Կիբեռանվտանգության կանոններ ծնողների եւ ուսուցիչների համար

Նախագծի հեղինակ՝
Անահիտ Պարզյան
YES Armenia ծրագրի
փորձագետ

YOUNG EXPERTS SCHEME
ARMENIA

This project is funded
by the European Union

Կիբեռհիգիենայի եւ առցանց անձնական տվյալների պահպանման 10 կանոն

1. Համակարգիչները, հեռախոսներն ու պլանշետները մաքուր պահել

Յուրաքանչյուր գործիք իր մեջ պարունակում է ծրագրային թերացումներ, որոնք երեւան են գալիս ժամանակի ընթացքում : Այս թերացումներից օգտվում են հաքերները եւ նրանք հարձակումներ են իրականացնում՝ գողանալով անձնական տվյալներ, նկարներ եւ այլն: Այս ամենից խուսափելու համար ծրագրային սպասարկման մասնագետները պարբերաբար թարմացնող ծրագրեր են ուղարկում , որոնք անպայման պետք է ակտիվացնել, ադպիսով մաքրելով էլ. գործիքը նախկին թերացումներից: Եթե կա ավտոմատ թարմացման հնարավորություն՝ ակտիվացնել այն:

2. Մտածել՝ հանրային վայրերում համացանցին միանալուց առաջ

Համացանցին միանալուց առաջ, մասնավորապես հանրային վայրերում, պետք է ուշադիր լինել հավելվածի կողմից տրվող հարցերին: Հավելվածները հարցնում են թույլտվություն ստանալ մուտք դեպի նամակներ, հաղորդագրություններ, նկարներ, գեոլոկացիա եւ այլն: Պետք է քննադատորեն մոտենալ այս հարցերին եւ մտածել՝ արդյո՞ք պետք է կիսել այսպիսի տեղեկատվություն: Շատ դեպքերում ուղղակի կարելի է մերժել ու միանալ, իսկ եթե մերժել հնարավոր չէ, ուրեմն պետք է մտածել եւ որոշել՝ ապահովություն, թե՞ համացանց:

3. Ակտիվացնել հակավիրուսային ծրագրերը

Պետք է մշտապես ակտիվացնել ու մաքրել էլ. գործիքները վիրուսներից համապատասխան հակավիրուսային ծրագերի միջոցով: Ինչպես տան մաքրությունն է կարեւոր վիրուսային հիվանդություններից խուսափելու ու պաշտպանվելու համար, այդպես էլ էլ. գործիքներին է անհրաժեշտ հակավիրուսային ծրագրերով պարբերաբար թարմացնել:

4. Ուժեղ գաղտնաբառ կիրառել

Գաղտնաբառերը պետք է լինեն հեշտ հիշվող, բայց բարդ՝ կռահելու համար: Խրախուսելի է ներառել մեծատառեր, թվեր ու այլ նշաններ՝ գաղտնաբառն ավելի ամուր դարձնելու համար: Յուրաքանչյուր գործիքի ու հավելվածի համար լավ է ունենալ առանձին գաղտնաբառ, որպեսզի նույնսկ եթե մեկը հափշտակվել է՝ պահպանել մնացյալը: Գաղտնաբառը չի կարելի կիսել ոչ մեկի հետ, ոչ մեկի, նույնիսկ՝ մոտիկ ընկերուհու:

5. Միշտ «դուռը փակել»

Էլ. գործիքից օգտվելուց հետո պետք է դուրս գալ տվյալ հավելվածից, «կողպել» գործիքը գաղտնաբառով:

6. Ստուգել կայքէջերի հավաստիությունը

Կայքէջերը միշտ չէ, որ անվտանգ են ու հավաստի: Դա պարզելու համար պետք է նայել կայքէջերի հասցեներին: Եթե այն սկսվում է https կամ shttp-ով, ապա այն անվտանգ ու հավաստի կայքէջ է, իսկ եթե այն սկսվում է http-ով, ապա այն անվտանգ չէ:

7. Քննատադաբար մոտենալ համացանցի տեղեկատվությանը

Ամեն ինչ չէ, որ ճիշտ է գրված է համացանցում: Պետք է քննադատաբար մոտենալ այն նյութերին, որ հայտնվում են համացանցում: «Բժիշկները թաքցնում են.... Խմիր մեկ բաժակ ու միանգամից կնիհարես 30 կգ...», քիչ հավանական է, որ ճիշտ է, սակայն, երբ բացվում են այդ էջերը՝ հավանականություն կա, որ կարող են վարակել համակարգիչները: Եթե մի բան շատ պարզ է ու շատ լավը ճիշտ լինելու համար, հավանաբար սուտ է:

8. Յոթ անգամ մտածել, նոր ներբեռնել

Այն ինչ ներբեռնվում է համացանց, այն մնում է համացանցում, երբեք չի ջնջվում: Նույնիկս եթե օգտատերը ջնջում է իր ներբեռնած նյութը, միեւնույն է, այն մնում է համացանցում, կարող է պահպանվել այլ օգտատերերի մոտ ու տարածվել: Այսպիսով կարեւոր է մտածել ներբեռնելուց առաջ:

