Տեղեկատվական անվտանգություն բոլորի համար

Որքան էլ դուք չեք սիրում տեխնիկական մանրամասները, անվտանգ լինելու համար պետք է հետաքրքրվել համակարգչի, ծրագրերի, ցանցի աշխատանքից: «Ես դրանցից բան չեմ հասկանում» մեթոդը չի փրկում կյանքում: Սա ինտերնետն է, այստեղ կարող են թալանել, վնասել եւ այլն, եւ այլն, եւ այլն...

Ընդհանուր համակարգը

Համակարգիչ, խելախոս, պլանշետ

Ընդհանուր համակարգը

Եթե օգտվում եք Windows օպերացիոն համակարգից, ապա ունեցեք միացրած եւ միշտ թարմ հակավիրուսային ծրագիր

Թարմ պահեք օպերացիոն համակարգը, մի անջատեք Update-ը

Օգտվեք լիցենզիոն ծրագրերից, որոնք գողացած չեն: Իսկ ավելի լավ է օգտվել OpenSource բաց կոդով տարբերակներից

Ընդհանուր համակարգը

Փորձեք օգտվել Open Source բաց կոդերով օպերացիոն համակարգերից եւ ծրագրերից: Դրանք ավելի անվտանգ են՝ չնայած, որ այդքան թիթիզ չեն

Ընդհանուր համակարգը

Խելախոսների (սմարթֆոնների) եւ պլանշետների դեպքում հավելվածները տեղադրեք միայն պաշտոնական խանութներից. Google Play, App Store:

Մնացած դեպքերում ինչ ասես կարող է պատահել:

Գաղտնաբառերը

Գաղտնաբառերը պետք է

- Լինեն երկար 10-12 նիշից
- Պարունակեն տառեր, մեծատառեր, թվեր, հատուկ նշաններ (օրինակ, !, $, #, ?)

Գաղտնաբառեր

Վատ գաղտնաբառի օրինակ.

Gago123456

Լավ գաղտնաբառի օրինակ.

Gago!DuDemqEs537

Գաղտնաբառերը պետք է

Տարբերվեն կայքից կայք. կրկնվող գաղտնաբառը արդեն իսկ վտանգ է

Գաղտնաբառերը պետք է

պաշտպանվի ամենալավ տարբերակով՝ Two-Factor Authentication: Սա մի քիչ բարդ է, բայց հուսալի:

Facebook-ում սա միացնելու մասին կարող եք կարդալ այստեղ: Նմանատիպ հնարավորություն այսօր տրամադրում են գրեթե բոլոր լուրջ կայքերը

e-Mail

Զգուշացեք անհայտ հասցեատերերից եկած նամակներից.

- մի բացեք նման նամակներին կցած ֆայլերը: .zip, .rar, .exe ֆայլերից պետք է հեռու մնալ, նույնիսկ եթե ծանոթ է ուղարկել
- մի կտացրեք նույնիսկ ծանոթ թվացող հղումներին՝ պետք լինելու դեպքում հավաքեք ձեռքով

SMS

Տարատեսակ մեսենջերներ Viber, Skype, Whatsapp եւ այլն

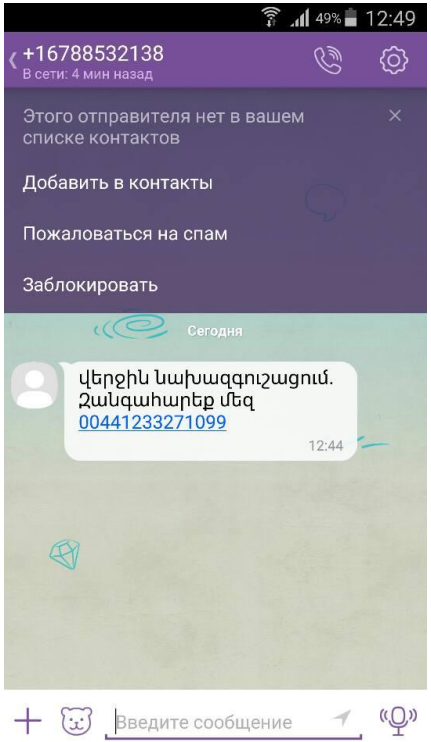
Անծանոթ համարներից ստացված SMS□ներ

Դրանք պետք է անտեսվեն, քանի որ կարող են օգտագործվել.

