ԿԱՆԳՆԵՔ | ՄՏԱԾԵՔ | ՄԻԱՑԵՔ™

Մաքուր պահեք համակարգչային տեխնիկան

- **Արդիականացրեք անվտանգության ծրագրաշարը.** Վիրուսներից, վնասակար ծրագրերից և այլ առցանց սպառնալիքներից լավագույն պաշտպանությունը անվտանգության ծրագրաշարը, զննարկիչը և օպերացիոն համակարգը արդիականացնելն է:
- **Ավտոմատացրեք ծրագրաշարի թարմացումները.** Շատ համակարգչային ծրագրեր ավտոմատ են միանում և թարմացվում իմացյալ ռիսկերից պաշտպանվելու նպատակով: Միացրած պահեք ավտոմատ թարմացումները, եթե այդպիսի տարբերակ կա:
- **Պաշտպանեք բոլոր այն սարքերը, որոնք միանում են Համացանցին.** Համակարգիչներից բացի վիրուսներից և վնասակար ծրագրերից պաշտպանության կարիք ունեն նաև սմարթֆոնները, խաղ-համակարգերը և ցանցին միացող այ լսարքերը:
- **Միացրեք և զննեք.** USB կրիչները և այլ արտաքին սարքերը ևս կարող են վարակվել վիրուսներով և վնասակար ծրագրերով: Անվտանգության ծրագրերի միջոցով ստուգեք դրանք:

Պաշտպանեք անձնական բնույթի տեղեկությունները

- **Պաշտպանեք ձեր հաշիվները.** Հայցեք պաշտպանություն, որն ավելի ուժեղ է, քան գաղտնաբառերը: Հաշիվների տրամադրողների մեծ մասն այժմ առաջարկում են ինքնության ստուգման լրացուցիչ ուղիներ նախքան տվյալ կայքում որևէ գործունեություն ծավալելը.
- **Ընտրեք երկար և ուժեղ գաղտնաբառեր.** Օգտվեք մեծատառերի և փոքրատառերի, ինչպես նաև թվերի և խորհրդանիշերի համադրությունից՝ ստեղծելու ավելի անվտանգ գաղտնաբառեր:
- **Յուրահատուկ հասցե, յուրահատուկ գաղտնաբառ.** Յուրաքանչյուր հասցեի համար ունեցեք առանձին գաղտնաբառ, ինչը կօգնի ապակողմնորոշել կիբեռհանցագործներին:
- **Գրեք այն և ապահով տեղում պահեք.** Ցանկացած մեկը կարող է մոռանալ գաղտնաբառը: Կազմեք գաղտնաբառերի ցանկ և պահեք այն ապահով մի տեղ, ձեր համակարգչից հեռու:
- **Եղեք ձեր առցանց ներկայության տերը.** Կայքերում գաղտնիության և անվտանգության կարգավորումները դրեք այնպես, որ տեղեկություններ փոխանակելու տեսանկյունից դրանք հարմար լինեն ձեզ: Ճիշտ է սահմանափակելը, թե ում հետ և ինչպես եք տեղեկություններ փոխանակում:

Միացեք զգուշորեն

- **Եթե կասկածում եք, ջնջեք.** Էլեկտրոնային փոստով ստացված, Թվիթերում կամ այլուր տեղադրված հղումները, առցանց գովազդը հաճախ այն լավագույն միջոցներն են, որոնցով կիբեռհանցագործները վնասում են ձեր համակարգիչը: Եթե հղումը կասկածելի է թվում, նույնիսկ եթե գիտեք դրա աղբյուրը, ավելի լավ է ջնջեք այն, կամ նշեք որպես փոստաղբ:
- **Աչալուրջ եղեք Wi-Fi-ի կետերի հարցում.** Սահմանափակե՛ք ձեր գործունեության տեսակները և փոփոխեք ձեր համակարգչի անվտանգության կարգավորումները՝ սահմանափակելու դրա մատչելիությունն այլ անձանց համար:

  Պաշտպանե՛ք ձեր գնումարները. Բանկային գործարքներ կամ գնումներ կատարելիս ստուգե՛ք և համոզվե՛ք, որ կայքն անվտանգ է: Եթե ցանցային հասցեն սկսվում է https://-ով, նշանակում է, որ կայքը լրացուցիչ միջոցներ է ձեռնարկել ձեր տեղեկությունները պաշտպանելու նպատակով: Http://-ն անվտանգ չէ:

Ցանցի հարցում եղեք գիտակ

- **Թարմացրեք ձեր գիտելիքները: Ուսումնասիրեք համացանցային անվտանգության նոր ուղիները:** Ամենավերջին տեղեկություններին ծանոթացեք վստահելի կայքերից և կիսեք դրանք ընկերների, ընտանիքի անդամների և գործընկերների հետ՝ խրախուսելով նրանց լինել գիտակ համացանցիհարցում:
- **Գործելուց առաջ մտածեք.** Զգուշացեք այնպիսի հաղորդագրություններից, որոնք ձեզ կոչ են անում գործելու անմիջապես, առաջարկում են բաներ, որոնք չափազանց լավն են այդպիսիք լինելու համար կամ հայցում են անձնական բնույթի տեղեկություններ:
- **Ունեցեք պահուստավորված օրինակներ.** Պաշտպանեք ձեր արժեքավոր ստեղծագործությունը, երաժշտությունը, լուսանկարները և այլ թվային տեղեկությունները՝ ստեղծելով դրանց էլեկտրոնային կրկնօրինակները և անվտանգ կերպով պահուստավորելով դրանք:

Եղեք լավ առցանց քաղաքացի

- **Ինչն առավել անվտանգ է ինձ համար, անվտանգ է նաև այլոց համար.** Այն, ինչ անում եք համացանցում, կարող է ազդել շատերի վրա տանը, աշխատավայրում և ողջ աշխարհում: Ճիշտ համացանցային սովորություններ ունենալուց շահում է համաշխարհային թվային հանրությունը:
- **Տեղադրեք այնպիսի նյութեր այլոց մասին, որ կուզենայիք այլոք տեղադրեին ձեր մասին.**
- **Օգնեք պետական մարմիններին կիբեռհանցագործության դեմ պայքարում.** Հաղորդեք հափշտակված ֆինանսական միջոցների, ինքնության և կիբեռհանցագործությունների մասին http://www.ic3.gov (Internet Crime Complaint Center, Ինտերնետային հանցագործությունների կենտրոն) և http://www.onguardonline.gov/filecomplaint (FTC, Առևտրի դաշնային հանձնաժողով).