9. Կիրառել «Ծնողական վերահսկողություն» գործառույթը

Երեխաների գործիքների վրա կարելի է ակտիվացնել «Ծնողական վերահսկողություն» գործառույթը, որը կպաշտպանի երեխաներին անհամապատասխան նյութեր դիտելուց, կարդալուց կամ հանդիպելուց: Անհրաժեշտ է ապաակտիվացնել այն հավելվածները, որոնք կարող են երեխայի հոգեբանության վրա վատ ազդեցություն թողնել կամ առաջացնել կախվածություն: Երեխաների հետ պետք է սահմանել համացանցից օգտվելու կանոններ ու խստորեն պահպանել դրանք թե՛ տանը եւ թե՛ այլ վայրում:

10. Մտածել երեխաների անվտագության մասին

Երեխաների մասին տեղեկատվություն, նրանց դպրոցի հասցե, բնակության վայր, անձնագրի կամ այլ նկար, մասնավորապես, սոցիալական էջերում տեղադրելը խստորեն խախտում է երեխաների անձնական տվյալների պաշտպանության իրավունքը եւ սպառնում նրանց անվտանգությանը: Երեխաներին վերաբերվող նյութեր ներբեռնելիս պետք է մտածել այն լսարանի մասին, որը կտեսնի այդ նյութերը. այն կարող է շատ ավելի մեծ լինել, քան կցանկանայիք: Նման տեղեկատվության հրապարակայնացման համար խստորեն պետք է մոտենալ լսարանի ընտրությանը, սահմանել ու ձեւավորել փակ խմբեր, չնշել դպրոցի կամ տան հասցեն, որը կարող է ցույց տալ երեխայի մշտական տեղակայման վայրը: Պետք է մտածել երեխաների ապագայի հեղինակության մասին և խուսափել այնպիսի տեղեկատվության ու նկարների ներբեռնումից, որը հետագայում անհարմար վիճակի մեջ կարող է դնել երեխային, նույնիսկ եթե դա հիմա շատ զվարճալի է:

Կիբեռհետապնդումներ

Կիբեռտիրույթում քաղաքավարության կանոնները նույնն են, ինչ իրական կյանքում, սակայն ոչ բոլորն են հետեւում քաղաքավարության կանոններին: Պետք է խոսել եւ տեղեկացնել երեխաներին ու դեռահասներին, որ համացանցում նույնպես մարդիկ պատասխանատու են իրենց կատարած գործողությունների համար: Անհրաժեշտ է բացատրել, որ համացանցում նույնպես պետք է հետեւել քաղաքավարության կաննոններին, մասնավորապես՝

- ✓ **Լինել քաղաքավարի**
- ✓ **Լինել անկեղծ**
- ✓ **Չկոպտել, չվիրավորել, չծաղրել, չհետապնդել**
- ✓ **Վարվել այնպես, ինպես կցանկանային, որ իրենց հետ վարվեին**

Երեխաները պետք է վստահություն զգան եւ կիբեռհետապնդման դեպքում կատարեն հետեւյալ քայլերը

➢ **կիսվեն ծնողների եւ/կամ ուսուցիչների հետ,**
➢ **պահմանեն սպառնալիքները՝ հետագայում դրանք որպես իրեղեն ապացույց ներկայացնելու համար:**
➢ **ապակտիվացնեն ու փակեն տվյալ սպառանցող աղբյուրի հետ հաղորդակցման աղբյուրը**
➢ **Անհրաժեշտության դեպքում պետք է դիմել ոստիկանություն:**

Նույնիսկ գաղտնի կամ կեղծ սոցիալական էջերի օգտատերերին կարելի է հայտնաբերել IP հասցեների միջոցով:

Կիբեռհետապնդումը լուրջ հոգեբանական ճնշումների պատճառ կարող է դառնալ երեխաների ու դեռահասների համար: Նման իրավիճակի հայտնաբերման դեպքում անհրաժեշտ է միջոցներ ձեռնարկել անդառնալի հետեւանքներից խուսափելու համար:
Կիբեռհետապնդումը հանցագործություն է:

Դրական թվային հետք

Չնայած բոլոր մարտահրավերներին՝ համացանցը անսպառ գիտելիքի, տեղեկատվության, ինչպես նաեւ ժամանցի աղբյուր է երեխաների ու դեռահասների համար: Անհրաժեշտ է օգտվել այդ հնարավորությունից՝ պահպանելով «երթեւեկության կանոնները»:

Օգտվելով այդ անսպառ ռեսուրսից՝ երեխաներն ու դեռահասները մեծ հնարավորություններ ունեն ոչ միայն սպառելու այդ տեղեկատվությունը, այլ նաեւ ստեղծելու իրենցը ու համայն աշխարհի հետ կիսելու իրենց մտքերը:

Այս ամենն արդյունավետ դարձնելու համար պետք է՝

- ✓ **Օգնել ճիշտ ու անվտանգ օգտվել համացանցից՝ համատեղ սահմանելով անվտանգության կանոններ**

Համացանցը կարող է նաեւ բարի գործեր կատարելու հարթակ լինել

- ✓ **Երեխայի/դեռահասի հետ կարելի է մտածել եւ ուղղորդել նախագծերի կամ սոցիալական աշխատանքների ստեղծման ուղղությամբ, որոնք ներբեռնելով համացանց՝ կհամախմբեն/բարի գործ կկատարեն աշխարհին ավելի լավը դարձնելու համար:**

Այն ինչ երեխան/դեռահասը ներբեռնում է համացանց, կարող է նպաստել նրա հետագա կյանքի կայացմանը:

- ✓ **Պետք է սովորեցնել եւ ուղղորդել բարի եւ հանրության համար պիտանի նյութերով համացանցը «լցնելուն»:**