- ձեզանից դրամ շորթելու
- խուճապ ստեղծելու համար

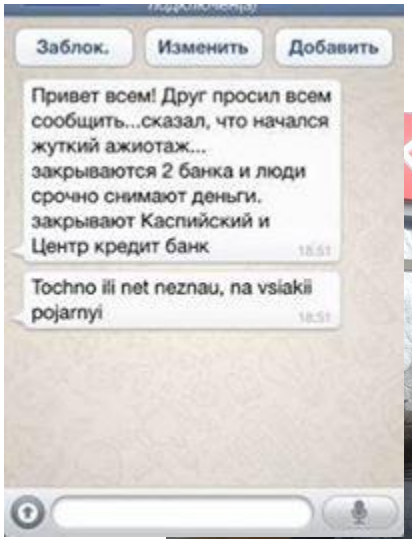
Անծանոթ համարներից ստացված SMS□ները ՝

կարող են օգտագործվել ձեզանից գումար գողանալու համար: Հայաստանում նման փորձերը շատացել են



Անծանոթ համարներից ստացված SMS□ները ՝

Օրինակ, Ղազախստանում օգտագործվեցին բանկային համակրգը
խարխլելու համար

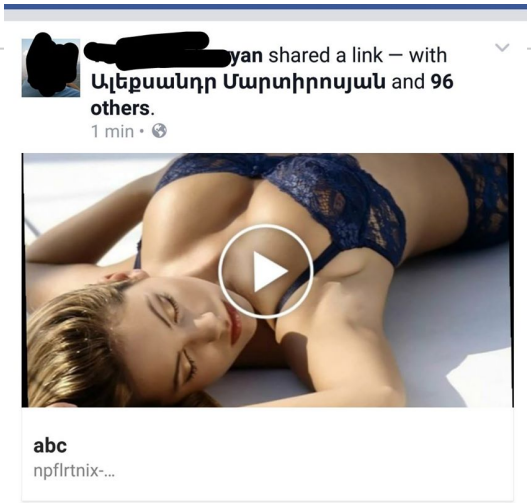


Սոցիալական ցանցեր

Մի կտացրեք անմիջապես ամեն բանի, ինչին հայացքը դիպչում է.

մի հատ խորը շունչ քաշեք, ուշադիր նայեք, հասկացեք ինչ է՝ նոր կտացրեք

Սոցիալական ցանցեր



Նույնիսկ ձեր ընկերոջից եկած գեղեցիկ աղջիկների նկարներին մի կտացրեք առանց մտածելու: Օրինակ, հարցրեք, թե դա ինչ է: Եթե դա վիրուսն է տարածում, ապա նա չի պատասխանի ձեր ընկերոջ տեղը: Դեռ որ...

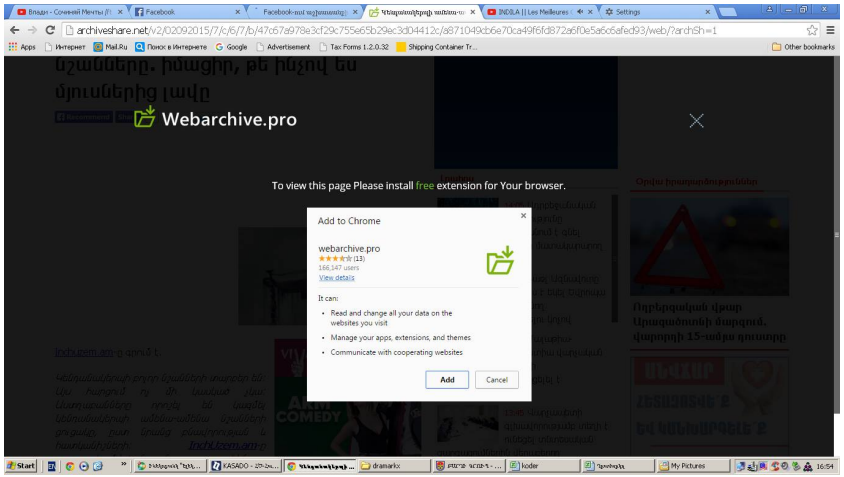
Սոցիալական ցանցեր

Եթե չեք դիմացել, կտացրել եք, ոչ մի բանի ձեռք մի տվեք:

Անհապաղ հեռացեք այդտեղից:

Սոցիալական ցանցեր

Հենց այս քայլի վրա հաքերները փորձում են ձեր մոտ մի զզվանք տեղադրել, օրինակ archiveshare, որի պատճառով ձեր ընկերները ձեզ արդեն չեն սիրում



Սոցիալական ցանցեր

Եթե կայքերը առաջարկում են ձեզ թարմացնել Flash, Java, տեղադրել Chrome Extension՝ անհապաղ հեռացեք այդ կայքերից: Մեծ հավանականությամբ դուք հարձակման եք ենթարկվում:

Տեղեկատվության աղբյուրները

Տեղեկատվության աղբյուրները

Միշտ ունեցեք ձեր կողմից վստահելի

- լրատվամիջոցներ
- կոնկրետ թեմաների վերաբերյալ վստահելի աղբյուրներ. ԶԼՄ-ներ, բլոգներ, փորձագետներ, որոնք կան սոցցանցերում

Տեղեկատվության աղբյուրները

- Ճգնաժամային իրավիճակներում հավատացեք միայն տվյալ, ստուգված աղբյուրներին
- Բոլոր մնացած աղբյուրներին մոտեցեք կասկածով եւ մի տարածեք դրանք առանց ստուգելու

Ամենակարեւորը. ուշադիր լինելը եւ զգացմունքներին չտրվելը փրկում է 10 վտանգից 9-ից

Սամվել Մարտիրոսյան

FB.com/Samvel
Twitter: @Kornelij