյալների այլ նաև հեղինակային իրավունքի խախտման և անօրինական բովանդակության վերաբերյալ կարևոր հարցեր:

10. Էլեկտրոնային փոստ: (Slide 19)

Էլեկտրոնային փոստը համացանցի միջոցով միմյանց միացված համակարգիչների միջև հաղորդագրությունների փոխանակման համակարգ է: Էլեկտրոնային նամակը սովորաբար վայրկյանների ընթացքում է հասնում հասցեատիրոջը, իսկ վերջինս որոշում է, թե երբ կարդա ու պատասխանի: Ճկուն և արդյունավետ այդ համակարգը էապես փոխել է մեր աշխատելու և հաղորդակցվելու եղանակը: Էլ-փոստով օրական միլիարդավոր հաղորդագրություններ են ուղարկվում:

Էլ. փոստի հասցեն բաղկացած է երկու մասից՝ տեղային և դոմեյնային, որոնք անջատվում @ նշանով:

11. Զրուցարաններ: (Slide 20)

Զրուցարանը ընդհանուր հասկացություն է, որը վերաբերում է քննարկումներին հատկացված կապուղում տեղի ունեցող ինտերակտիվ հաղորդակցությանը: Օգտվողները զրուցասենյակներում խոսում են մարդկանց խմբերի կամ էլ ընկերոջ հետ՝ օգտվելով ակնթարթային հաղորդակցման ծառայություններից: Ցանցում գործող զրուցարանային ծրագրերից շատերը, օրինակ՝ Skype, Yahoo Chat-ը, ICQ-ն և AOL Chat-ը առաջարկում են զանազան զրուցասենյակներ, որոնցում ներգրավված են անմիջական քննարկումների մասնակցող մարդկանց տարբեր խմբեր:

12. Բլոգեր: (Slide 21)

«Բլոգ» բառը weblog անգլերեն բառի կրճատ տարբերակն է: Այն խմբի կամ անհատի կողմից ստեղծվող և հրապարակվող ցանցային օրագիր է: Բլոգները որպես երևույթ համացանցում հայտնվել են վերջին ժամանակներս: Բլոգները սովորողներին հնարավորություն են տալիս

վերահսկել իրենց ուսուցման գործընթացը և ստեղծել հասարակական ֆորում՝ իրենց մտքերն ու զգացմունքները հրապարակելու համար:

13. Սոցիալական ցանցեր: (Slide 22)

Սոցիալական ցանցը վեբ համակարգի վրա հիմնված առցանց ծառայություն է, որն օգտվողներին առաջարկում է հաղորդակցման զանազան եղանակներ՝ զրուցասենյակների, հաղորդագությունների, էլեկտրոնային նամակների և ֆայլերի փոխանակման, տեսաձայնագրությունների և ձայնային զրուցարանի, բլոգավարման, քննարկումների խմբերի և այլ գործիքների միջոցով: Սոցիալական ցանցերը կառուցվում են անձնական էջերի, կամ նկարագրերի շուրջ, որոնք պարունակում են անձնական տվյալներ, տեղեկություններ հետաքրքրությունների, ընկերների ցանցի և այլնի վերաբերյալ: Սոցիալական ցանցերը միավորում են համանման հետաքրքրություններ ունեցող կամ միևնույն բնագավառը ներկայացնող մարդկանց համայնքները և նրանց, ով հետաքրքրված է այլ մարդկանց գործունեությամբ:

14. Վեբ-2(Slide 23)

Վեբ 2.0 –ի կայքերը օգտվողներին հնարավորություն են տալիս անել ավելին, քան պարզապես ստանալ տեղեկատվություն: Այստեղ կան հսկայական առավելություններ այն ավանդական կայքերի նկատմամբ, որոնք այցելուներին ընձեռում են միայն դրանք դիտելու հնարավորություն, և որոնց բովանդակությունը կարող է փոփոխվել միայն կայքի սեփականատերերի կողմից:

Վեբ 2.0-ի ամենակիրառելի չորս տեխնոլոգիաներն են՝ բլոգները, փոդքաստները, սոցիալական ցանցերը և վիքիները:

15. Շարժական (բջջային) տեխնոլոգիաներ (Slide 24)

Շարժական տեխնոլոգիայի և անհատական համակարգիչների ոլորտները գնալով նմանվում են իրար, քանի որ շատ բջջային հեռախոսներ ներկայումս ունեն համացանցային գննարկիչի և էլեկտրոնային փոստի հնարավորություններ. գնալով աճում է անլար կապով համակարգիչների թիվը, մի մասն էլ օգտագործում են արբանյակին կապ:

16. Որքան էլ մենք փորձում ենք խուսափել համացանցի վտանգներից, նրանք առկա են և դրանց ազդեցությունը կարող է վտանգել մեր երեխաների հոգեբանությանը ու սխալ աշխարհայացք ձևակերպել նրանց մոտ: Մանկավարժների և ծնողների դերը այդ հարցում շատ կարևոր է: (Slide 25)

Այժմ ներկայացնեն համացանցում առկա վտանգները. (Slide 26)

- Ցանցային խաբեբայություն: (Slide 27) Phishing-ը դա անհատին հնարքների միջոցով թյուրիմացության մեջ զցելն է, ստիպելով նրան կամավոր տրամադրել իր անձնական

տվյալները. Արդյունքում գողանում կամ կեղծում են անհատի տվյալները եւ ստանում մուտք նրա հաշվեհամարներին, էլեկտրոնային փոստին, PIN կոդերին եւ այլն:

Ուշադիր եղեք խարդախությունների նկատմամբ

- ✓ Որոշ նշանների միջոցով կարելի է տարբերակել նմանատիպ նամակները
- ✓ Մեծ շահման մասին հայտարարություններ
- ✓ Հայտնի ընկերությունների կողմից արված առաջարկություններ
- ✓ Առաջարկներ, որոնք շատ գրավիչ են ճշմարիտ լինելու համար
- ✓ Տառասխալներ կամ քերականական սխալներ նամակներում

Օգտագործեք Anti-Phishing և anti-spam տեխնոլոգիաներ նմանատիպ նամակներից խուսափելու համար

1. **Հեղինակային իրավունք : (Slide 28)** Առանց հեղինակային իրավունքի իրավատիրոջ կողմից լիցենզիա կամ թույլտվություն ստանալու հեղինակային իրավունքով պաշտպանված ծրագրաշարի չթույլատրված պատճենումը համարվում է ծրագրաշարի գողություն: Պատկերանշանը հեղինակային իրավունքով պաշտպանված նյութ է, որն օգտագործվում է հեղինակային իրավունքի իրավատիրոջ կողմից որպես նույնացման նշան: Առանց իրավատիրոջ թույլտվության պատկերանշանի պատճենումը կամ օգտագործումը անօրինական է:
2. **Դոմեյնի կեղծում : (Slide 29)** Pharming- ը դոմեյնի անվանվան կեղծում է, որի արդյունքում օգտվողներին ուղղորդում է կեղծ կայքը: Օգտվողները սկսում են իրականացնել գործառնություններ կեղծ կայքի միջոցով , ինչը ենթադրում է անձնական տվյալների մուտքագրում, ինչպես նաև հաշվեհամարների եւ վարկային քարտերի տվյալների մուտքագրում: Այս դեպքում կեղծ կայքի հեղինակները կարող են օգտագործել տվյալները սեփական նպատակների համար:
3. **Տվյալների գողություն: (Slide 30)** Ոչ վստահելի կոմերցիոն կայքերը կարող են չկատարել պայմանագրով ստանձնած իրենց պարտավորությունները, կարող են ոչ նպատակային օգտագործել ձեր անձնական տվյալները եւ ֆինանսական տեղեկությունները: Կոմերցիոն վեբ-կայքերը կարող են նաև երեխաներին առաջարկել ծառայություններ, որոնք ապօրինի են: Հաճախակի նման կայքերը ստեղծվում են այն երկրներում ուր չկան իրավական արգելող մեխանիզմներ:

Ինչպես տարբերակել նման կայքերը. իրական կյանքում ճանաչված եւ կայացած ընկերությունները վստահելի են նաև առ-ցանցում:

Ի՞նչ կապ ունի համացանցը հետապնդման կամ ոտնձգության հետ:

4. **Կիբեռհետապնդում (Slide 31)** Bullying (անգլ. **հետապնդում**, հալածանք, ահաբեկում, սպառնում) հասկացությունը կարող է տարբեր սահմանումներ ունենալ: Հետապնդումը կարող է ենթադրել խոսքային կամ ֆիզիկական շփում: Մեր օրերում կարող է լինել նաև համացանցով կամ բջջային հեռախոսով իրականացվող վիրտուալ հետապնդում, այդ թվում նվաստացուցիչ կամ չարամիտ բովանդակությամբ հաղորդագրություններ,

Էլեկտրոնային նամակներ, զրուցասենյակներում կամ հաղորդագրության հարթակներում արված մեկնաբանություններ և ծայրագույն դեպքում (որ էլ ավելի սարսափելի է), անհատին կամ անհատների որոշակի խմբի վնաս հասցնելու նպատակով ստեղծված կայքեր: Կիբեռհետապնդողները օգտագործում են նաև բջջային հեռախոսներ այլ մարդկանց անհարմար դրության մեջ լուսանկարելու կամ անարգի բովանդակությամբ sms- կամ mms- հաղորդագրություններ տարածելու նպատակով:

Կիբեռհետապնդումից և ոտնձգությունից պաշտպանվելու երեք ոսկե կանոնները. (Slide32)

- 1) հնարավորության դեպքում ստեղծել վիրավորական բովանդակությամբ նյութի կրկնօրինակը ,
- 2) անջատել համապատասխան սարքը (համակարգիչը կամ բջջային հեռախոսը),
- 3) կատարված միջադեպի մասին հայտնել վստահելի չափահասի:

5. Մասնավորություն (Slide 33)

Մասնավորությունը (մասնավոր կյանքի անձեռնմխելիությունը կամ անձնական տվյալների գաղտնիությունը) սեփական անձնական տեղեկությունների մատչելիության և օգտագործման վրա տարածվող վերահսկողության աստիճանն է:

17. Ներկայացնեմ ապօրինի, վնասակար եւ ոչ պատշաճ բովանդակության դեմ պայքարի միջոցները և գործիքները , մասնավորապես kaspersky գործիքները: (Slide 34)

Kaspersky -ն աշխարհում ամենահայտնի հակավիրուսային ծրագրերից մեկն է:

Kaspersky Internet Security համակարգը հնարավորություն է տալիս ոչ միայն օգտվել ապահով ինտերնետից այլ և ծնողական վերահսկողություն (parental control)գործառույթի շնորհիվ վերահսկել համակարգչի և ինտերնետի օգտագործումը Ձեր երեխաների կողմից,

- հնարավորություն է տալիս կարգավորել և արգելափակել երեխաների մուտքը ոչ ցանկալի բովանդակությամբ ինտերնետ կայքեր
- արգելափակում է առցանց գործողությունները
- վերահսկում և արգելափակում է համակարգչի օգտագործումը

Orange ընկերությունը հնարավորություն է տալիս մարտ և ապրիլ ամիսներին անվճար օգտվել Kaspersky ծառայություններից: Ծրագիրը կարող էք ներբեռնել այցելելով <http://orangearmenia.am/internet/services/kaspersky/>այնուհետև ուղարկել SMS 135 կարճ համարին Ձեր Ինտերնետ Հիմա հեռախոսահամարից: (Slide 35)

18. Քննարկումներ հետևալ հարցերի շուրջ (Slide 36-44)

1. Ո՞ր տարիքից կարելի է համացանց մտնել:

2. Կարող ենք արդյոք ունենալ անձնական էլեկտրոնային հասցեն, ստեղծել ընդներկամ գրանցվել սոցիալական ցանցերում
3. Ի՞նչ տնային կանոններ պետք է սահմանել համացանցի օգտագործման համար:
4. Որ տարիքից օգտագործել Ակնթարթային հաղորդակցման ծրագրերը:
5. Կարո՞ղ եք արդյոք մեծահասակները կարդալ երեխաների հաղորդագրությունները:
6. Արդյո՞ք վեբ-խցիկները հուսալի են:
7. Ինչ է համացանցային կախվածությունը:
8. Ի՞նչ պետք է իմանալ համակարգչային վիրուսների մասին:
9. Ի՞նչ պետք է անել, երբ անհանգստացնում են համացանցում:
10. Արդյո՞ք օգտակար են ֆիլտրող ծրագրերը:
11. Ինչու է վտանգավոր -պոռնոգրաֆիան –
12. Ինչ կարող են «սովորեցնել» դեպրեսիվ երիտասարդական հոսանքներ-
13. Ինչպես կարող է համացանցը «նպաստել» թմրամոլությանը:
14. Ինչ ազդեցություն ունեն սոցիալական ցանցերը և զրուցարանները դեռահասների հաղորդակցական հմտությունների զարգացման վրա

19. www.safe.am կայքի, “Ապահով համացանց” <http://www.safe.am/esafetykit/start.html> և [wildwebwoods](http://www.wildwebwoods.com) խաղերի ներկայացում (Slide 45)

20. բուկլետի (Slide 46) և ոսկե կանոնների մոդելի ներկայացում և այդ բուկլետների տրամադրում ծնողներին: [Ամփոփում - Համացանցի ապահով օգտագործման ընտանեկան կանոնների ներկայացում](http://www.orangearmenia.am/internet/safe-internet/) <http://www.orangearmenia.am/internet/safe-internet/>

ՈՍԿԵ ԿԱՆՈՆՆԵՐ ԾՆՈՂՆԵՐԻ ՀԱՄԱՐ (Slide 47-54)

21. Համոզվեք, որ ձեր համակարգիչը ապահովված է հրապատով (firewall) , ինչպես նաև հակավիրուսային ու հակալրտեսային ծրագրաշարով: Թարմացրեք այդ ծրագրերը եւ հետեւեք դրանցից եկող ազդանշաններին: Ստուգեք, արդյո՞ք ձեր ինտերնետային ծառայության մատուցողը առաջարկում է հակավիրուսային եւ հակալրտեսային գործիքներ, որ կարող եք օգտագործել:

- ✚ Ծագագործեր փոստաղբային գտիչ (ֆիլտր) եւ հնարավորինս գաղտնի պահեք ձեր էլեկտրոնային հասցեն՝ այն վերում չհրապարակելով: Խուսափեք անձանոթների կողմից ուղարկված էլեկտրոնային նամակներից եւ անպայման զննեք այն, եթե այնուամենայնիվ որոշել եք բացել:
- ✚ Օպերացիոն համակարգի, համացանցային զննարկիչի, որոնման համակարգի եւ էլեկտրոնային փոստ ծրագրերի համար առավելագույնի հասցրեք ծնողական վերահսկողության կարգավորումները: Երեխաների համար ստեղծեք օգտվողի անհատական գրանցումներ: Համոզվեք, որ գաղտնիության կարգավորումները ամենաբարձր աստիճանի վրա են (այցելեք ձեր զննարկիչի „options/ընտրանք„ հրահանգացանկը):
- ✚ Օգտագործեք լրացուցիչ ֆիլտրող ծրագրաշար:
- ✚ Կապվեք մասնագետի հետ, երբ ձեր համակարգիչը սկսում է վատ աշխատել. այն կարող է վարակված լինել: Ինտերնետային ծառայության մատուցողը նույնպես պետք է կարողանա խորհրդատվություն տրամադրել:
- ✚ Համացանցում անցանկալի բովանդակության հանդիպելիս, զեկուցեք ազգային համացանցային թեժ գծին (տես Օգտակար հղումներ):
- ✚ Հնարավորության դեպքում նստեք երեխաների կողքին, երբ նրանք նավարկում են համացանցում: Դա լավագույն ձևն է քննարկելու եւ վստահություն նվաճելու համար: Միասին սովորելը դարձրեք ձեր նպատակը:
- ✚ Հիշեք, որ անվտանգության կանոնները ձեր ու ձեր երեխաների համար են: Քաջալերեք նրանց ասել այն ամենի մասին, ինչն իրենց տարօրինակ է թվում: