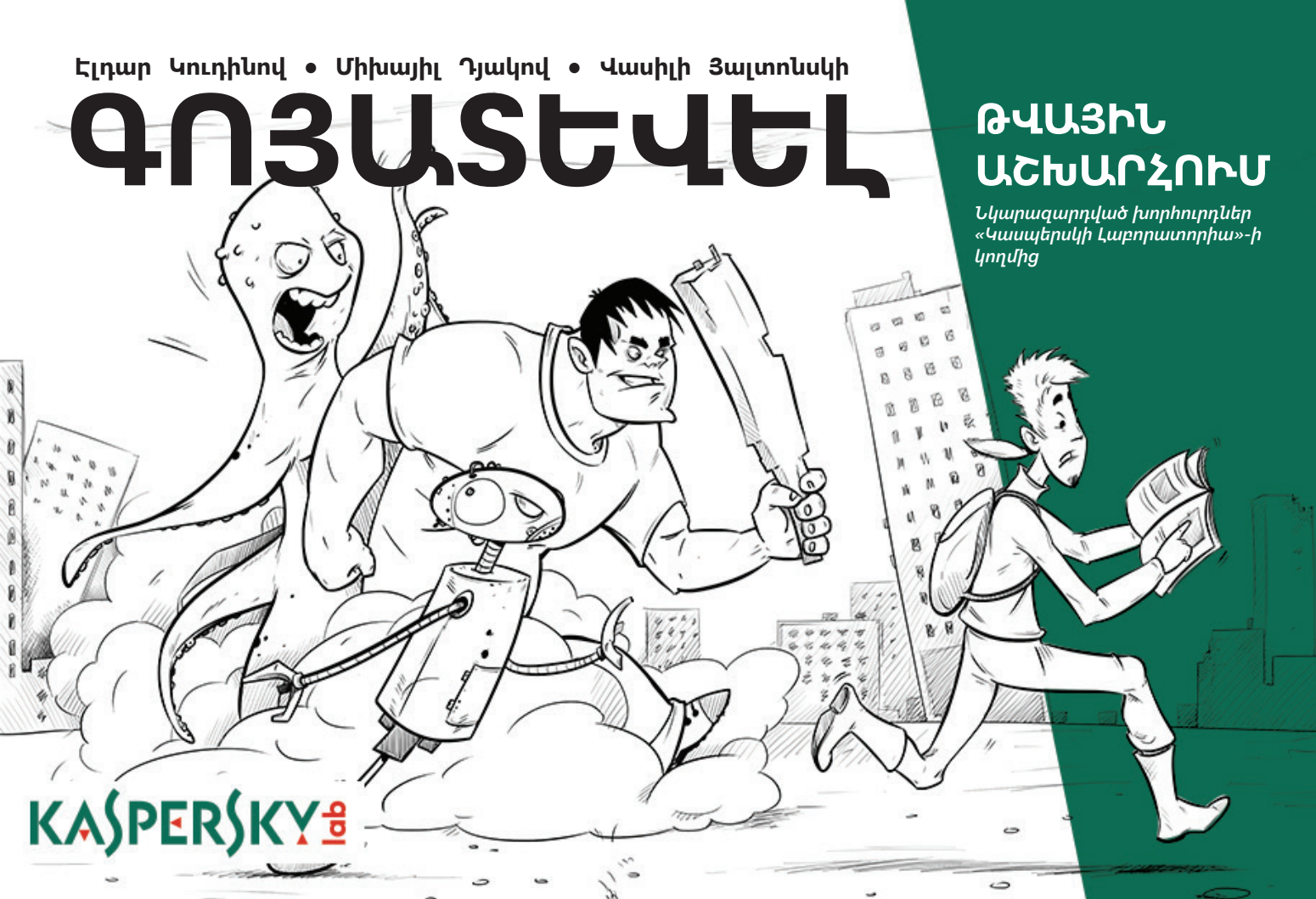
Էլդար Կուդինով • Միխայիլ Դյակով • Վասիլի Յալտոնսկի

ԳՈՅԱՏԵՎԵԼ

ԹՎԱՅԻՆ ԱՇԽԱՐՀՈՒՄ

Նկարազարդված խորհուրդներ «Կասպերսկի Լաբորատորիա»-ի կողմից



KASPERSKY lab

Էլդար Կուդինով • Միխայիլ Դյակով • Վասիլի Յալտոնսկի

ԳՈՅԱՏԵՎԵԼ

ԹՎԱՅԻՆ ԱՇԽԱՐՀՈՒՄ

Նկարազարդված խորհուրդներ «Կասպերսկի Լաբորատորիա»-ի կողմից

2016

Էլդար Կուդինով, Միխայիլ Դյակով, Վասիլի Յալտոնսկի

Գոյատևել թվային աշխարհում: Նկարազարդված խորհուրդներ «Կասպերսկի Լաբորատորիա»-ի կողմից:

Թվային աշխարհի ծաղկումը այնպիսին չէր, ինչպես մենք պատկերացնում էինք: Անհատական համակարգիչները և շարժական սարքերը գիտելիքը մատչելի դարձրեցին մարդկանց համար և տվեցին նոր հնարավորություններ այդ գիտելիքը փոխանակելու համար: Մարդկանց առօրյա գործունեությունը դարձել է դյուրին նոր տեխնոլոգիաների շնորհիվ՝ առաջին հերթին համացանցի միջոցով: Բայց շատ արագ պարզվեց, որ մեդալն ունի հակառակ երեսը՝ եղան անձնական ինֆորմացիայի գողության առաջին դեպքերը, թվային վնասատու ծրագրերը «սովորեցին» վնաս հասցնել, իսկ տարբեր հանցագործներ և այլասերվածներ սկսեցին համացանցը օգտագործել որպես սեփական խաղահրապարակ: Բայց գտնվեցին մարդիկ, ովքեր դեմ կանգնեցին քաոսին և հավաքեցին դրա դեմ պայքարի իրենց ամբողջ փորձը՝ հաջորդ սերունդներին փոխանցելու համար: Այստեղ լեգենդի մռայլ մասը ավարտվում է, և սկսվում է մեր պատմությունը...

Հետևելով «Կասպերսկի Լաբորատորիա»-ի խորհուրդներին՝ դուք չեք դառնա համացանցի խարդախների և կիբեռհանցագործների զոհը, իսկ ձեր համակարգիչը կլինի հուսալի պաշտպանված վիրուսներից և վնասաբեր ծրագրերից:

Գիրքը պատրաստել են.

Էլդար Կուդինովը
Միխայիլ Դյակովը
Վասիլի Յալտոնսկին
Մաքսիմ Բարանովսկին
Սերգեյ Մալենկովիչը
Յուլյա Պոլոզովան
Եվգենի Չերնիշևը

ՆԱԽԱԲԱՆ

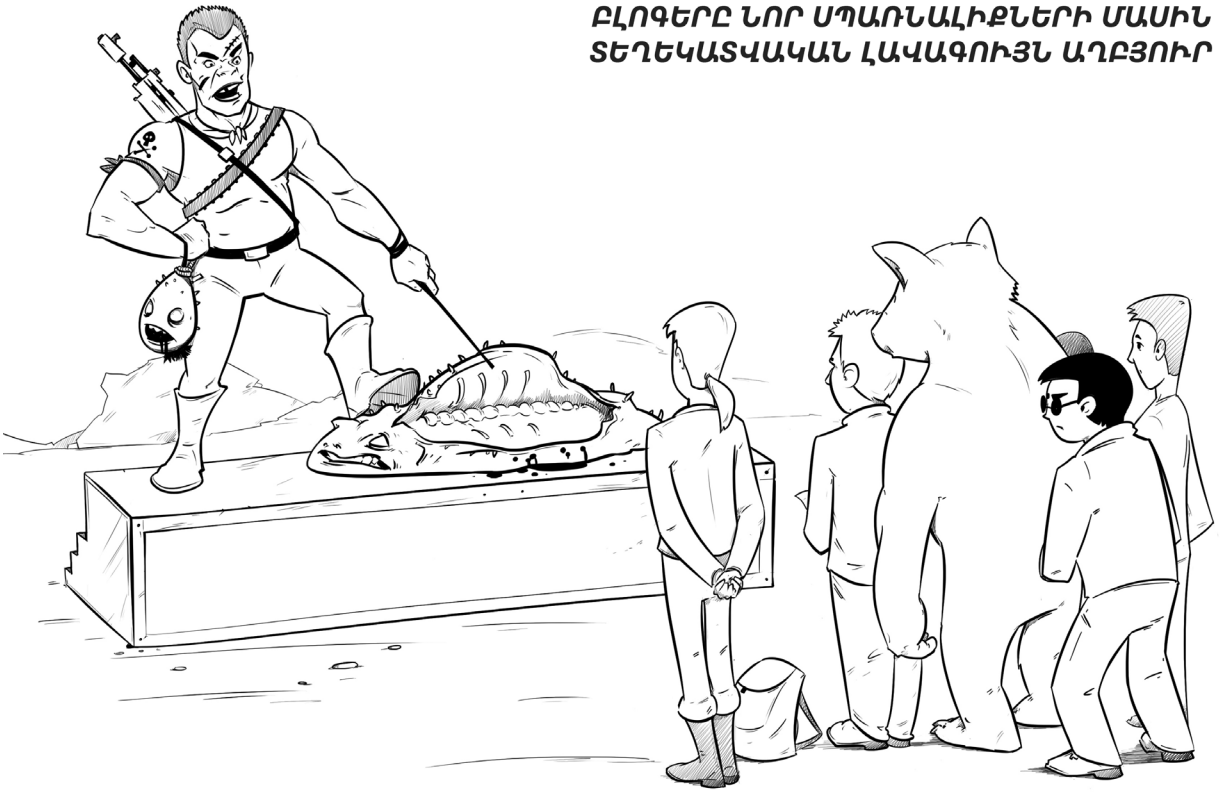
Թվային աշխարհի ծաղկումը այնպիսին չէր, ինչպես մենք պատկերացնում էինք: Անձնական համակարգիչները և բջջային սարքերը գիտելիքը մատչելի դարձրեցին մարդկանց համար և տվեցին նոր հնարավորություններ այդ գիտելիքը փոխանակելու համար: Մարդկանց առօրյա գործունեությունը դարձել է դյուրին նորագույն տեխնոլոգիաների շնորհիվ՝ առաջին հերթին համացանցի միջոցով: Բայց շատ արագ պարզվեց, որ մեդալն ունի հակառակ երեսը՝ եղան անձնական ինֆորմացիայի գողության առաջին դեպքերը, վնասատու ծրագրերը «սովորեցին» վնաս հասցնել, իսկ տարբեր հանցագործներ սկսեցին համացանցը օգտագործել որպես սեփական խաղահրապարակ: Գտնվեցին մարդիկ, ովքեր դեմ կանգնեցին քաոսին և հավաքեցին իրենց փորձը հաջորդ սերունդներին փոխանցելու համար: Այստեղ լեգենդի մռայլ մասը ավարտվում է, և սկսվում է մեր պատմությունը:

ԿԻԲԵՌՍՊԱՌՆԱԼԻՔՆԵՐԻՑ ՊԱՇՏՊԱՆՈՒՄ Է ԳԻՏԵԼԻՔԸ

ԽՈՐՀՈՒՐԴ 1: **ՕԳՏԱԿԱՐ ԳԻՏԵԼԻՔՆԵՐ**

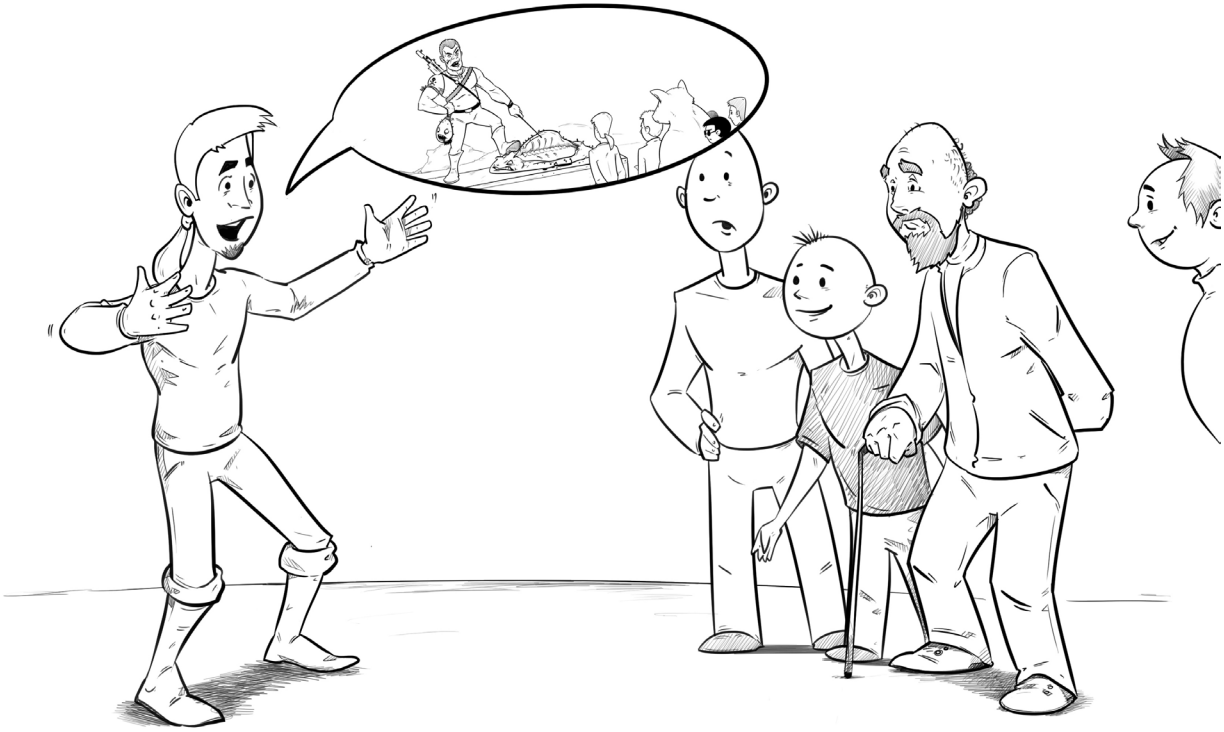
Պատկերացրեք, որ հեռախոսային ցանցի միջոցով վիրուսը մտնում է համակարգչի մեջ, միացնում է այն գիշերով և հրահանգում է գործարկել միջուկային հրթիռները... Ստացվեց մի պատկեր հոլիվուդյան ֆիլմերից, որոնք հեռու են իրականությունից: Իրականում վնասատու ծրագրերը գործում են այլ կերպ և հարձակվում են այլ թիրախների վրա: Վիրուսները օգտվում են այն հանգամանքից, որ համակարգչային համակարգերը ունեն խոցելի տեղեր և այն, որ համակարգիչների օգտատերերը չգիտեն ինֆորմացիոն անվտանգության հիմունքները: Եթե ցանցահենը ուզենա վարակել ինչ-որ մեկի համակարգիչը՝ նա կուղարկի էլեկտրոնային նամակ՝ վարակված ներդիրով: Եթե նամակի բովանդակությունը համոզիչ լինի, ապա հասցեատերը ինքը կգործարկի վնասատու ծրագիրը: Այդ պատճառով ազնիվ մարդկանց հաղթանակը կիբեռհանցագործների հետ մրցելիս ուղղակիորեն կապված է վտանգների մասին տեղեկացված լինելուց:

ՀԱԿԱՎԻՐՈՒՍԱՅԻՆ ԱՌԱՋԱՏԱՐ ԸՆԿԵՐՈՒԹՅՈՒՆՆԵՐԻ ԲԼՈԳԵՐԸ ՆՈՐ ՍՊԱՌՆԱԼԻՔՆԵՐԻ ՄԱՍԻՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԼԱՎԱԳՈՒՅՆ ԱՂԲՅՈՒՐ



ԽՈՐՀՈՒՐԴ 2: ԻՆՖՈՐՄԱՑԻԱՅԻ ԱՂԲՅՈՒՐՆԵՐ

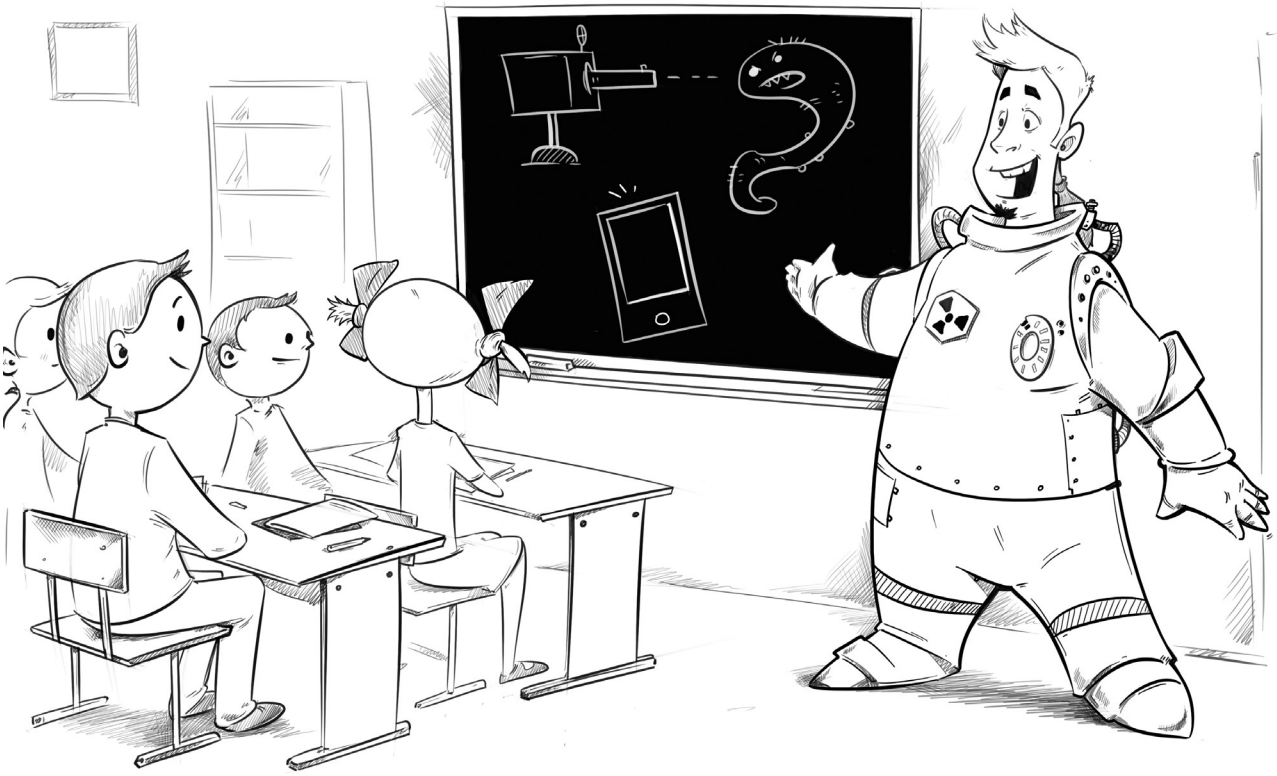
Տեղեկացված լինել նշանակում է պատրաստ լինել հակազդելու: Այսպիսի դիրքորոշումը ճիշտ է ինֆորմացիոն սպառնալիքների դեպքում: Սպառնալիքների և պաշտպանության հակամարտության մեջ հաղթում է ոչ թե նա, ով լավ է զինված, այլ նա, ով ավելի շատ բան գիտի հակառակորդի մասին: Հակավիրուսային ընկերությունների բլոգներում միշտ կարելի է գտնել տեղեկություններ վիրուսների, չարագործների հնարքների և ծրագրային ապահովման խոցելիության մասին: Ուշադիր ընթերցողն այնտեղ կկարդա, թե ինչպես չընկնել հանցագործների ծուղակը և կանխարգելել հարձակումը համակարգչի վրա:



ԿԻՍՎԵՔ ՁԵՐ ՍՏԱՑԱԾ ԳԻՏԵԼԻՔՆԵՐՈՎ ՀԱՐԱՁԱՏՆԵՐԻ ՀԵՏ

ԽՈՐՀՈՒՐԴ 3: ՀՈԳԱՏԱՐՈՒԹՅՈՒՆ ՀԱՐԱՁԱՏՆԵՐԻ ՆԿԱՏՄԱՄԲ

Ազնիվ օգտատերերի վրա հարձակվելու համար ցանցահենները ստեղծել են ֆիշինգ, էքսպլոյտներ, մալվերտայզինգ և ուրիշ անհասկանալի բառեր: Բայց սա ամենավտանգավորը չէ: Կիբեռհանցագործների զինանոցի ամենահզոր զենքը նրանց զոհերի անտեղյակությունն է կիբեռսպառնալիքների մասին: Չի կարելի պաշտպանվել մի բանից, ինչի գոյության մասին դու չգիտես, և այստեղ առաջին պլան է դուրս գալիս պոտենցիալ զոհերի միջև ինֆորմացիայի ազատ փոխանակումը: Ձեր հարազատներին մանրամասն պատմեք նոր կիբեռսպառնալիքների մասին:



ԵՐԵԽԱՆԵՐԻ ՀԵՏ ԿԻՍԵՔ ԳԻՏԵԼԻՔՆԵՐԸ ԿԻԲԵՌԱՇԽԱՐՀԻ ՄԱՍԻՆ

ԽՈՐՀՈՒՐԴ 4: **ԵՐԵԽԱՆԵՐԻ ՈՒՍՈՒՑՈՒՄԸ**

Ժամանակակից ծնողները թերագնահատում են իրենց երեխաների ունակությունները համակարգչի, գաջետների և համացանցի յուրացման գործում: Երեխան երեկ խոսել չգիտեր, իսկ այսօր արդեն գրանցվել է մի քանի կայքերում և վարում է սեփական ալիքը «YouTube»-ում: Ձեզնից է կախված, թե ինչպիսի կիբեռհարձակումների կկարողանա նա դիմակայել: Բացի ձեզնից ոչ ոք չի պատմի երեխային համացանցի գայթակղությունների և վտանգների մասին: Այդ գիտելիքները այսօրվա դեռահասին ավելի անհրաժեշտ են, քան սեռական դաստիարակությունը:

ՄԻ ԹՈՂԵՔ ՁԵՐ ՓՈՍՏԱՅԻՆ ՀԱՍՑԵՆ ՀԱՍԱՐԱԿԱԿԱՆ ՎԱՅՐԵՐՈՒՄ,
ԵԹԵ ՉԵՔ ՈՒԶՈՒՄ ԴԱՌՆԱԼ ՍՊԱՄԵՐՆԵՐԻ ԹԻՐԱԽԸ

ԽՈՐՀՈՒՐԴ 5: **ՓՈՍՏԸ ԱՌԱՆՑ ԱՂԲԻ**

Երկրագնդի յուրաքանչյուր բնակչին հուզիչ խոսքերով և ձեռնտու առևտրային առաջարկ անելը գովազդային գործակալների երազանքն է, ինչը հնարավոր է դարձել էլեկտրոնային փոստի շնորհիվ: Մեր օրերում այդպիսի մարդկանց ձեռքով չեն բարևում, քանի որ գովազդային նամակների սպամ հոսքը գերազանցել է բոլոր բանական սահմանները՝ ծանրաբեռնելով համացանցը և օգտատերերի գիտակցությունը: Օգտատերը ստիպված է ամեն օր մաքրել իր էլեկտրոնային փոստարկղը գովազդից: Որպեսզի ժամանակ չծախսեք աղբը հեռացնելու համար, հանրամատչելի վայրերում ձեր հասցեն մի հրապարակեք, հակառակ դեպքում հանրային ֆորումում հայտնվելուց մի քանի վայրկյան հետո ձեր էլեկտրոնային փոստը կընկնի սպամերի ձեռքը: Ահա և առաջընթացի պտուղները:

**ՈՒՇԱԴԻՐ ՈՒՍՈՒՄՆԱՍԻՐԵՔ ՊԱՇՏՈՆԱԿԱՆ ՆԱՄԱԿԸ,
ՄԻՆՉ ԱՅՆՏԵՂ ԳՐՎԱԾ ՀՐԱՀԱՆԳՆԵՐԻՆ ՀԵՏԵՎԵԼԸ**

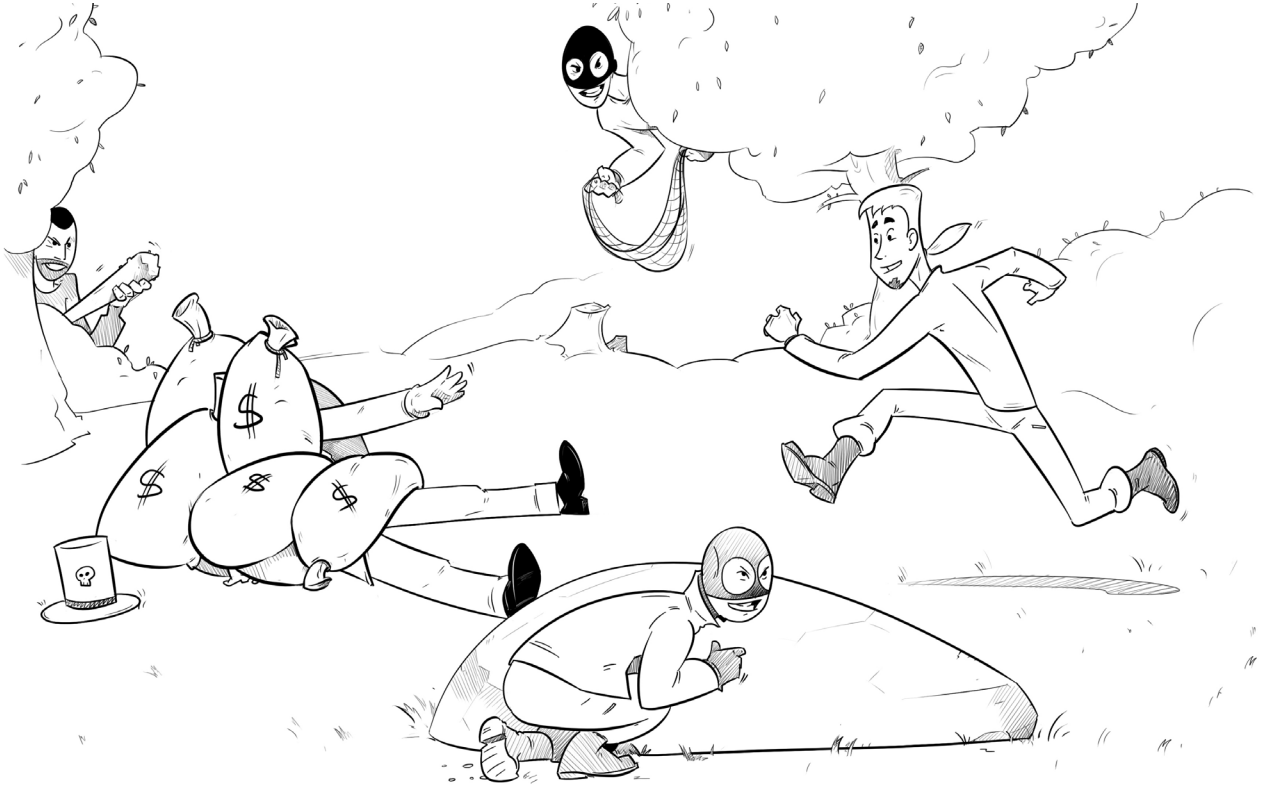
ԽՈՐՀՈՒՐԴ 6: **ԿԵՂԾ ՆԱՄԱԿՆԵՐ**

Դուք չէիք սպասում էլեկտրոնային փոստով նամակ ստանալ հարկային տեսչությունից, բայց ստացել եք: Նամակում պահանջվում է անհապաղ վճարել տուգանքը, հակառակ դեպքում սպառնում են գործը ուղարկել դատախազություն կամ դատարան: Մի բարկացեք և մի շտապեք սեղմել նամակում եղած հղումների վրա կամ բացել կցված փաստաթղթերը: Սկզբում համոզվեք, որ նամակը իսկապես հարկային տեսչությունից է: Պետական հիմնարկների կամ հայտնի ընկերությունների անունից ուղարկված կեղծ նամակների միջոցով կիբեռվարակներ տարածելը ամենատարածված մեթոդն է: Չարագործները կարող են ներկայանալ որպես հարկային տեսուչ, դատարանի ներկայացուցիչ կամ որևէ պաշտոնյա, սոց. ցանցի կամ ինտերնետ-մատակարարի ներկայացուցիչ: Նրանց նպատակն է շեղել ձեր ուշադրությունը և կատարել իրենց անհրաժեշտ գործողությունները: Այդ պատճառով որևէ հաղորդագրություն ստանալիս կապի այլ միջոցներով ստուգեք դրա իսկությունը: Մի ծուլացեք, զանգահարեք , օրինակ, հարկային տեսչություն և պարզեք՝ ձեզ հաղորդագրություն ուղարկել են, թե՝ ոչ:

ՄԻ ԲԱՑԵՔ ԿԱՍԿԱԾԵԼԻ ՆԵՐԴԻՐՆԵՐԸ

ԽՈՐՀՈՒՐԴ 7: **ԹԱՔՆՎԱԾ ՍՊԱՌՆԱԼԻՔ**

Դուք սիրո՞ւմ եք անակնկալներ: Համացանցում շատ մարդիկ կան, որոնք սիրում են անակնկալներ մատուցել: Այդ անակնկալները ձեզ դուր չեն գա, որովհետև դրանց ստեղծմանը մասնակցել են չարամիտները և վնասատու ծրագրային ապահովումը: Օրինակ, դուք կարող եք նամակ ստանալ հղումով՝ «շատ զիլ վիդեո է, կմեռնես» կամ «ֆոտոներ այն երեկույթից»: Մտածեք, թե ով և ինչու է ձեզ նման բան ուղարկել: Ամենայն հավանականությամբ ուղարկողին դուք չեք ճանաչում, իսկ ֆոտոների փոխարեն տրոյան է: Անգամ եթե շատ եք սիրում անակնկալներ՝ մի բացեք այդպիսի նամակները:



ՄԻ ՀԱՎԱՏԱՑԵՔ «ՆԻԳԵՐԻԱՑԻ» ԴԺԲԱԽՏ ՄԻԼԻՈՆԱՏԵՐԵՐԻՆ

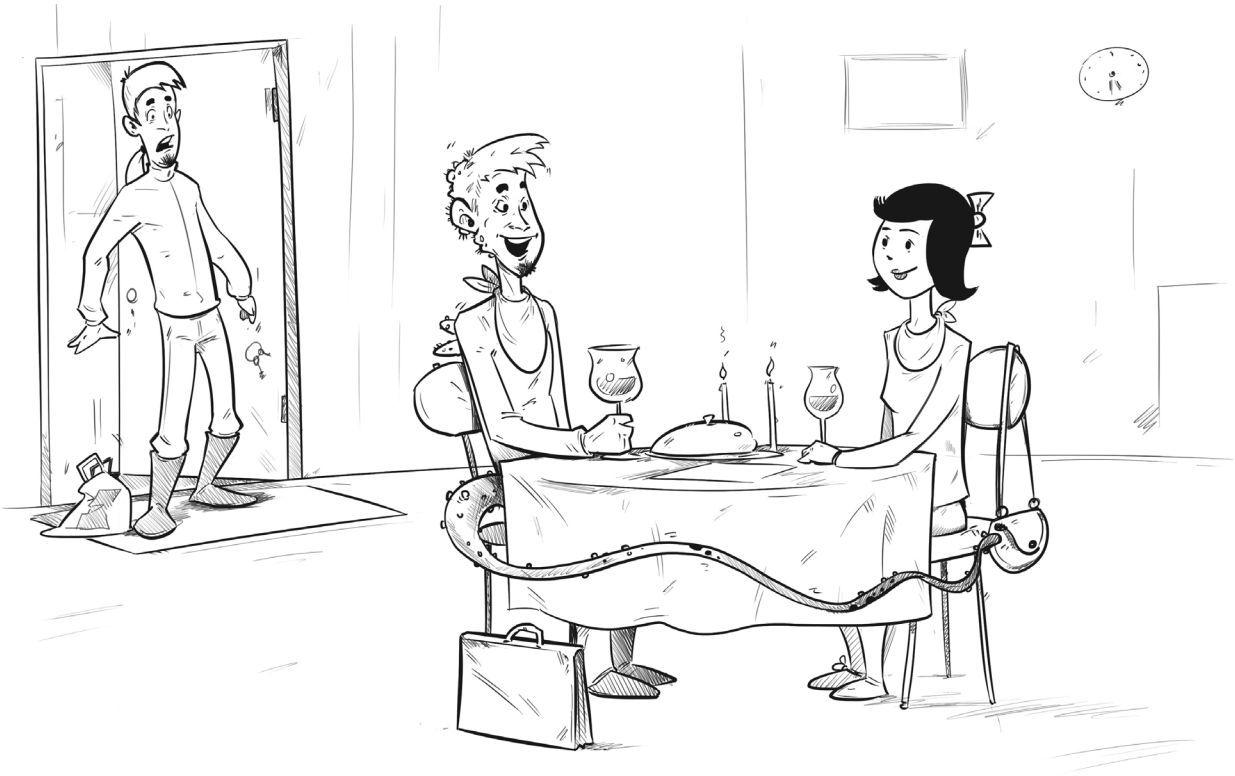
ԽՈՐՀՈՒՐԴ 8: **ԿԵՂԾ ՀԱՐՈՒՍՏՆԵՐ**

Եթե հեռավոր ապագայում կիբեռհնագետները սկսեն ուսումնասիրել այսօրվա անթիվ-անհամար Էլեկտրոնային նամակները՝ նրանց կզարմացնի Նիգերիայում ապրող միլիոնատերերի քանակը: Հնարավոր է, որ այդ երկիրի անունը նշվի դասագրքերում՝ որպես կախարդական երկիր, որտեղ ապրում էին հեքիաթային հարստություն ունեցող, բայց շատ դժբախտ մարդիկ: Մեր օրերում այդ հեքիաթներին պետք չէ հավատալ: Եթե անգամ այդ ոչ հարուստ երկրում գտնվի միլիոնատեր՝ դժվար թե նա օգնություն խնդրի հեռավոր Ռուսաստանում ապրող անծանոթ մարդուց Էլեկտրոնային փոստի միջոցով: Իրականում նիգերիացի միլիոնատերերի, աֆրիկացի արքայազների և հարուստ, բայց դժբախտ կերպարների անունից նամակները ուղարկում են հանցագործները, որոնք հույս ունեն մարդկանց ագահությունից օգուտ քաղել: Նրանք, ովքեր ուզում են «միլիոնատիրոջ» հետ կիսել նրա հարստությունը, վճարում են «դրամական փոխանցման ձևակերպման» համար, «ժառանգության հարկը» կամ «փաստաբանի ծառայությունների» համար, և այսպիսով կերակրում են հեռավոր երկրում ապրող քաղցած, բայց խորամանկ հանցագործին և նրա ընկերներին:

ՍՊԱՄ-ՑՐՈՒՄԸ ԱՇԽԱՏԱՆՔԻ ԱՌԱՋԱՐԿՈՒԹՅՈՒՆՆԵՐԻ ԼԱՎԱԳՈՒՅՆ ԱՂԲՅՈՒՐԸ ՉԷ

ԽՈՐՀՈՒՐԴ 9: **ՎՏԱՆԳԱՎՈՐ ՍՊԱՄ**

Ստրկատերերը չէին ենթադրում, որ մարդիկ մեծ ուրախությամբ պատրաստ են լուծը քաշել առանց վարձատրության: Պետք է ընդամենը խաբել նրանց՝ ոսկե սարեր խոստանալով: Ամենահեշտ միջոցը անվճար կամ էժան աշխատուժ հավաքագրելու համար սովորական սպամն է: Պետք է հորինել խոսուն վերնագիր և գրավիչ խոստումներ: Եթե դուք չեք խաբվի համացանցում փող աշխատելու գրավիչ առաջարկությամբ, ապա կլինեն հարյուրավոր մարդիկ, ովքեր հաճույքով կարձագանքեն գովազդային գրավիչ առաջարկություններին:



ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ԳՈՂՈՒԹՅՈՒՆԸ ԲԵՐՈՒՄ Է ՏՉԱՃ ՀԵՏԵՎԱՆՔՆԵՐԻ

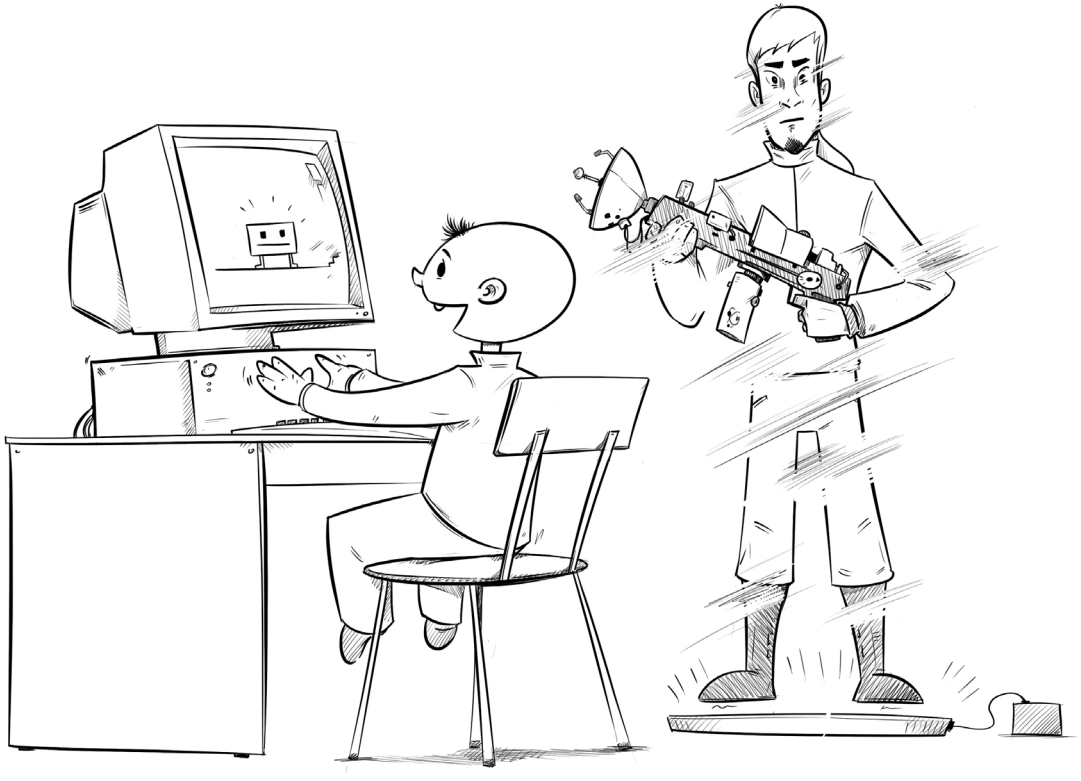
ԽՈՐՀՈՒՐԴ 10: **ԱՆՁԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ**

Մարդիկ տարբեր են, բայց համացանցում օգտատեր Արամը տարբերվում է օգտատեր Տիգրանից անվան և գաղտնաբառի յուրահատուկ համադրությամբ, որոնք, ինչպես և այլ տվյալներ, կարելի է գողանալ կամ կեղծել: Եթե Արամին պետք լինի համացանցում ներկայանալ որպես Տիգրան, բավական է, որ նա անցնի «գաղտնաբառի վերականգնում» գործընթացը: Իսկ դրա համար նա Տիգրանի մասին պետք է իմանա մի քանի տվյալ, որոնք կարող է գտնել սոց. ցանցում Տիգրանի բաց պրոֆիլում: Դրանք կարող են լինել Տիգրանի կնոջ ծննդյան օրը կամ Տիգրանի սիրելի շան անունը: Այս տվյալները, որպես պատասխան կարող են տրվել ստուգող հարցերին, որոնք տրվում են Էլեկտրոնային փոստի գրանցման համար: Տիրանալով Տիգրանի փոստին, Արամի համար հասանելի կլինեն բոլոր այն ծառայությունները, որտեղ Տիգրանն իր փոստի հասցեն նշել է որպես գրանցման հասցե: Այստեղից հետևություն՝ անձնական տվյալները շատ արժեքավոր են, կարիք չկա դրանք ամեն տեղ հրապարակել:

ԾՆՈՂՆԵՐԻ ՀԱՇՎԱԳՐԱՆՑՈՒՄԸ ԱՆՑԱԹՈՒՂԹ Է ՄԵԾԱՀԱՍԱԿՆԵՐԻ ԱՇԽԱՐՀ

ԽՈՐՀՈՒՐԴ 11: **ՀԱՄԱՑԱՆՑԸ ԵՐԵԽԱՆԵՐԻ ՀԱՄԱՐ**

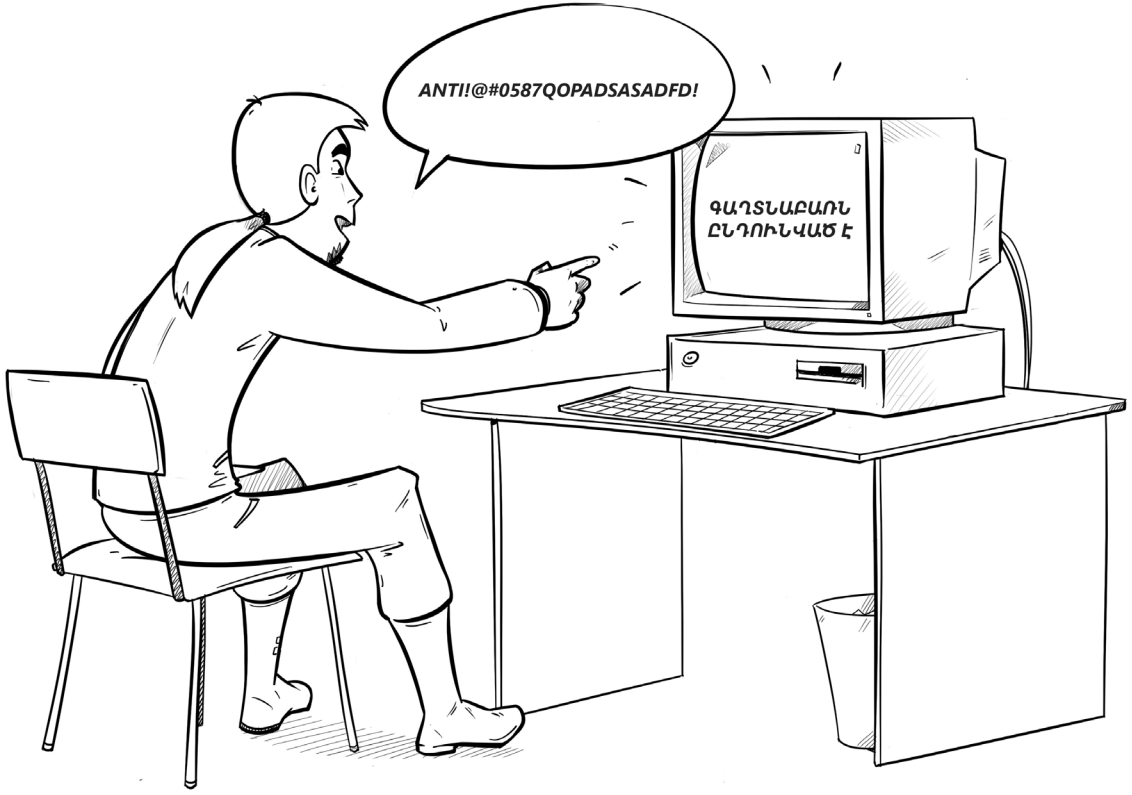
Ծնողների վերահսկողական ծրագրերը հիմնականում լավ են աշխատում՝ համացանցում երեխաներին զերծ պահելով վնասակար ինֆորմացիայից և անցանկալի շփումներից: Սակայն այդ ծրագրերը չեն օգնի, եթե երեխան իմանա հաշվագրանցման գաղտնաբառը: Նա կարող է այդ գաղտնաբառով մուտք գործել մեծահասակներին հասանելի տիրույթը: Իրական կյանքում երեխան տարբերվում է մեծահասակից, բայց կիբեռաշխարհում ամեն ինչ ավելի հեշտ է, այնտեղ օգտատիրոջ լուսանկարը կամ փաստաթղթերը չեն հարցնում: Հիշեք, ինչքան խիստ եք որևէ բան արգելում երեխային, այնքան ավելի է նա դրան ձգտում: Գաղտնաբառը երեխայի համար չպետք է հասանելի լինի:



ԾՆՈՂՆԵՐԻ ՀՍԿՈՂՈՒԹՅՈՒՆԸ ԵՐԵԽԱՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՄԻՋՈՑ

ԽՈՐՀՈՒՐԴ 12: **ԵՐԵԽԱՅԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ**

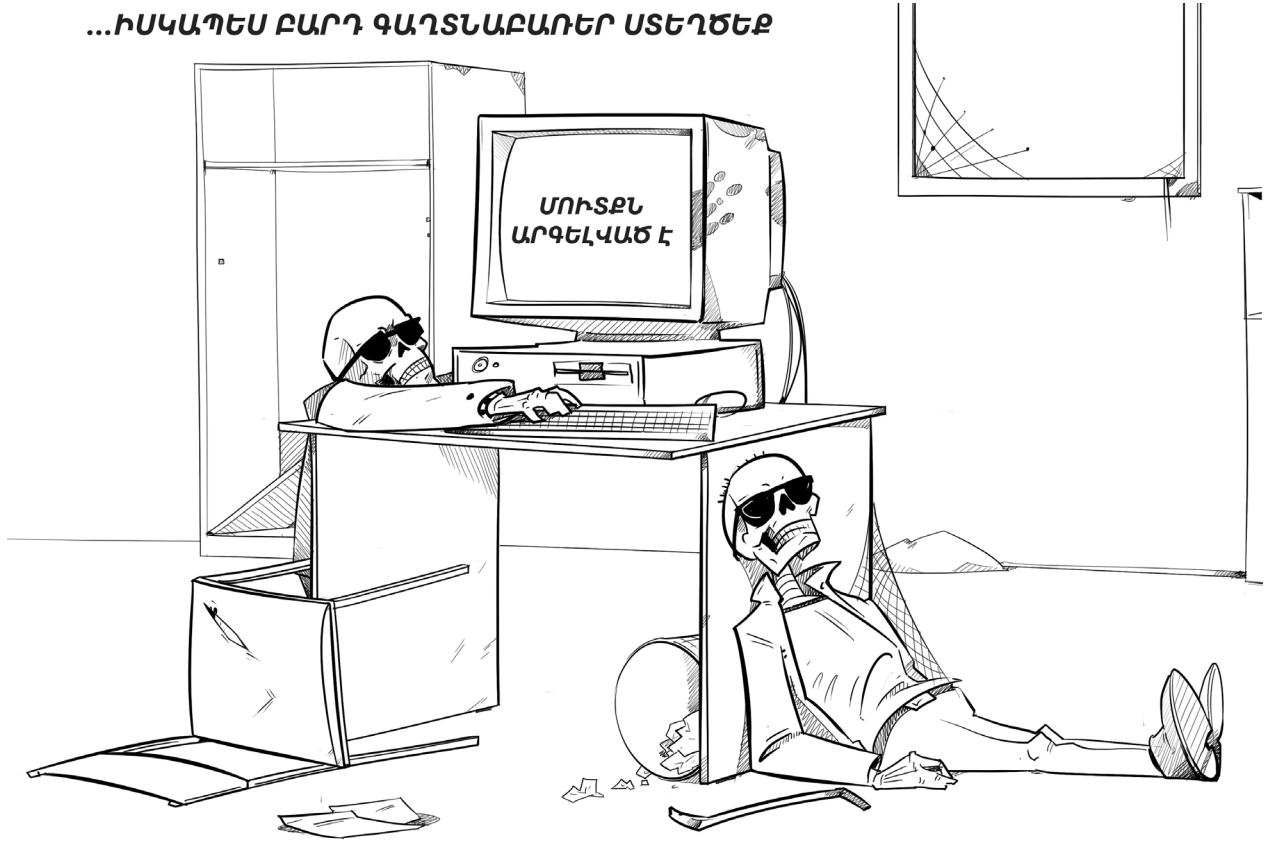
Երբ երրորդ դասարանում սովորող ձեր դուստրը սկսի գռեհիկ խոսել կամ տարբեր սեռերի ներկայացուցիչների հարաբերությունների մասին իր տեղեկացվածությունը հայտնի, մի շտապեք բարկանալ նրա համադասարանցիների կամ ձեր անզուսպ հարևանների վրա: Չարիքի աղբյուրը ոչ թե դպրոցն ու բակն են, այլ ձեր երեխայի համակարգիչը: Հաճախ ծնողները երեխայի զարգացման և ուսման մեջ հաջողությունների հասնելու համար հասանելի են դարձնում համացանցը՝ չմտածելով այնտեղի պարունակությունը զտելու մասին: Համացանցում եղած շատ նյութեր երեխաների համար չեն: Կա երեք տարբերակ ձեր երեխային վերահսկելու համար՝ 1. Խլել համակարգիչը, 2. նստել նրա կողքին և հետևել, թե ինչ է անում, 3. Օգտվել ծնողների վերահսկողական ծրագրերից: Ընտրեք ըստ ձեր ճաշակի:



ՍՏԵՂԾԱԳՈՐԾԱԲԱՐ ՄՈՏԵՑԵՔ ԳԱՂՏՆԱԲԱՌԵՐԻ ՍՏԵՂԾՄԱՆԸ

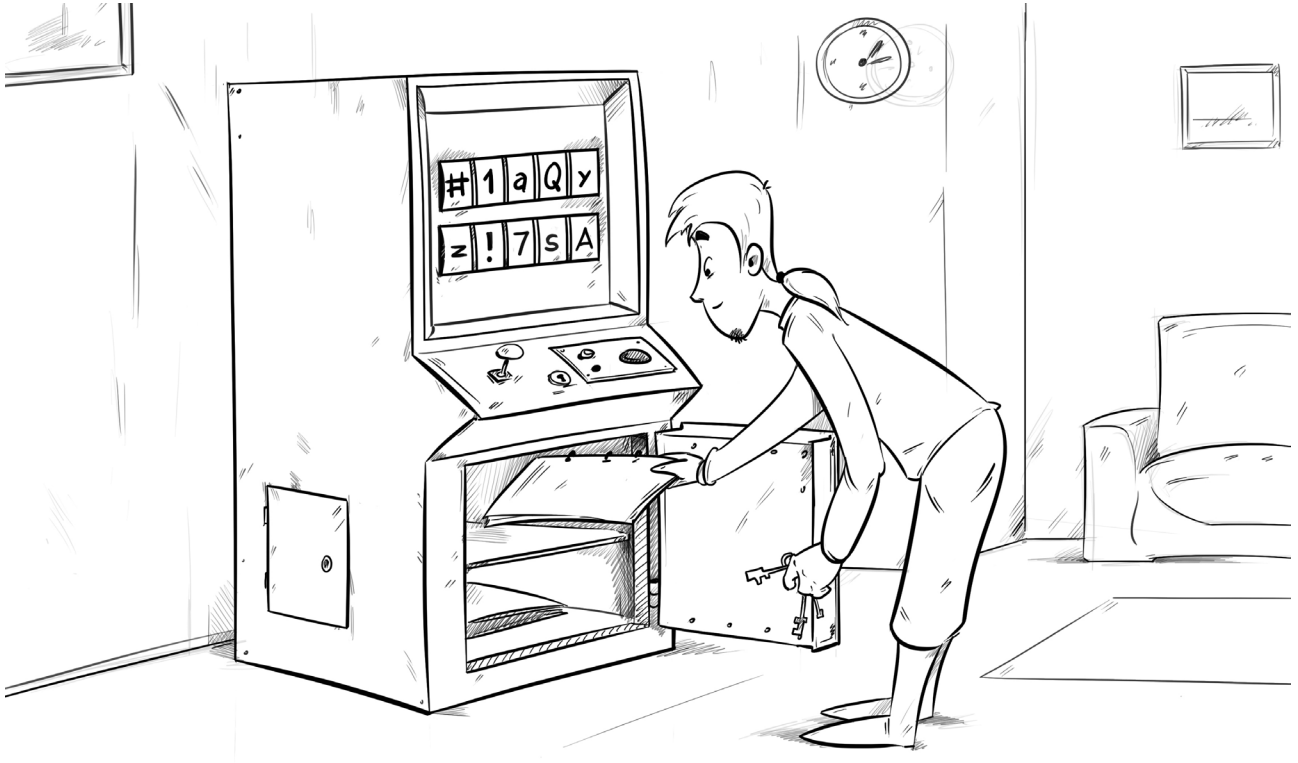
ԽՈՐՀՈՒՐԴ 13: **ԲԱՐԴ ԳԱՂՏՆԱԲԱՌ**

Ցանցահենները սկսում են գաղտնաբառն ընտրել օգտվելով հատուկ բառարաններից, որտեղ արձանագրված են միլիոնավոր գաղտնաբառեր, որոնք երբևէ օգտագործվել են: Շատ հնարավոր է, որ ձեր մտածած գաղտնաբառը նույնպես լինի այդ բառարանում: Ցանկալի չէ տարածված բառերը, կինոֆիլմերի վերնագրերը, երգերի տողերը, ձեր կատվի անունը, ծննդյան ամսաթիվը և այլ տեղեկություններ, որոնք կարելի է գտնել համացանցում կամ կռահել, օգտագործել որպես գաղտնաբառ:


...ԻՍԿԱՊԵՍ ԲԱՐԴ ԳԱՂՏՆԱԲԱՌԵՐ ՍՏԵՂԾԵՔ
ՄՈՒՏՔՆ
ԱՐԳԵԼՎԱԾ Է

ԽՈՐՀՈՒՐԴ 14: **ՀՈՒՍԱԼԻ ԳԱՂՏՆԱԲԱՌ**

Բարդ գաղտնաբառ ստեղծելու ամենահեշտ ձևը զուգորդումն է: Ընտրեք բառակապակցություն, որը զուգորդվում է ծառայության կամ կայքի հետ, գրեք այն լատինատառ, որոշ տեղերում ավելացրեք թվեր և հատուկ նշաններ, արդյունքում կունենաք երկար և հուսալի գաղտնաբառ: Այսպիսի գաղտնաբառը հեշտ է հիշել, քանի որ առաջին հայացքից տառերի, թվերի և նշանների անիմաստ թվացող համադրությունը ձեզ համար իմաստակիր է:



ՕԳՏԱԳՈՐԾԵՔ ՄԵՆԵՋԵՐՆԵՐ՝
ԳԱՂՏՆԱԲԱՌԵՐԻ ՍՏԵՂԾՄԱՆ ԵՎ ՊԱՀՊԱՆՄԱՆ ՀԱՄԱՐ

ԽՈՐՀՈՒՐԴ 15: **ԳԱՂՏՆԱԲԱՌԵՐԻ ՊԱՀՊԱՆՈՒՄԸ**

Որքան բարդ է գաղտնաբառը, այնքան դժվար է այն բացահայտել: Որքան պարզ է գաղտնաբառը, այնքան հեշտ է այն հիշել: Այսինքն գաղտնաբառը պետք է լինի և բարդ, և պարզ միաժամանակ՝ պարադոքս, որն ամեն մեկը չէ, որ կարող է լուծել: Եթե զուգորդումով գաղտնաբառ կազմելը ձեզ դուր չի գալիս՝ փորձեք օգտվել գաղտնաբառերի մենեջեր-ծրագրից: Այդ ծրագիրը կստեղծի ձեզ համար բարդ, յուրահատուկ գաղտնաբառեր առցանց-ծառայությունների, սոց. ցանցերի, հավելվածների և այլնի համար, իսկ հետո այդ գաղտնաբառերը կպահպանի ծածկագրված իր բազայում: Ձեզ կմնա ստեղծել գլխավոր գաղտնաբառը մենեջեր գաղտնաբառերի համար: Հիշեք, այն պետք է այնքան բարդ լինի, որ դժվար լինի բացահայտելը և այնքան պարզ, որ հեշտ լինի հիշելը:

**ԱՐԺԵՔԱՎՈՐ ՏՎՅԱԼՆԵՐԻ ԿՐԿՆՕՐԻՆԱԿԸ
ԿԱՐԵԼԻ Է ՏԵՂԱԴՐԵԼ ՀԵՌԱԿԱ ՊԱՀՈՑՈՒՄ**

ԽՈՐՀՈՒՐԴ 16: **ՊԱՀՈՒՍՏԱՅԻՆ ՊԱՏՃԵՆՈՒՄ**

Համակարգիչներն էլ «մահանում», նույնիսկ «հանկարծամահ» են լինում: Կորցնել «երկաթի կտորը»՝ նույնիսկ ամենաժամանակակիցը, այնքան ցավալի չէ, որքան ընտանեկան լուսանկարների արխիվի, դիպլոմային նախագծի կամ տարիներով հավաքած պորտֆոլիոյի կորուստը: Բարեբախտաբար այդ բոլորը կարելի է անվճար կամ ոչ թանկ վճարով տեղադրել խոշոր ընկերությանը պատկանող տվյալների մշակման աղետակայուն կենտրոնում: Ինքնուրույն կամ հատուկ ծրագրային ապահովման միջոցով ժամանակ առ ժամանակ կարելի է համակարգչի կամ սմարթֆոնի տվյալները կրկնօրինակել այդ կենտրոն, որպեսզի վթարի դեպքում այդ տվյալները լինեն ձեզ համար հասանելի: Այդպիսի պահոցները կոչվում են ամպ և այսօր մեծ տարածում ունեն:

...ԵՎ ԱՅԴ ԴԵՊՔՈՒՄ ՁԵՐ ՖԱՅԼԵՐԸ ԿԴԻՄԱՆԱՆ ՑԱՆԿԱՑԱԾ ԱՂԵՏԻ

ԽՈՐՀՈՒՐԴ 17: **ՏՎՅԱԼՆԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ**

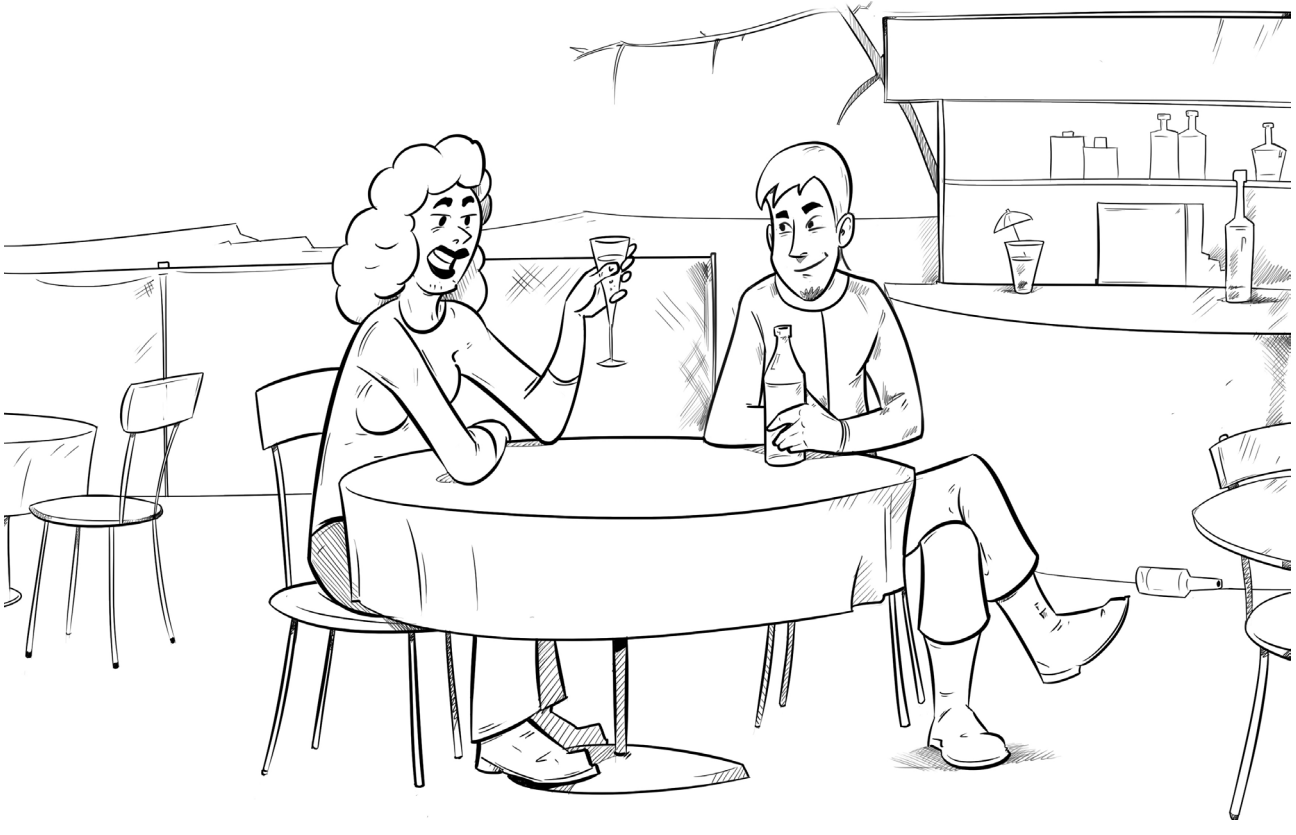
Եթե որևէ աղետի պատճառով մարդկությունը ոչնչանա, ապա հեռացված պահոցների շնորհիվ Երկիր մոլորակը ուսումնասիրող այլմոլորակայինները կհիանան երկրային զուգարանների և վերելակների ներքին հարդարումով, այդտեղ արված սելֆիներով, կլսեն Ջասթին Բիբերի երգերը և կկարդան միլիոնավոր գրառումներ, որոնք ամեն վայրկյան հայտնվում են համացանցում:

ՀԱՄԱՑԱՆՑՈՒՄ ԸՆԿԵՐԱՑԵՔ ՆՐԱՆՑ ՀԵՏ ՈՒՄ ԱՆՁԱՄԲ ՃԱՆԱՉՈՒՄ ԵՔ

ԽՈՐՀՈՒՐԴ 18: **ՍՏՈՒԳՎԱԾ ԾԱՆՈԹՈՒԹՅՈՒՆՆԵՐ**

«Friend» և «ընկեր» բառերի բառարանային նշանակությունը նույնն է: Բայց իրականում վիրտուալ ֆրենդներին պետք չէ որպես ընկեր ճանաչել: Մի բան է, երբ ցանցում ձեր ընկերներն են այն մարդիկ, որոնց դուք կյանքում ճանաչում եք, իսկ այլ բան է, երբ ցանցում ձեր ընկերներն են ուզում դառնալ ձեզ անծանոթ մարդիկ: Իրական կյանքում չափազանց ընկերասեր մարդու համար նոր «ընկերները» տարբեր անախորժություններ են ստեղծում՝ կոնֆլիկտային վիճակ ընտանիքում կամ կողոպուտ: Կիբեռտարածքում ձեզնով հետաքրքրվող անծանոթները կարող են լինել խաբեբաներ, մանկապիղծներ, վնասատու ծրագրեր կամ փոստաղբ (սպամ) տարածողներ:

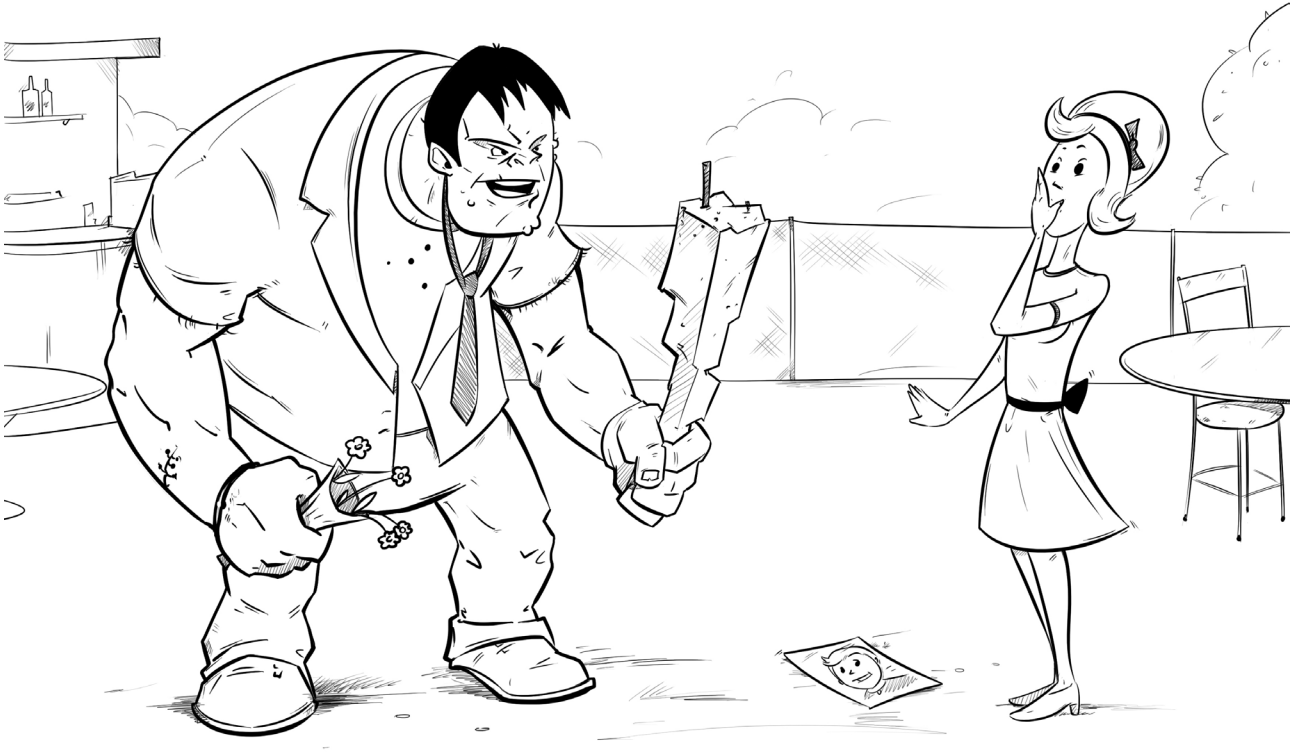
ՀԳՈՒՇԱՑԵՔ ԳԱՅԹԱԿՂԻՉ ԻՆՏԵՐՆԵՏ-ԳԵՂԵՑԿՈՒՀԻՆԵՐԻՑ



ԽՈՐՀՈՒՐԴ 19: **ԳԱՅԹԱԿՂՈՒՉ ԳԵՂԵՑԿՈՒՀԻՆԵՐ**

Ինտերնետ-ծանոթությունները նման են բազմաթիվ անհայտներով հավասարմանը: Համացանցում գործընկերը ցույց կտա ձեզ այն, ինչ ուզում է ցույց տալ: Երկար ժամանակ նամակագրություն ունենալով նրա հետ, դուք չեք կարող ասել, թե ով էկրանի այն կողմում: Էկրանի մյուս կողմում գտնվող անծանոթ մարդու վարքագիծը բացատրել հնարավոր չէ: Չարյաց փոքրագույնն է, եթե ինտերնետ-գեղեցկուհին իրականում գեղեցկուհի չլինի: Հնարավոր է, որ կեղծ լինեն ընտանեկան կացության մասին տվյալները, տարիքը և նույնիսկ սեռային պատկանելությունը:

...ԻՆՏԵՐՆԵՏ-ԳԵՂԵՑԿՈՒՀԻՆԵՐԸ ՄԻՇՏ ՉԷ, ՈՐ ԱՐԴԱՐԱՑՆՈՒՄ ԵՆ ՀՈՒՅՍԵՐԸ



ԽՈՐՀՈՒՐԴ 20: **ԱՆՑԱՆԿԱԼԻ ԿԱՊԵՐ**

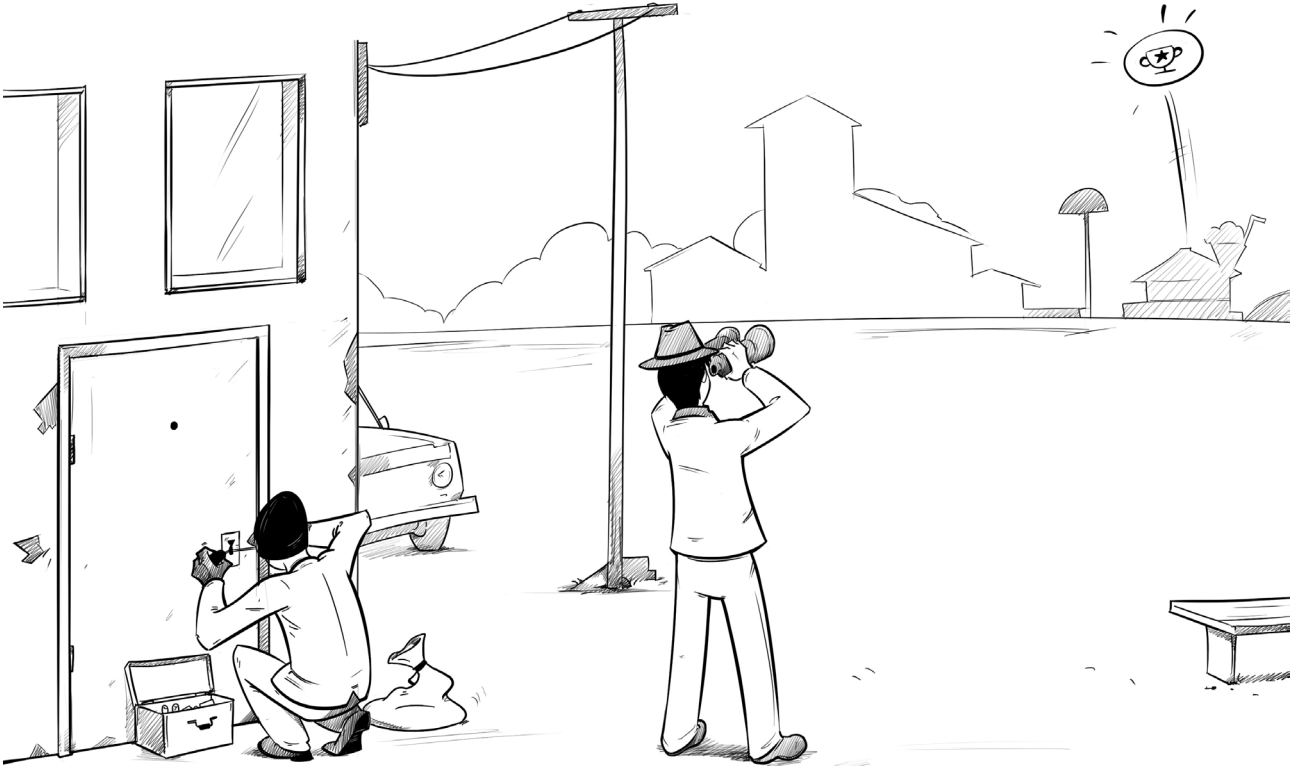
Գիտակցված խաբեության կարող են գնալ և իգական, և արական սեռի ներկայացուցիչները: Մեծամասամբ շտկումներ են անում լուսանկարներում կամ ծննդյան թիվ են փոխում: Ավելի վատ է, երբ երկրորդ կեսը խաբեբա է: Այդ դեպքում դուք կկորցնեք ոչ միայն ձեր ժամանակը, այլ հնարավոր է և ձեր փողերը, առողջությունը և նույնիսկ՝ կյանքը: Բայց համացանցում լավ մարդիկ ավելի շատ են, պետք է ուշադիր լինեն զրուցակից ընտրելիս, իսկ անձնական ծանոթությունը մի փոքր հետաձգել:

ԾՆՈՂԱԿԱՆ ՎԵՐԱՀՍԿՈՂՈՒԹՅՈՒՆԸ ՊԱՇՏՊԱՆՈՒՄ Է ԱՆՑԱՆԿԱԼԻ ՇՓՈՒՄԻՑ

ԽՈՐՀՈՒՐԴ 21: **ՎՏԱՆԳԱՎՈՐ ԸՆԿԵՐՆԵՐ**

Մեծահասակ մարդը կարող է համացանցում չգնալ անցանկալի ծանոթությունների, իսկ երեխան այդքան գիտակից չէ: Անծանոթ օգտատիրոջ հետ շփումը կարող է ոչ միայն տհաճ լինել, այլև վտանգավոր: Երեխան չի գիտակցում, որ ոմն VinnieThePooh1967 մանկապիղծ է, որը ցանկանում է հանդիպել և առանձնանալ երեխայի հետ: Ծնողը պետք է հետևի և զտի սոց. ցանցերում և հաղորդագրություններում հայտնվող ծանոթությունների առաջարկները:

ԵՐԲ ԴՈՒՔ ԳՐԱՆՑՎՈՒՄ ԵՔ ՍՐՃԱՐԱՆՈՒՄ,
ԱՅԴ ՄԱՍԻՆ ՏԵՂԵԿԱՆՈՒՄ ԵՆ ՈՉ ՄԻԱՅՆ ՁԵՐ ԸՆԿԵՐՆԵՐԸ



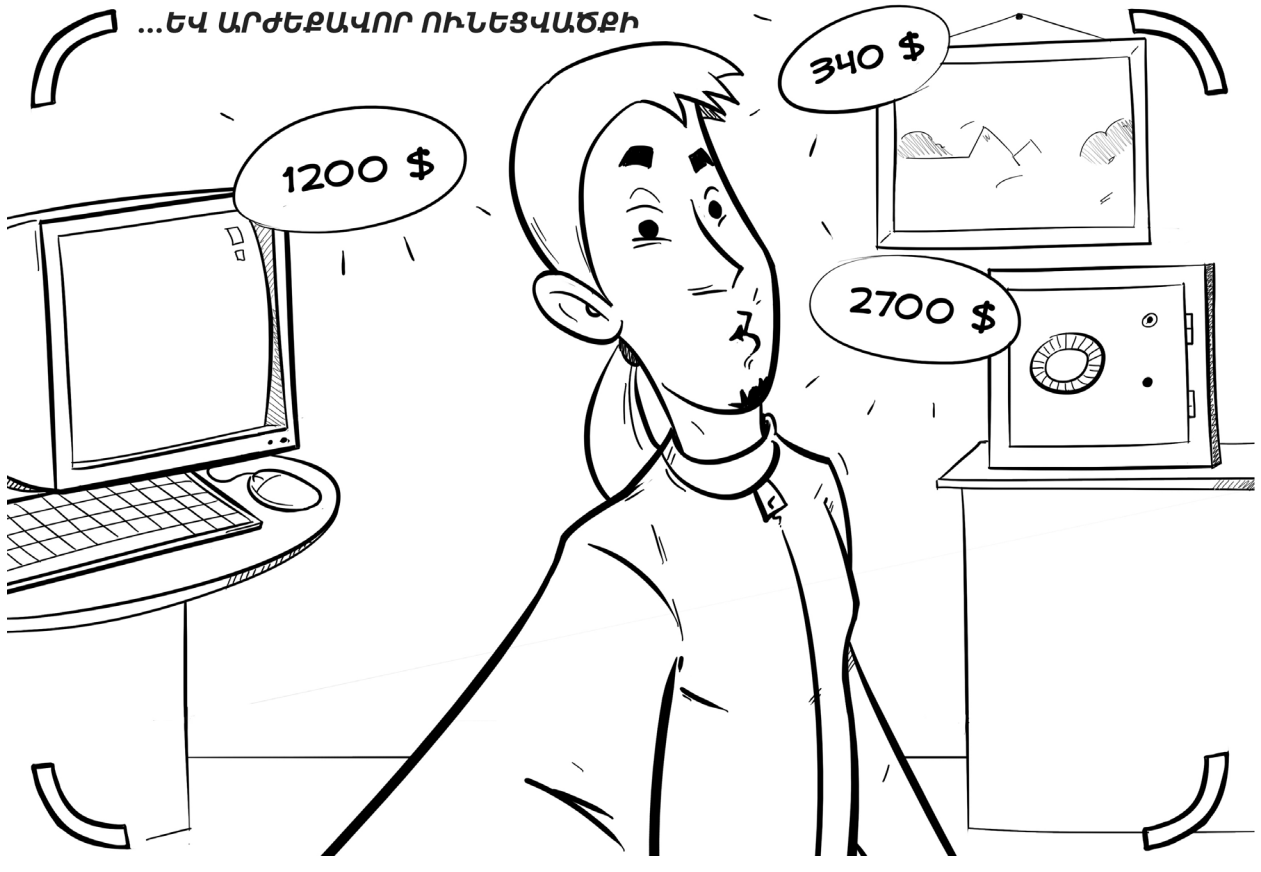
ԽՈՐՀՈՒՐԴ 22: **ՎԻՐՏՈՒԱԼ ԼՐՏԵՍՈՒԹՅՈՒՆ**

Եթե հանցագործները պատրաստվում են ձեզ կողոպտել, ապա նրանք սկսում են հետևել ձեզ, ձեր բնակարանին, ամառանոցին կամ մեքենային: Բայց լրտեսելու այս ձևը իր տեղը զիջում է այլ ձևերի: Այսօր ունենք տեխնոլոգիապես կատարելագործված գողեր, որոնք հեշտությամբ կարող են սոց. ցանցերում բաժանորդագրվել ձեր նորացումներին: Այս մարդկանց ձեռնտու է, որ օգտատերը սոց. ցանցում հայտնում է իր գտնվելու վայրի մասին: Հերթական անգամ ձեր տեղը նշելուց առաջ մտածեք, թե «Odnoklassniki», «Vkontakte» կամ «Facebook» ցանցերում ձեր «ընկերներից» քանիսն են իսկապես ձեր ընկերները:

ԿԱՐԻՔ ՉԿԱ ՑԱՆՑՈՒՄ ՏԵՂԱԴՐԵԼ ԱՆՁՆԱԿԱՆ ՓԱՍՏԱԹՂԹԵՐԻ ԼՈՒՍԱՆԿԱՐՆԵՐԸ

ԽՈՐՀՈՒՐԴ 23: **ՊԱՀՊԱՆԵՔ ՓԱՍՏԱԹՂԹԵՐԸ**

Մեր ինֆորմացիոն դարում շատերը ապրում են անթաքույց՝ մոտիկ ընկերներին, անհայտ «ֆոլովերներին» և «ֆրենդներին» ցուցադրելով վերջին լուսանկարները, տեսահոլովակները, մանրամասն պատմում են օրվա անելիքների մասին: Ձեր ընկերները ձեր անկեղծ տեղեկատվությանը մեծ ուշադրություն չեն դարձնի, իսկ թշնամիները կհետաքրքրվեն դրանով: Փորփրելով համացանցը հանցագործը կարող է արժեքավոր ինֆորմացիա գտնել իր «զոհի» մասին, ինչը կարող է բավարար լինել կեղծ փաստաթղթեր պատրաստելու համար: Դատարանում տուժողը հավանաբար կկարողանա ապացուցել, որ ինքը չի այդ չորս վարկը վերցրել, բայց տհաճ զգացողությունը երկար ժամանակ կմնա:


...ԵՎ ԱՐԺԵՔԱՎՈՐ ՈՒՆԵՑՎԱԾՔԻ
1200 $
340 $
2700 $

ԽՈՐՀՈՒՐԴ 24: **ՃՈԽ ԿՅԱՆՔ**

Համացանցի զարգացման շնորհիվ հանցագործներին այլևս պետք չեն ուղղորդողներ: Մարդիկ այսօր համացանցում տեղադրում են իրենց ճոխ բնակարանի, թանկարժեք մեքենայի կամ նոութբուքի լուսանկարները և հայտնում են, որ հաջորդ շաբաթ իրենց երկրորդ կեսի հետ մեկնելու են հանգստի, այսինքն՝ նրանց ողջ հարստությունը մնալու է առանց հսկողության: Հանցագործ աշխարհի ներկայացուցիչները ունակ են օգտվել սոց. ցանցերից, մանավանդ, որ դրանք նյութական օգուտ կարող են բերել նրանց: Թե համացանցում, թե նրանից դուրս համեստ լինելը անվտանգ է:

ՀԱՆՑԱԳՈՐԾՆԵՐԸ ՊԱՏՐԱՍՏ ԵՆ ԳՈՂԱՆԱԼ ԱՆԳԱՄ ՆԵՐԽԱՂԱՅԻՆ ԳՈՒՅՔԸ

ԽՈՐՀՈՒՐԴ 25: **ԽԱՂԻ ՏՎՅԱԼՆԵՐԻ ԳՈՂՈՒԹՅՈՒՆ**

Ինչ-որ մեկը կոտրել է ձեր հաշվագրանցումը առցանց խաղերում, գողացել է ձեր թուրը, սիրելի տանկը և իններորդ մակարդակի խոզուկին: Զարմանալ պետք չէ, շուկայի օրենքը ասում է՝ ամեն իր արժե այնքան, որքան նրա համար պատրաստ են վճարել: Համակարգչային խաղերում հաշվագրառումը և մեծ տարածում ունեցող խաղերի առարկաները շատ արժեքավոր են: Ձեզնից գողանում են ոչ թե պիքսելներ, այլ ձեր ժամանակը և աշխատանքը: Եթե դուք արժևորում եք դրանք, ուրեմն մտածեք թվայնացված ձեր ունեցվածքի համարժեք պաշտպանության մասին: Սկսեք գաղտնաբառերի բարդացումից, նույնն արեք էլեկտրոնային փոստի հետ, որը կցագրված է խաղային հաշվագրառումներին:

ՈՒՇԱԴԻՐ ՁԵՎԱԿԵՐՊԵՔ ՈՐՈՆՈՂԱԿԱՆ ՀԱՐՑՈՒՄՆԵՐԸ

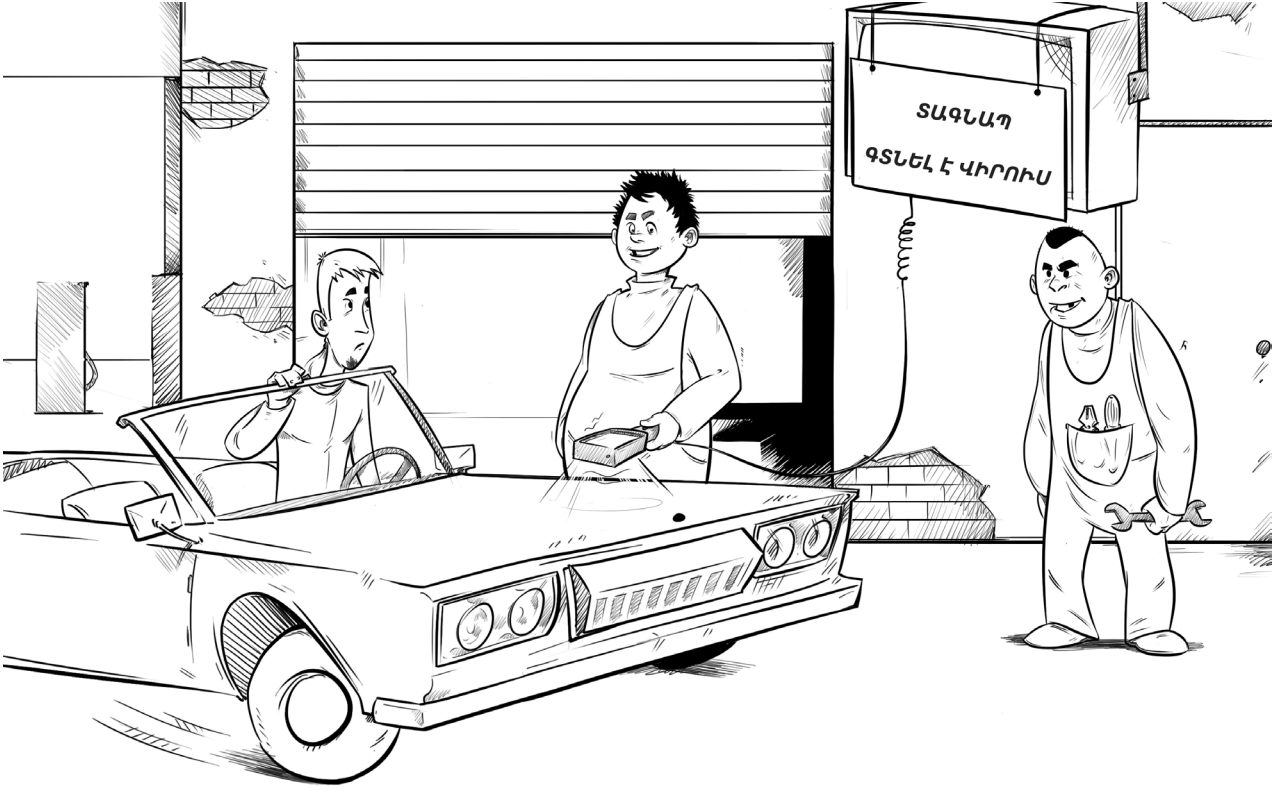
ԽՈՐՀՈՒՐԴ 26: ՃԻՇՏ ՄՈՏԵՑՈՒՄ ՈՐՈՆՈՂԱԿԱՆ ՀԱՐՑՈՒՄՆԵՐԻՆ

Մարդուն հատուկ է սխալվելը: Մարդը կարող է սխալվել որոնողական հարցումներ գրելիս: Որոնողական համակարգերը արդեն սովորել են հուշել օգտատերերին ճիշտ տարբերակը: Այդ համակարգերի դեմ գործում են կիբեռհանցագործության բնագավառի լավագույն ներկայացուցիչները, որոնք մտածում են, թե որ հարցումներին առաջարկել իրենց ձեռնտու պատասխանը: Հարցումը գրելիս հնարավոր է, որ ինչ-որ մի տառ բաց թողնեք կամ սխալ գրեք, այդ դեպքում դուք չեք գտնի այն, ինչ փնտրում էիք: Բայց հնարավոր է, որ ձեզ առաջարկվի ձեր որոնած էջի նման էջ, սակայն այն լինի վնասատու: Այս դեպքում հնարավոր է, որ ձեր համակարգիչը վարակվի, դուք կորցնեք ձեր անձնական տվյալները, նաև՝ փողերը:

ՈՒՇԱԴՐՈՒԹՅՈՒՆ ԴԱՐՁՐԵՔ ԿԱՅՔԻ ՀԱՍՑԵԻՆ

ԽՈՐՀՈՒՐԴ 27: **ԿԵՂԾ ԿԱՅՔԵՐ**

Ֆիշինգը կիբեռհանցագործների սիրած մարտավարությունն է: Դժվար չէ ստեղծել կայք, որի արտաքին տեսքը նման է հանրածանոթ կայքին, օրինակ՝ «Одноклассник» կամ «Facebook» կայքին, իսկ հետո տեղադրել այն մի հասցեով, որը իսկական հասցեից տարբերվում է մի քանի տառով: Դրանից հետո մեծ թվով օգտատերերի կայքի անունից ուղարկում են նամակներ՝ խնդրելով փոխել , օրինակ, «Одноклассники» գաղտնաբառը և հղում անել կեղծ կայքին: Եթե հավատաք խաբեբաներին՝ ձեր էջը սոց. ցանցում այլևս ձերը չի լինի: Հակավիրուսային ընկերությունները մշտապես փնտրում և արգելափակում են ֆիշինգային էջերը, բայց օգտատերերն էլ պետք է ուշադիր լինեն:

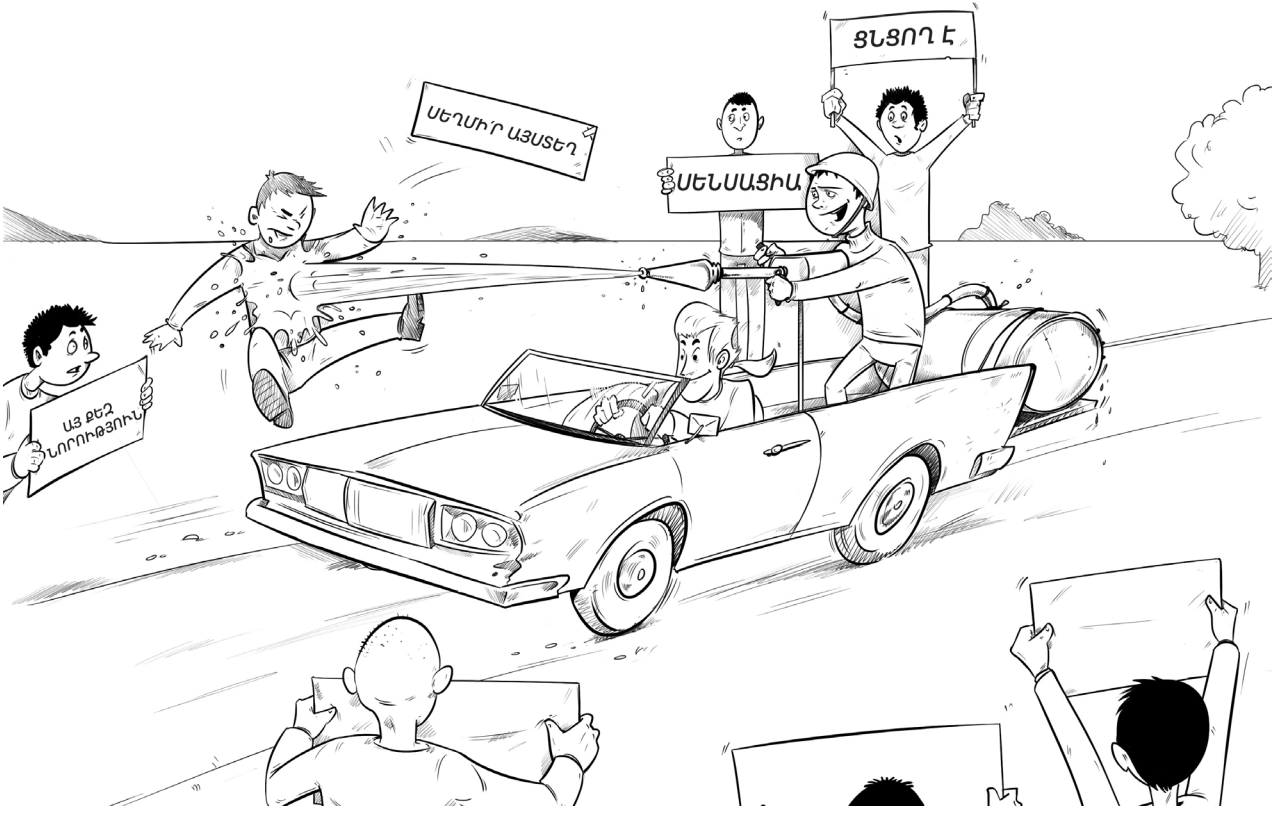


ՄԻ ՀԱՎԱՏԱՑԵՔ ՀԱՄԱԿԱՐԳՉԻ ՎԱՐԱԿՎԱԾՈՒԹՅԱՆ ՄԱՍԻՆ ԿԱՅՔԵՐԻ ՈՒՂԱՐԿԱԾ ՀԱՂՈՐԴԱԳՐՈՒԹՅՈՒՆՆԵՐԻՆ

ԽՈՐՀՈՒՐԴ 28: **ՍՈՒՏ ԾԱՆՈՒՑՈՒՄՆԵՐ**

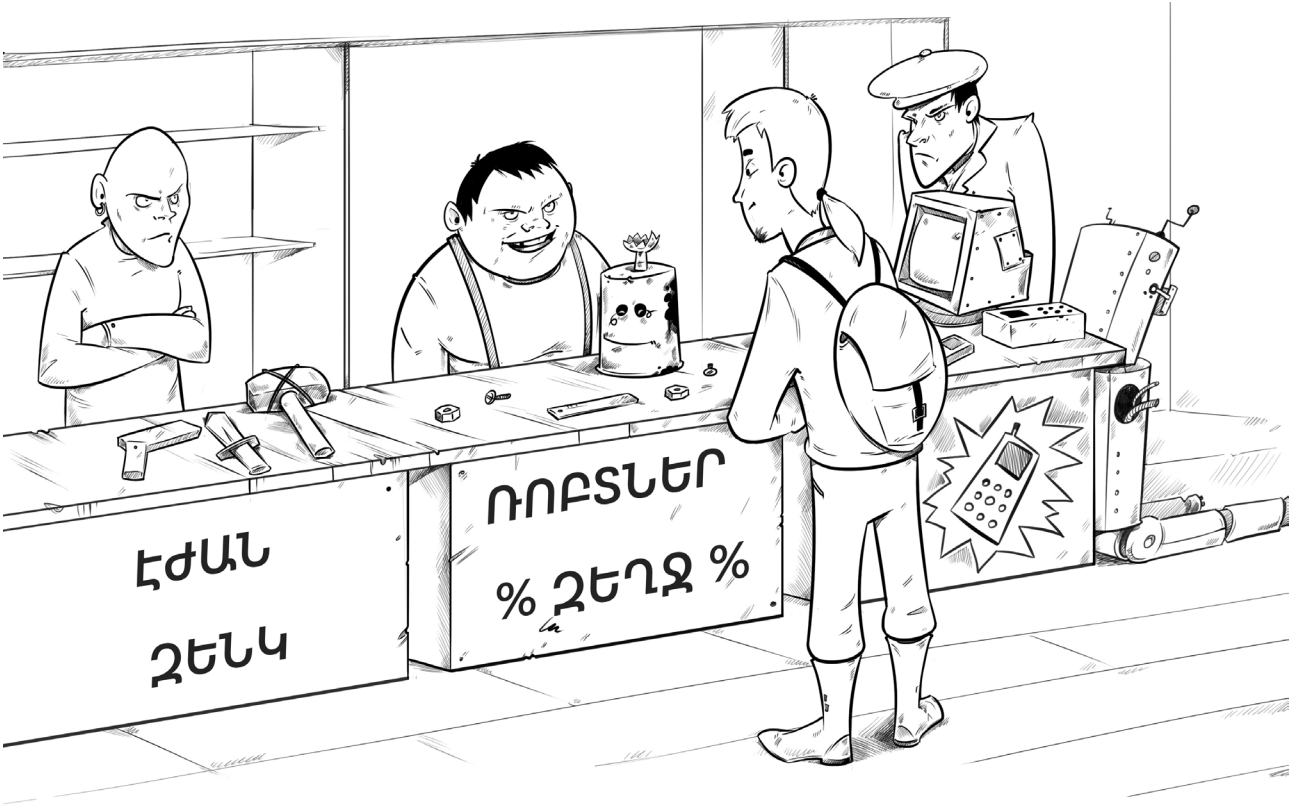
Ներբեռնելով նոր կայքը և տեսնելով գույնզգույն վահանակ, որը զգուշացնում է ձեզ, որ ձեր համակարգչում կան վիրուսներ, մի վախեցեք և մի շտապեք համաձայնվել այն ամենին, ինչ ձեզ առաջարկում է վահանակը: Ի՞նչպես կարող է վահանակը իմանալ, որ ձեր համակարգչում կան վիրուսներ: Այսպես փորձում են ձեզ ստիպել ներբեռնել «հրաշք» հակավիրուսային ծրագիր, և հենց այդ ժամանակ էլ վիրուսները կհայտնվեն ձեր համակարգչում: Այսպիսի վահանակների միջոցով տարածվում են վնասատու ծրագրային ապահովումները: Ճիշտ կլինի փակել վահանակը և կայքը՝ ոչ մի լավ բան այնտեղ չեք գտնի:

ԳՈՎԱԶԴԱՅԻՆ ՎԱՀԱՆԱԿՆԵՐԸ ՔՈՂԱՐԿՈՂ ԾՐԱԳԻՐԸ ԿԱԶԱՏԻ ՎՏԱՆԳԱՎՈՐ ԳԱՅԹԱԿՂՈՒԹՅՈՒՆՆԵՐԻՑ



ԽՈՐՀՈՒՐԴ 29: ՀԱՄԱՑԱՆՑՆ ԱՌԱՆՑ ԳՈՎԱԶԴԱՅԻՆ ՎԱՀԱՆԱԿՆԵՐԻ

Գիտնականները (երևի բրիտանացի) ապացուցել են, որ գովազդը ազդում է նույնիսկ նրանց վրա, ովքեր գովազդին ուշադրություն չեն դարձնում: Նշանակում է, որ դուք, որքան հնարավոր է արագ, պետք է ազատվեք գովազդային վահանակներից, որոնք լինում են կայքերում և զբաղեցնում են բրաուզերի պատուհանի մեծ մասը, իսկ «պոպ-ապ» կոչվող վահանակները քողարկում են ամբողջ պատուհանը: Գովազդի զոհը չդառնալու համար պետք է տեղադրել հատուկ ծրագիր, որը փակում է գովազդային վահանակները: Այդ ծրագրերը լինում են ինչպես առանձին հավելվածների, այնպես էլ բրաուզերների լրացումների տեսքով: Ուշադիր եղեք, որպեսզի հակագովազդային հավելվածի փոխարեն չտեղադրեք գովազդային հավելված: Պետք է հիշել, որ գովազդը հնարավոր է դարձնում կայքերի անվճար լինելը, այդ պատճառով էլ հակագովազադային որոշ հավելվածներ հնարավոր են դարձնում որոշ գովազդների դիտումը:



ԱՅՑԵԼԵՔ ՄԻԱՅՆ ՀԱՆՐԱՃԱՆԱՉ, ՍՏՈՒԳՎԱԾ ԻՆՏԵՐՆԵՏ-ԽԱՆՈՒԹՆԵՐԸ

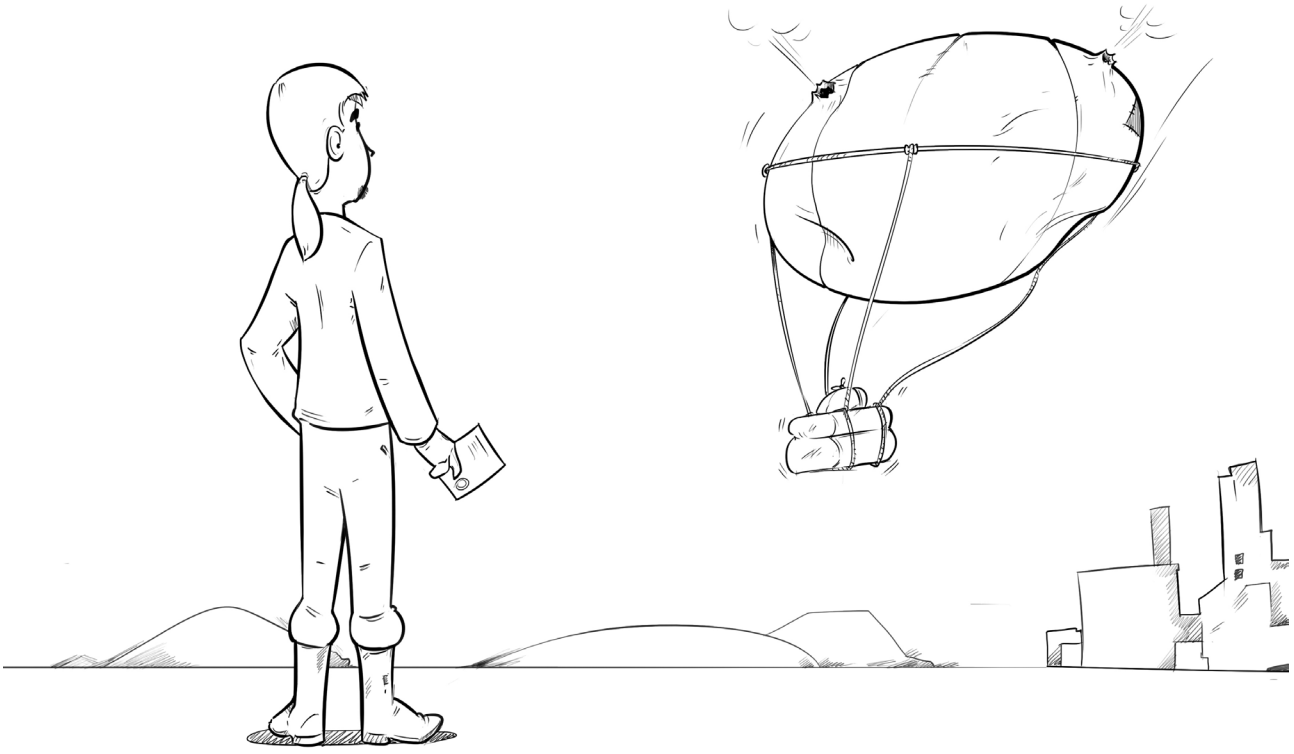
ԽՈՐՀՈՒՐԴ 30: **ԿԵՂԾ ԽԱՆՈՒԹՆԵՐ**

Հանցագործի աշխատանքը բարդ չէ՝ պատճենել ինտերնետ-խանութի պարունակությունը, մի քիչ փոփոխել, տեղադրել իր կայքի հասցեում (դոմեն), մի քիչ գովազդել այդ ապրանքը: Ինտերնետ-խանութի հաճախորդներից հանցագործը կիմանա նրանց անունները, հասցեները, բանկային քարտերի տվյալները: Իսկ եթե ապրանքի համար վճարման էջին տրված լինեն այն տարբերակները, որոնց միջոցով հնարավոր է գումարը փոխանցել էլեկտրոնային դրամապանակին, ապա կսկսվի դրամի մեծ հոսք: Այս բոլորը արվում է այնքան պարզ և հեշտ, որ վախենալու է ինչ-որ բան համացանցով գնել: Հանցագործների ծուղակը չընկնելու համար կան մի քանի կանոններ: Դրանցից մեկն այն է, որ չարժե գնում կատարել այնտեղ, որտեղ որևէ մեկին որևէ բան չի հաջողվել գնել: Օգտվեք ստուգված, հայտնի խանութներից:

...ՈՐՈՆՔ ՈՒՆԵՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԱՎԱՍՏԱԳԻՐ

ԽՈՐՀՈՒՐԴ 31: **ԱՆՎՏԱՆԳ ԱՌԵՎՏՈՒՐ**

Ճիշտ ինտերնետ-խանութը օգտագործում է պաշտպանված HTTPS հաղորդակարգը հավաստագրով, որը ստորագրել է օրինական հաստատող կենտրոնը: Համոզվելու համար պետք է նայել հասցեի տողին: Եթե տեսնում եք «https://...» և վառվում է ծածկագրված նկար (սովորաբար կանաչ կողպեք) ուրեմն դուք ճիշտ տեղում եք: HTTPS պաշտպանում է բազմաթիվ վտանգներից՝ սեփական կայքի նենգափոխումից, հաղորդվող ինֆորմացիայի անօրինական ճանապարհով ձեռքբերումից, ուղարկվող և ստացվող տվյալների փոփոխումից:



ԵՎ ՄԻ ՄՈՌԱՑԵՔ ՃՇՏԵԼ ԱՌԱՔՄԱՆ ՀՆԱՐԱՎՈՐՈՒԹՅՈՒՆԸ ԵՎ ԴՐԱ ԱՐԺԵՔԸ

ԽՈՐՀՈՒՐԴ 32: **ԽԱԲԵԲԱՆԵՐԸ ԱՌԱՔՄԱՆ ՈԼՈՐՏՈՒՄ**

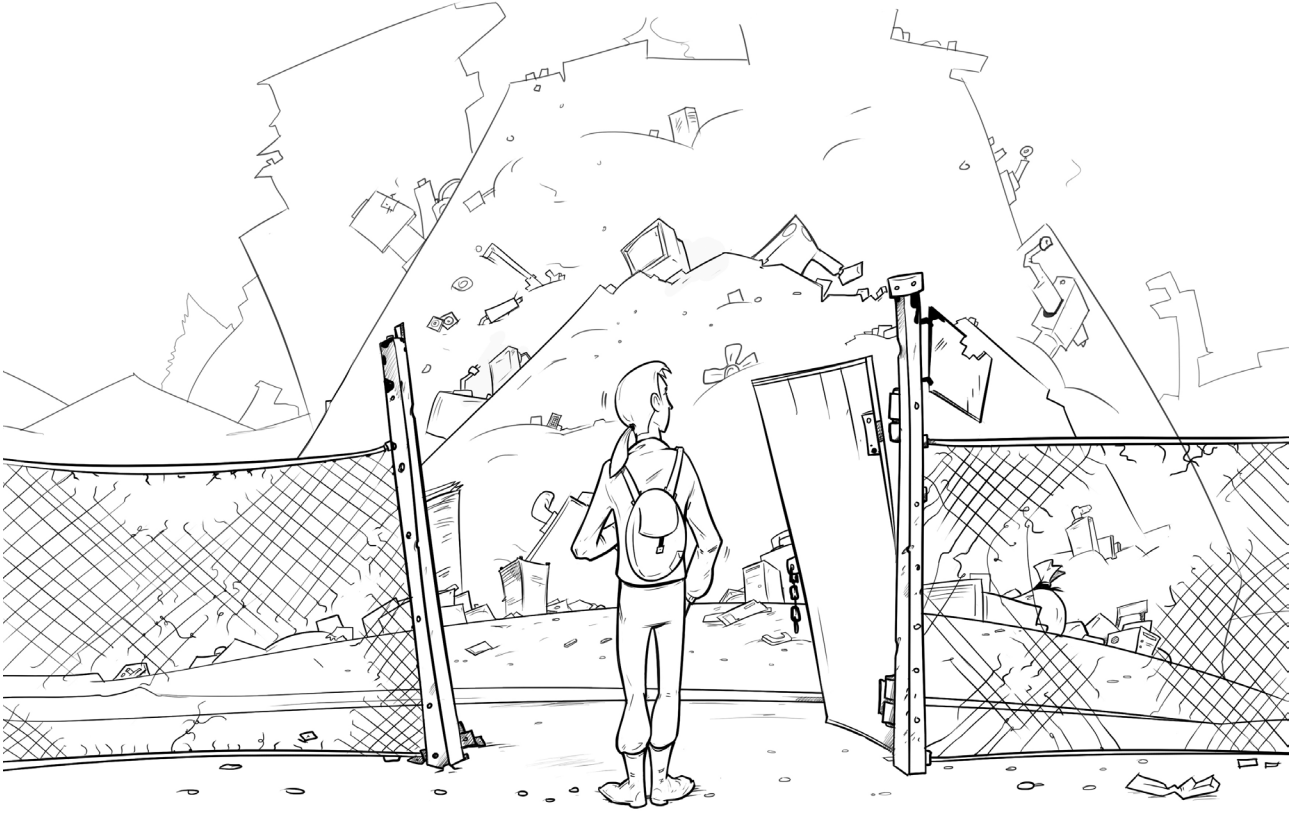
Շատերն են հայտնվել այն վիճակում, երբ ինտերնետ-խանութում ապրանք պատվիրելուց հետո այն մի դեպքում բարձվել է, մյուս դեպքում տրվել է առաքիչին, մի այլ դեպքում էլ պահեստում չի եղել: Այս դեպքերը կարող են լինել խանութի առևտրային համակարգի խափանման պատճառով, բայց հնարավոր է, որ լինեն հանցագործների հնարքները, քանի որ նրանք որևէ մեկին որևէ բան վաճառել չեն պատրաստվում, այլ հավաքում են հնարավոր զոհերի տվյալները: Եթե ապրանքի համար արդեն վճարված է բանկային քարտով կամ էլեկտրոնային դրամապանակի միջոցով, վերը նկարագրված դեպքերը մեծ անհանգստություն կպատճառեն պատվիրատուին: Զարմանալի չէ, որ Հայաստանում վճարման ամենատարածված մեթոդը առաքիչին առձեռն վճարումն է՝ ապրանքը ստանալուց և ստուգելուց հետո:

ԵԹԵ ՁԵՐ ԲԱՆԿԱՅԻՆ ՔԱՐՏԸ ՉԱՍԱՆԵԼԻ Է ՁԵՐ ԵՐԵԽԱՅԻՆ,
ԱՊԱ ՆԱ ԱՆԱՐԳԵԼ ԱՌԵՎՏՈՒՐ ԿԱՆԻ

ԽՈՐՀՈՒՐԴ 33: **ԲԱՆԿԱՅԻՆ ՔԱՐՏԵՐԸ ԵՎ ԵՐԵԽԱՆԵՐԸ**

Ինտերնետում արված գնումների համար բանկային քարտով վճարելը շատ հարմար է, մանավանդ, որ խանութը թույլ է տալիս քարտը կցել հաշվագրանցմանը և ամեն անգամ տվյալները չբեռնել: Մի զարմացեք, եթե անծանոթ գնումների համար հաշիվներ ստանաք, օրինակ՝ Արամ MP3-ի բոլոր սկավառակների հավաքածուի համար: Այս փաստը խոսում է այն մասին, որ ձեր երեխաները սովորել են օգտվել ձեր բանկային քարտից և կարողանում են օգտվել ինտերնետ-խանութից: Նույնիսկ սովորական խանութներում քարտով վճարելիս վաճառողները միշտ չէ, որ ձեր փաստաթղթերն են հարցնում, իսկ համացանցում կան բազմաթիվ ծառայություններ, որոնք ընդունում են քարտերը առանց լրացուցիչ գաղտնաբառերի և ծածկագրերի: Մինչև երեխաները կդառնան որոշակի տարիքի՝ ցանկալի է քարտերը նրանցից պահել:

ՏՈՐԵՆՏ-ՏՐԵԿԵՐԸ ՕԳՏԱԿԱՐ ԻՆՖՈՐՄԱՑԻԱՅԻ ՇՏԵՄԱՐԱՆ



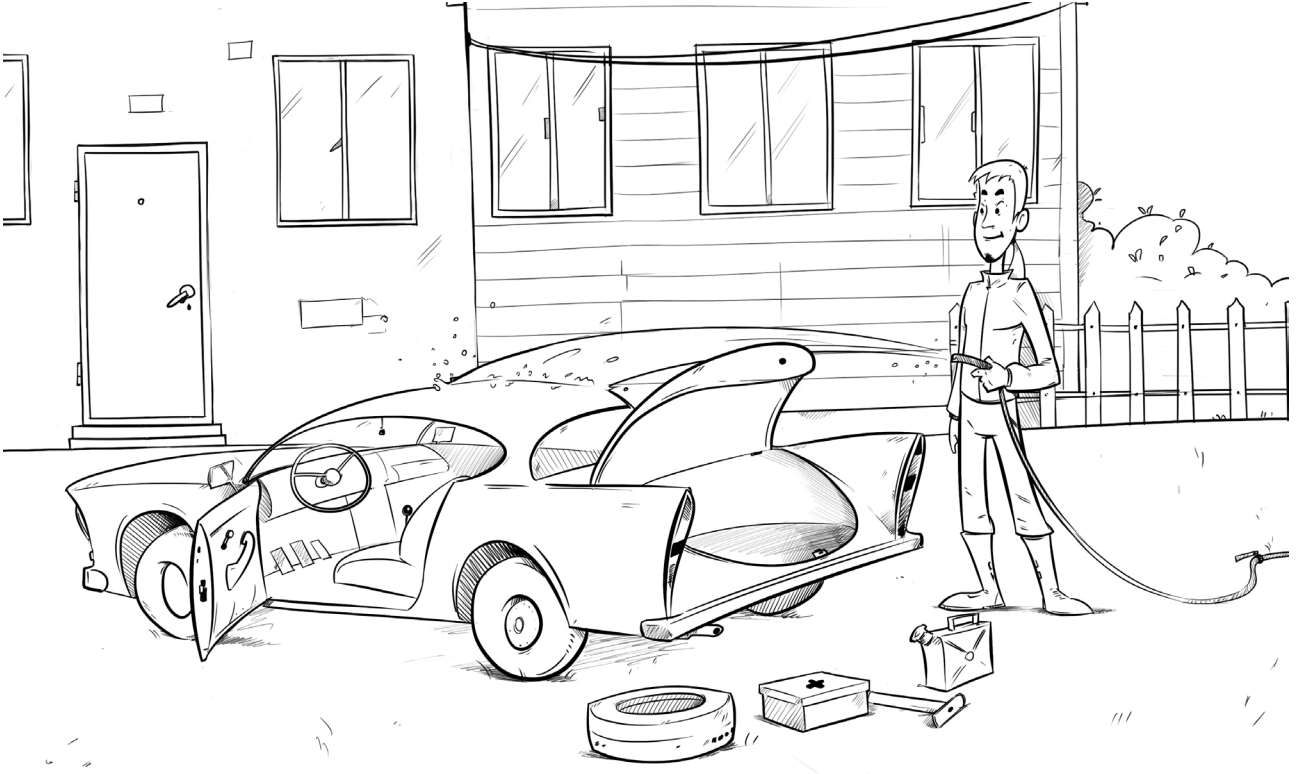
ԽՈՐՀՈՒՐԴ 34: **ՖԱՅԼԵՐԻ ՊԱՀԵՍՏ**

Տորենտ-տրեկերը հղումների քարտարան է, որտեղ ֆայլերի անվճար փոխանակման սիրահարները տեղադրում են հղումներ օգտակար ծրագրեր, կինոնկարներ, խաղեր, գրքեր և շատ այլ բաներ ներբեռնելու համար: Անհրաժեշտ ֆայլի ներբեռնումը կտարվում է հատուկ ծրագրի (տորենտ-հաճախորդ) միջոցով, ընդ որում, ֆայլը ներբեռնվում է տորենտ-տրեկերի մի քանի օգտատերերի համակարգիչներից: Այդ օգտատերերը վաղօրոք ներբեռնել էին այդ ֆայլը: Տրեկերում կարելի է գտնել կոմերցիոն ծրագրի կեղծ պատճեն, հոլիվուդյան նորագույն կինոնկարի պատճեն, ինչ-որ նյութ մեծահասակների համար և նույնիսկ անօրինական բաներ: Եվրոպայի որոշ երկրներում տորենտ-տրեկերի ակտիվ օգտատերերը հայտնվել են իրավապահների ուշադրության կենտրոնում, իսկ Ռուսաստանում այդպիսի ռեսուրսները արգելափակում է Ռուսաստանի վերահսկողության կոմիտեն: Ակնհայտ են անվճար ինչ-որ բան ստանալու գործի արժեքավոր և թերի կողմերը:

... ԵՎ ՎՆԱՍԱՏՈՒ ԾՐԱԳՐԵՐԻ

ԽՈՐՀՈՒՐԴ 35: **ՏՈՐԵՆՏՆԵՐԻ ՎՏԱՆԳՆԵՐԸ**

Տորենտ-տրեկերն ունի նաև մութ կողմ: Յուրաքանչյուր այդպիսի կայք ունի հղումներ տարբեր ֆայլերի բազմաթիվ տերաբայթերի վրա, ընդ որում տեղադրել որևէ նորույթ կարող է ցանկացած մեկը: Այդ պատճառով որևէ բան այդտեղից ներբեռնելիս ինքներդ ձեզ հարցրեք՝ դուք վստահում եք այդ ոմն մեկին: Գեղեցիկ ձևավորված բաշխումը կարող է պարունակել տրոյան ծրագիր, որն ակնթարթորեն կդատարկի ձեր բանկային հաշիվը կամ կարգելափակի համակարգիչը և հետո էլ արգելքը բացելու համար փրկագին կպահանջի: Կիբեռհանցագործների համար ցանկացած տորենտ-տրեկեր հարմար, արագ և անանուն միջոց է վնասատու ծրագրեր տարածելու համար: Ցավոք, տորենտ-տրեկերի օգտատերերին դա չի վախեցնում:



ԳՈՐԾԸ ԱՆԵԼՈՒՑ ՉԵՏՈ ՄԱՔՐԵՔ ՔՈՒԿԻՆԵՐԸ

ԽՈՐՀՈՒՐԴ 36: **ՄԱՔՈՒՐ ԲՐԱՈՒԶԵՐ**

Բավական է, որ մտնեք բանկի կայքը, իսկույն տարբեր կայքերում հայտնվում են վահանակներ, որոնց վրա գրված են առաջարկներ ձեռնտու ներդրումների և մատչելի վարկերի մասին: Ոչ մի կախարդանք չկա, պատճառը «cookie»-ն են՝ տեքստային փոքր ֆայլերը, որոնք անհրաժեշտ են կայքերին, որպեսզի հիշեն օգտատերերին և նրանց նախընտրությունները: Բայց երրորդ կողմն էլ կարող է օգտվել դրանցից՝ համացանցում օգտատիրոջ գործողություններին հետևելու համար: Գովազդային վահանակների ցանցերը հենց այդպես էլ վարվում են: Ամենատհաճն այն է, որ ֆայլերը գողացող հանցագործները կարող են հանդես գալ ձեր անունից՝ չիմանալով գաղտնաբառը և կայքում հաշվագրանցման ձեր ծածկագիրը: «Cookie»-ները ձեր բրաուզերում կարող են «ապրել» տարիներով: Հասկանալի է, որ նրանցից ժամանակին պետք է ազատվել, իսկ ժամանակակից բրաուզերներն ունեն «cookie» հեռացնելու ֆունկցիան:

ԲՐԱՈՒԶԵՐԻ ԱՌԱՆՁՆԱՑՎԱԾ ՌԵԺԻՄԸ ԿԹԱՔՑՆԻ ՀԱՐՑՈՒՄՆԵՐԸ ԵՎ ԱՅՑԵԼՈՒԹՅՈՒՆՆԵՐԻ ՊԱՏՄՈՒԹՅՈՒՆԸ

ԽՈՐՀՈՒՐԴ 37: **ԱՌԱՆՁՆԱՑՎԱԾ ԻՆՏԵՐՆԵՏ**

Մենք չենք հարցնում, թե ինչով եք զբաղվում համացանցում և ուրիշներին էլ խորհուրդ չենք տալիս հետաքրքրվել դրանով, ամեն մեկին էլ պետք է անձնական տարածք՝ թեկուզ վիրտուալ: Բայց ձեր «cookie» և ձեր այցելած կայքերի պատմությունը ծառայում են ոչ միայն ձեր հարմարությանը, այլև համացանցում ձեր գործունեությանը հետևելուն: Հետքերը կորցնել հնարավոր է, բայց երբեմն ավելի հարմար է ընդհանրապես հետք չթողնել՝ դրա համար անհրաժեշտ է բրաուզերի առանձնացված ռեժիմ: Սա կարևոր է, եթե ձեր համակարգչով աշխատում են նաև ուրիշները:

**ՈՒՐԻՇԻ ՀԱՄԱԿԱՐԳԶՈՎ ԱՇԽԱՏԵԼԻՍ
ԱՆՁՆԱԿԱՆ ՔԻՉ ՏՎՅԱԼՆԵՐ ՕԳՏԱԳՈՐԾԵՔ**

ԽՈՐՀՈՒՐԴ 38: **ՉԵՏՔ ՉԹՈՂՆԵԼ**

Ցանկացած համակարգիչ ներծծում է ինֆորմացիան այնպես, ինչպես՝ սպունգը ջուրը: Այդպիսին է նրա կառուցվածքը: Եթե դուք աշխատում եք ուրիշի համակարգչով, ապա մի մոռացեք, որ կգտնվի հնարագետ մեկը և կքամի այդ սպունգը՝ տիրանալով արժեքավոր տվյալներին՝ այդ թվում և ձեր: Հայտնի չէ, թե ում ձեռքում կհայտնվեն ձեր այցելած էջերի ցուցակը, ձեր գաղտնաբառերն ու ծածկագրերը, ձեր գրած նամակները և հաղորդագրությունները: Բայց սա չի նշանակում, որ հանրամատչելի համակարգչից պետք չէ օգտվել, պետք է հիշել, որ այդ համակարգիչը ոչ միայն անվստահելի, այլ պոտենցիալ թշնամական միջավայր է:

... ԵՎ ՉԻՇԵՔ, ՈՐ ՀԱՆՐԱՄԱՏՉԵԼԻ ՀԱՄԱԿԱՐԳԻՉՆԵՐԸ ԿԱՐՈՂ ԵՆ ՎԱՐԱԿՎԱԾ ԼԻՆԵԼ

ԽՈՐՀՈՒՐԴ 39: **ՀԱՆՐԱՄԱՏՉԵԼԻ ՎԻՐՈՒՍ**

Ուրիշի համակարգչով աշխատելիս հնարավոր է այնտեղ թողնել արժեքավոր ինչ-որ բան, բայց հնարավոր է նաև այնտեղից ստանալ տհաճ ինչ-որ մի բան: Խոսքը վնասատու ծրագրերի մասին է, որոնցով կարող է վարակված լինել հանրամատչելի համակարգը: Վնասատու ծրագրերը տարածվում են տարբեր ձևերով: USB մուտքի մեջ մտցրած ձեր կրիչը վայրկյանների ընթացքում դառնում է վարակ տարածող: Չէ՞ որ հայտնի չէ, թե ինչ է եղել այն կրիչների վրա, որոնք ձեզնից առաջ այդ համակարգչում օգտագործել են ուրիշները և ինչ կայքեր են այցելել:

ՀԱՍԱՐԱԿԱԿԱՆ WI-FI-Ը ՆՈՒՅՆՆ Է, ԻՆՉ ՀԱՍԱՐԱԿԱԿԱՆ ԼՈՂԱՎԱԶԱՆԸ

ԽՈՐՀՈՒՐԴ 40: **ՑԱՆՑԱՀԵՆԻ ՇՐՋԱՊԱՏՈՒՄ**

Հանրային Wi-Fi-ը երբեն ավելի լավ է շարժական ինտերնետից, քանի որ ապահովում է համացանցի արագ հասանելիությունը և կարևորը՝ անվճար է: Բայց այդ կապուղին վատ է պաշտպանված և անձամբ ձեզ չի պատկանում: Այսինքն՝ դրա համալարումները հայտնի չեն և կիսում եք շրջապատի մարդկանց հետ: Ցավոք, նրանց մեջ կարող են լինել այնպիսիները, որոնց հետաքրքրում է ուրիշների անձնական ինֆորմացիան, նրանք գիտեն ինչպես ձեռք գցել տվյալները չպաշտպանված անհաղորդիչ ցանցերում: Տհաճ է, որ նրանց գոյության մասին դուք իմանում եք այն ժամանակ, երբ հանցագործները որոշում են օգտագործել գողացած գաղտնաբառերը և ձեր էլեկտրոնային փոստից սպամ ուղարկել կամ խմբագրում են սոց. ցանցում ձեր պրոֆիլը:

ՆԵՐԲԵՌՆԵՔ ԾՐԱԳՐԵՐԸ ՄԻԱՅՆ ԱՐՏԱԴՐՈՂԻ ԿԱՅՔԻՑ

ԽՈՐՀՈՒՐԴ 41: **ԱՆՎՏԱՆԳ ՆԵՐԲԵՌՆՈՒՄ**

Եթե ձեզ դուր է եկել ինչ-որ ծրագիր՝ մի շտապեք այն ներբեռնել որոնողական ծրագրի առաջարկած առաջին իսկ հղումից: Ծրագրից բացի հնարավոր է ներբեռնեք վիրուսներ: Վնասատու ծրագրերի և ձանձրացնող գովազդների տարածման ձևերից մեկն էլ հավելվածներում նրանց ներդրումն է: Հանցագործները գովազդում են վարակված հավելվածներով կայքերը և որոնողական ծրագրերը դրանք ցույց են տալիս ավելի շատ անգամ, քան արտադրողի պաշտոնական կայքերը: Եթե ծուլանում եք որոնել պաշտոնական կայքը՝ մտածեք, արժե՞ արդյոք վտանգել ձեր համակարգիչը և անձնական տվյալները:

...ԵՎ ՄԻ ՄՈՌԱՑԵՔ ԴՐԱՆՔ ՆՈՐԱՑՆԵԼ

ԽՈՐՀՈՒՐԴ 42: **ՆՈՐԱՑՈՒՄՆԵՐԻ ՆԵՐԲԵՌՆՈՒՄ**

Մեկ անգամ ներբեռնելով ծրագիրը կարող եք երկար ժամանակ օգտվել դրանից՝ ծրագիրը մեխանիզմ չէ, չի մաշվում: Բայց ցանկացած ծրագիր ունի սխալներ՝ խոցելի տեղեր, որոնք կարող են օգտագործել չարագործները համակարգիչը վարակելու համար: Ինչքան ծրագիրը հայտնի է, այնքան ավելի շատ չարագործներ փորձում են գտնել ծրագրի խոցելի տեղերը: Միաժամանակ ծրագրի հեղինակները իմանալով, որ իրենց հավելվածում կա խոցելի տեղ, շտապում են թողարկել նոր հավելված առանց խոցելի տեղերի: Նշանակում է, որ ներբեռնել ծրագիրը բավարար չէ, պետք է ժամանակին տեղադրել նրա մատչելի բոլոր նորացումները:

ՀԱՎԵԼՎԱԾԸ ՆԵՐԲԵՌՆԵԼՈՒ ԺԱՄԱՆԱԿ
ՈՒՇԱԴԻՐ ՈՒՍՈՒՄՆԱՍԻՐԵՔ ՏԵՂԱԿԱՅՄԱՆ ԼՐԱՑՈՒՑԻՉ ՀՈՒՇՈՒՄՆԵՐԸ

ԽՈՐՀՈՒՐԴ 43: **ԾՐԱԳՐԻ ՃԻՇՏ ՆԵՐԲԵՌՆՈՒՄ**

Անվճար ծրագրերը ուրախացնում են օգտատերերին: Բայց ծրագրերի հեղինակները ինչ-որ կերպ պետք է գումար վաստակեն: Այդ պատճառով նրանցից շատերը թույլ են տալիս իրենց ծրագիրը տեղադրել կողմնակի հավելվածների միջոցով, գործիքների վահանակների և բրաուզերների լրացումների միջոցով, որոնք կծանրաբեռնեն ավելորդ գործիքներով՝ խանգարելով նորմալ աշխատանքը, իսկ ամենավատը՝ կշատանան գովազդային վահանակները:

...ԼՐԱՑՈՒՑԻՉ ՄՈԴՈՒԼՆԵՐԻ ՏԵՂԱԴՐՈՒՄԸ ՀԵՆՑ ՍԿԶԲԻՑ ՉԵՂԱՐԿԵԼ

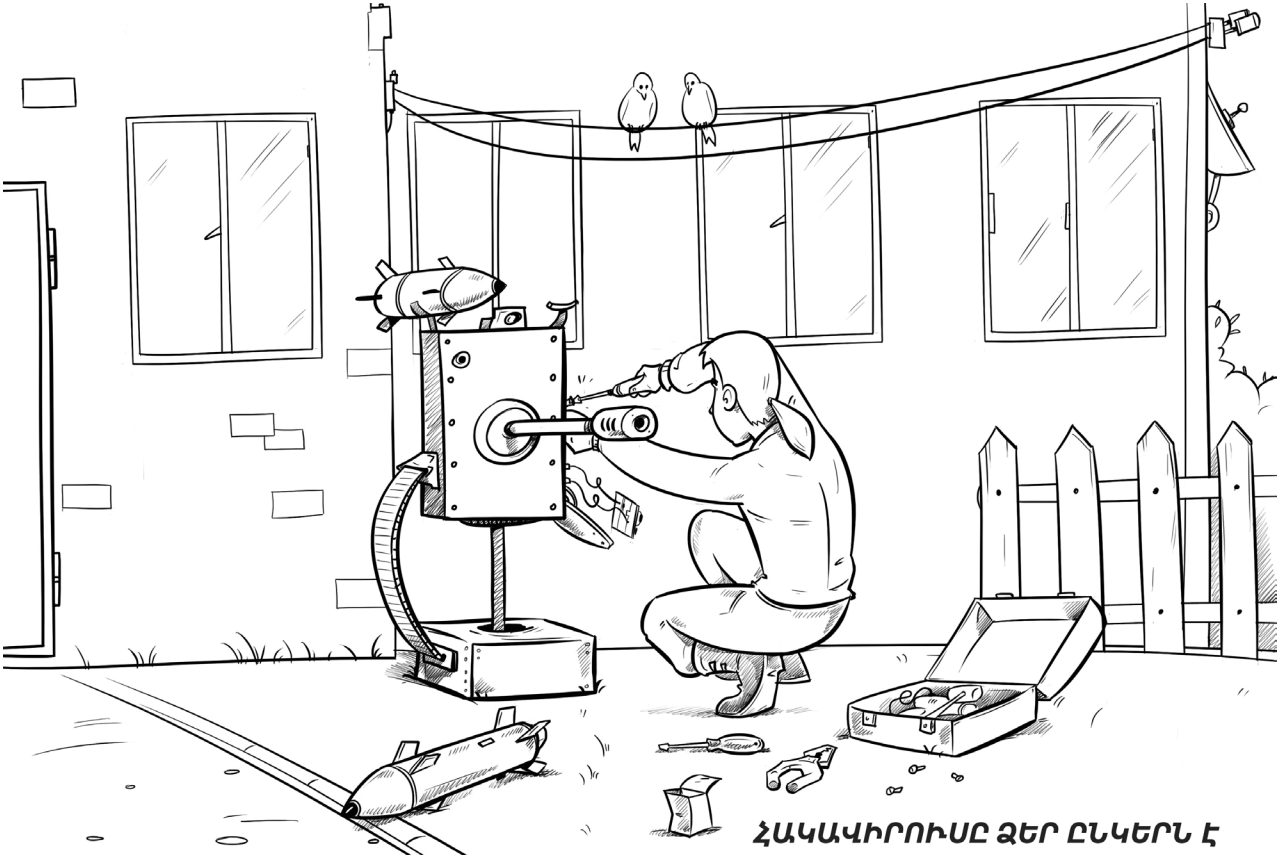
ԽՈՐՀՈՒՐԴ 44: **ԾՐԱԳՐԵՐ ԱՌԱՆՑ ԱՂԲԻ**

Իսկ հիմա լավ նորություն՝ համարյա միշտ ուղեկցող ավելորդությունների ներբեռնումը կարելի է չեղարկել ելակետային ծրագիրը տեղադրողի մեջ՝ փոփոխելով նրա համալարումները: Դրա համար ցանկացած հավելված ներբեռնելիս պետք է կարդալ էկրանի վրա հայտնվող հաղորդագրությունները և ուշադիր ուսումնասիրել տեղակայման պատուհանները: Այդ դեպքում հետո ստիպված չեք լինի մաքրել համակարգը տասնյակ անօգուտ, երբեմն վնասատու լրացումներից:

**ԿԱՐԴԱՑԵՔ ՀԱՎԱՍՏԱԳՐՎԱԾ ՀԱՄԱՁԱՅՆԱԳՐԵՐԸ,
ՆԵՐԱՌՅԱԼ՝ԾԱՆՈԹԱԳՐՈՒԹՅՈՒՆՆԵՐԸ**

ԽՈՐՀՈՒՐԴ 45: **ՀԱՄԱՁԱՅՆԱԳՐԻ ՍՏՈՒԳՈՒՄ**

Օգտակար ծրագիրը, որի համար դուք մեծ գումար եք վճարել, կարող է ունենալ թաքնված ֆունկցիաներ, որոնք ձեր օգտին չեն աշխատում: Կամ մեկ ուրիշ իրավիճակ. ծրագիրը գործ ունի ձեր տվյալների հետ, բայց ծրագիրը ստեղծողները չեն ուզում պատասխանատվություն կրել դրանց պահպանման համար, բայց շահագրգիռ են այդ տվյալները հայտնել գովազդատուին: Նման դեպքերում ծրագիր կազմողները մանրամասն մշակում են հավաստագրված համաձայնագրի տեքստն այնպես, որ իրենք հնարավորինս քիչ պատասխանատվություն կրեն: Մենք խորհուրդ ենք տալիս ուշադիր կարդալ այդ խճողված փաստաթուղթը մինչև ծրագրի տեղադրումը:



ՀԱԿԱՎԻՐՈՒՍԸ ՁԵՐ ԸՆԿԵՐՆ Է

ԽՈՐՀՈՒՐԴ 46: **ԲԱՂԱՅԻՆ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ**

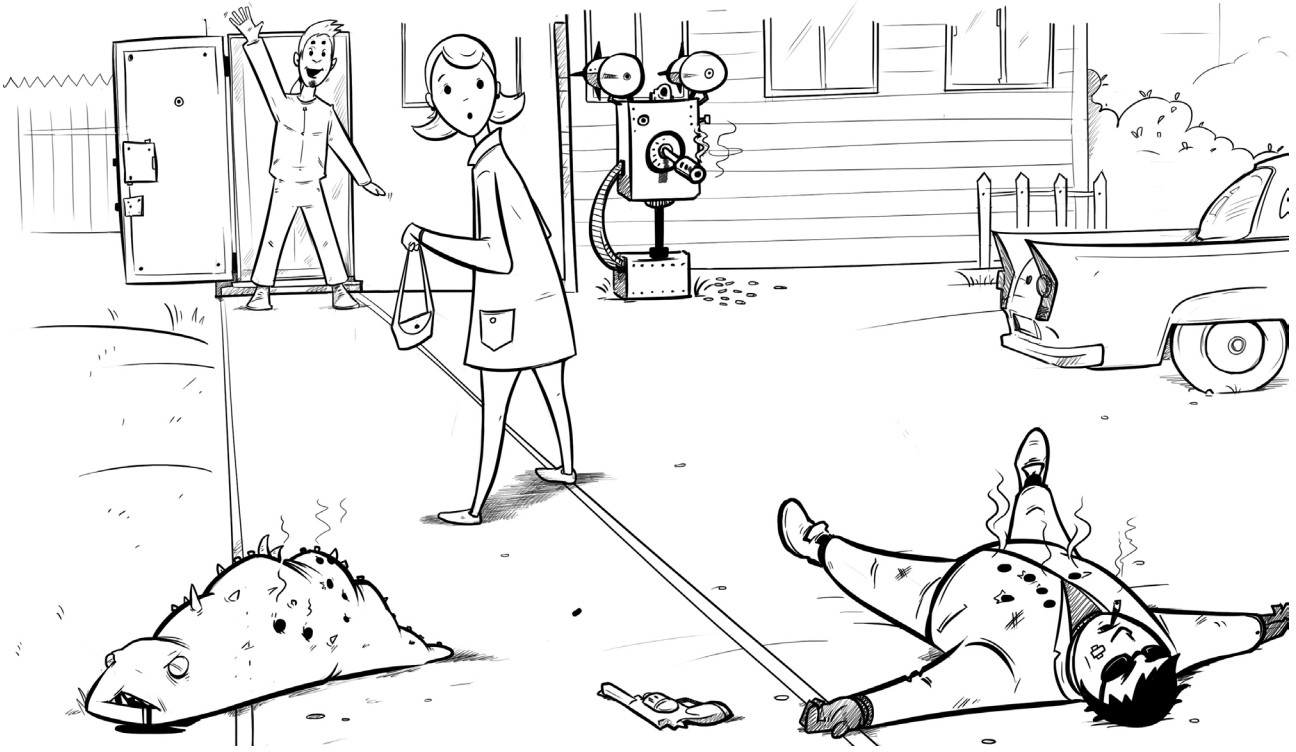
Սեփական տան կամ ամառանոցի բնակիչը երբևէ երազել է պաշտպանական ավտոմատ համակարգի մասին, որ իրեն կպաշտպանի գողերից, անկարգ երեխաներից, գողացած ապրանք վաճառողներից և հետաքրքրասեր հարևաններից: Օրենքով այդպիսի համակարգը արգելված է, իսկ կիբեռաշխարհում առանց պաշտպանական համակարգի հնարավոր չէ: Հակավիրուսային ծրագրային ապահովումը կպաշտպանի համակարգիչը տեղեկատվական սպառնալիքներից և սպամերների անցանկալի ուշադրությունից, դուք կկարողանաք հանգիստ աշխատել, սովորել և զվարճանալ համացանցի տեղեկատվական տարածքում:

ՄԻ ՎՍՏԱՀԵՔ ՁԵՐ ՀԱՄԱԿԱՐԳԻՉԸ ԱՆՑԱՆՈՒԹ «ԾՐԱԳՐԱՎՈՐՈՂՆԵՐԻՆ»

ԽՈՐՀՈՒՐԴ 47: **ՀԱԿԱՎԻՐՈՒՍԻ ՀԱՄԱԼԱՐՈՒՄԸ**

Ո՞վ կվստահի իր փողերը, փաստաթղթերը և անձնական գաղտնիքները առաջին պատահած անծանոթ մարդուն: Իհարկե ոչ ոք: Այսօր թանկարժեք իրերի ցուցակում անվարան կարելի է ավելացնել անձնական համակարգիչը, որը շատերի համար դարձել է և էլեկտրոնային դրամապանակ, և անձնական օրագիր: Այդ պատճառով համակարգչի համալարումները, և հատկապես այնտեղ տեղադրված պաշտպանական գործիքները, պատահական մարդու չի կարելի վստահել: Խնդիրը ոչ թե չարամտությունն է, այլ պատասխանատու վերաբերմունքը: Պարամետրերի անփույթ համալարումը կարող է ձեզ զրկել տեղեկատվական սպառնալիքների պաշտպանությունից:

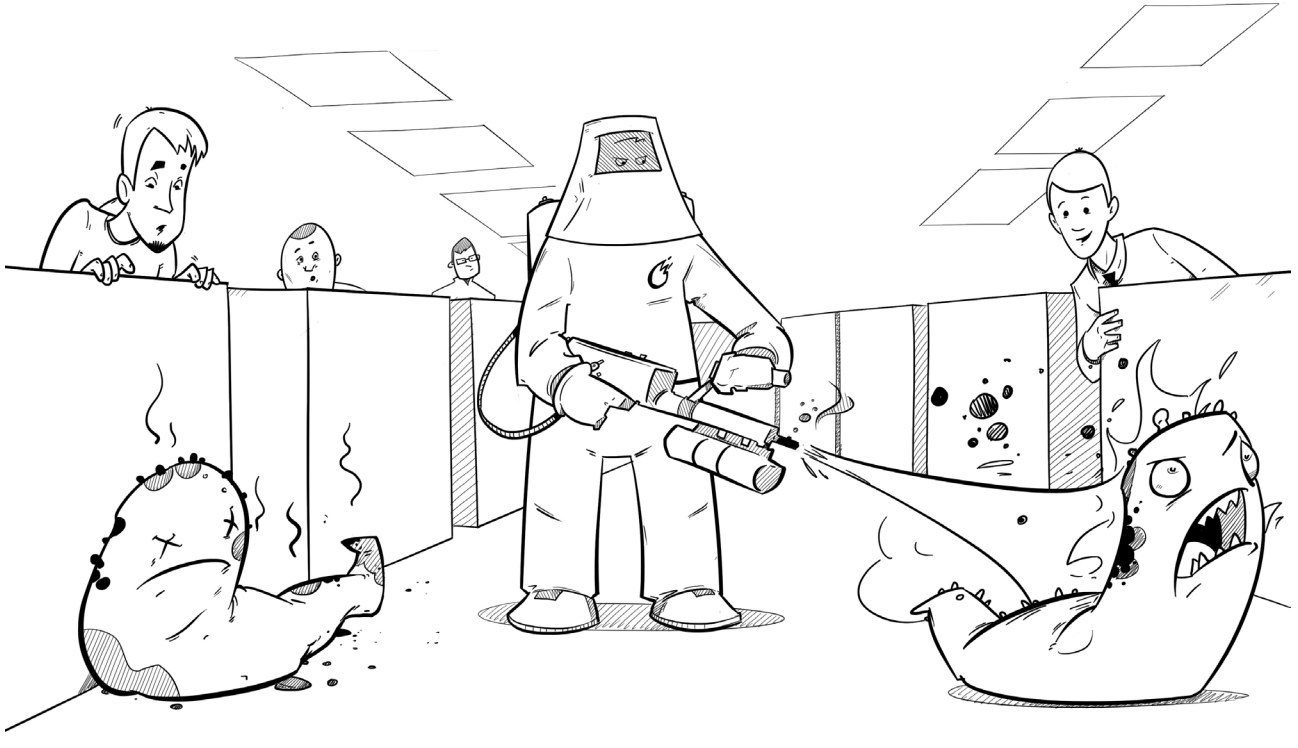
ՊԱՇՏՊԱՆԱԿԱՆ ՀԱՄԱԼԻՐ ԼՈՒԾՈՒՄԸ
ԿԱՉԱՏԻ ՁԵՋ ԱՆՑԱՆԿԱԼԻ ՀՅՈՒՐԵՐԻՑ



ԽՈՐՀՈՒՐԴ 48: **ՀՈՒՍԱԼԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ**

Համացանցը շատ վտանգավոր տեղ է: Երբ տեղ ես տալիս լավ ծրագրին, ապա նրա հետ հայտնվում են անկոչ հյուրեր, որոնք իսկույն հաստատում են իրենց իրավունքը ձեր օպերացիոն համակարգի նկատմամբ, տակնուվրա են անում կոշտ սկավառակը, լցնում են բրաուզերը գովազդով և ձեզնից գումար կպահանջեն համակարգչով անարգել աշխատելու համար: Խորհուրդ ենք տալիս այդպիսի հյուրերին իսկույն հեռացնել, բայց այնպես, որ օգտակար հավելվածները չտուժեն: Հուսալի ավտոմատ պաշտպանություն կապահովի հակավիրուսային արտադրանքը, որը տարբերում է լավերին և վատերին, և գնահատում է յուրաքանչյուր ծրագիր ըստ արժանվույն:

ԱՇԽԱՏԱՏԵՂԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ ԿԱՊԱՀՈՎԻ ՅԱՆՑԱՅԻՆ ԱԴՄԻՆԻՍՏՐԱՏՈՐԸ



ԽՈՐՀՈՒՐԴ 49: **ՄԱՍՆԱԳԵՏԻ ԱՇԽԱՏԱՆՔԸ**

Անհոգ աշխատակիցները գլխացավանք են ցանցային ադմինիստրատորի համար: Նրանք նման են փոքր երեխաների՝ կամ լարը կհանեն վարդակից, կամ սուրճ կթափեն ստեղնաշարի վրա, կամ էլ որևէ վնասատու ֆայլ կբեռնեն համակարգչի մեջ: Վերջին դեպքում ցանցային ադմինիստրատորը միշտ օգնության կհասնի՝ կարևորը չխանգարել նրան: Նա պետք է անարգել մոտենա աշխատատեղին և տեղեկանա հիվանդության ախտանիշների մասին: «Ես հիմա զբաղված եմ, մի փոքր ուշ», «Ոչ մի դեպքում մի գերբեռնիր», ««Excel»-ի այս 19 փաստաթղթերը փակել չի կարելի» արտահայտությունները դուր են գալիս չարագործներին՝ չէ որ այդ արտահայտությունները խանգարում են ցանցային ադմինիստրատորին կատարել իր աշխատանքը՝ ազատել ընկերությունը տեղեկատվական սպառնալիքներից:

ԱՇԽԱՏԱՏԵՂԻՑ ՀԵՌԱՆԱԼԻՍ ԱՐԳԵԼԱՓԱԿԵՔ ՀԱՄԱԿԱՐԳԻՉԸ

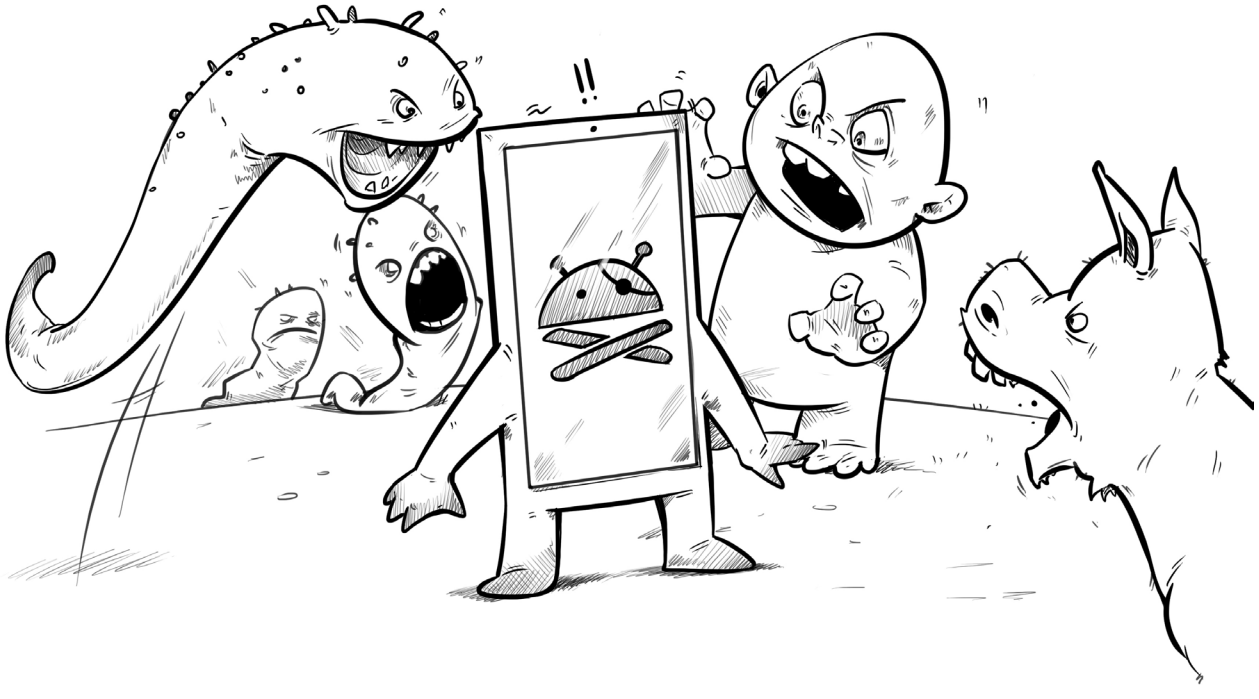
ԽՈՐՀՈՒՐԴ 50: **ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ ԱՇԽԱՏԱՎԱՅՐՈՒՄ**

Ցանկացած մարդու, ով ձեր բացակայության ժամանակ կհայտնվի ձեր աշխատատեղում, ընկերության համակարգիչները կընկալեն որպես ձեզ: Նման բան կարող է տեղի ունենալ, եթե ընդմիջման գնալիս համակարգը չարգելափակեք: Երբ վերադառնաք՝ ձեզ տհաճ անակնկալ է սպասում՝ ձեր համակարգչից ձեր կատակասեր գործընկերները տնօրենին անախորժ բաներ են ուղարկել կամ էլ տպիչին հրահանգել են տպել «Մատանիների տիրակալը» գունավոր նկարներով: Ավելի վատ կլիներ, եթե ձեր համակարգիչը հասանելի լիներ չարամիտներին: Աշխատատեղից հեռանալիս անհրաժեշտ է ընդամենը երկու ստեղն սեղմել:

ՈՉ ՊԵՏՔԱԿԱՆ ՓԱՍՏԱԹՂԹԵՐԸ ԳՑԵՔ ՇՐԵԴԵՐԻ ՄԵՋ

ԽՈՐՀՈՒՐԴ 51: **ՉԹՎԱՅՆԱՑՎԱԾ ՓԱՍՏԱԹՂԹԵՐ**

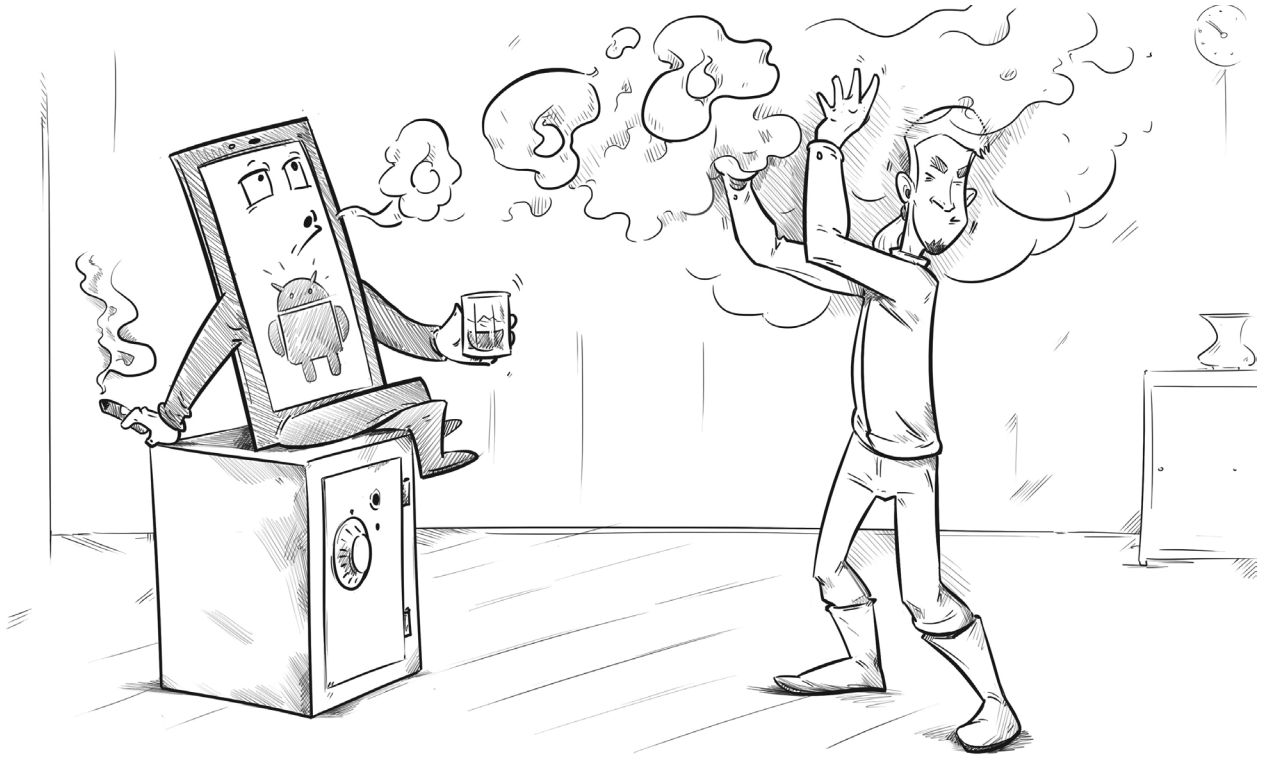
Այն, ինչ ձեզ համար աղբ է, հանցագործի համար ինֆորմացիայի թանկարժեք աղբյուր է: Հին, ոչ պետքական փաստաթղթերը և ցուցակները վաղ թե ուշ հայտնվում են աղբարկղում: Եթե դրանք չեք գցել շրեդերի մեջ, ապա հանցագործները այդտեղից շատ տեղեկություններ կարող են կորզել՝ կազմակերպության կնիքի արտատպությունը, ղեկավարների ստորագրությունների նմուշները, կոնտրագենտների հասցեները, անունները և վճարման վավերապայմանները, աշխատակիցների ցուցակները և այլն: Մի զարմացեք, երբ մեկ ուրիշը կստանա ապրանքը ձեր առաքիչի փոխարեն կամ կազմակերպության հաշվից գումար կհանի:



«ROOT»-Ի ԵՆԹԱՐԿՎԱԾ ՍՄԱՐԹՖՈՆԸ ԽՈՅԵԼԻ Է ՀԱՆՑԱԳՈՐԾՆԵՐԻ ՀԱՄԱՐ

ԽՈՐՀՈՒՐԴ 52: **ՍՄԱՐԹՖՈՆԻ «ԿՈՏՐՈՒՄԸ»**

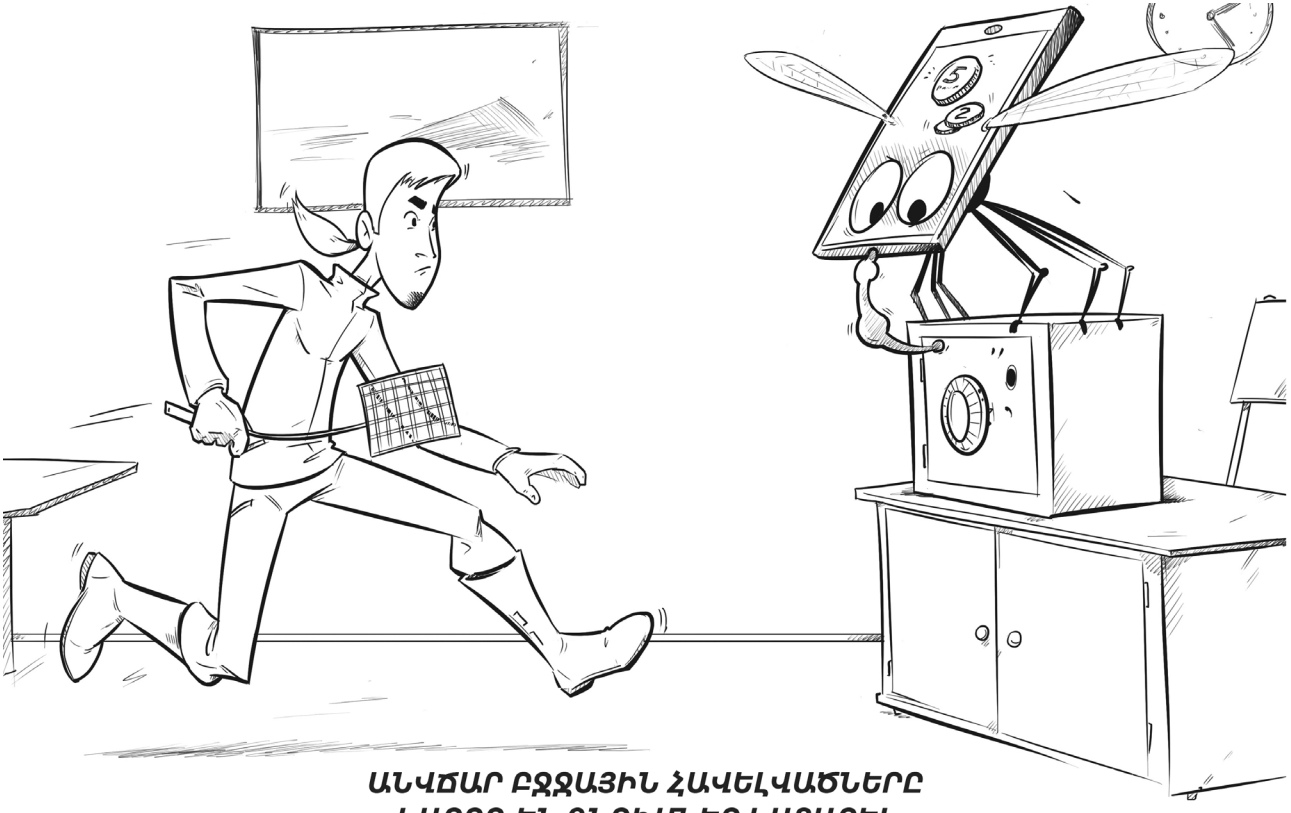
Ժամանակակից բջջային պաշտպանական համակարգերը սահմանափակում են սմարթֆոնի տիրոջ ազատությունը՝ թույլ չեն տալիս փոփոխել ցանցային ֆայլերը: Սահմանափակումից ազատվել օգնում է սմարթֆոնի «կոտրումը» և ադմինիստրատորի իրավունքների ձեռքբերումը: Այս գործողությունը կոչվում է «root» կամ «jailbreak»: Իրավունքների ընդլայնման առավելությունները գնահատում են ոչ միայն օգտատերերը, այլև հացագործները, որոնք մասնագիտացել են բջջային սարքերի սպառնալիքների գործում: Հարձակվել «կոտրած» պաշտպանական համակարգի վրա ավելի հեշտ է, հետևաբար «root»-հասանելիություն ունեցող սարքի վարակման հավանականությունը մեծանում է:



ՆԱԽՔԱՆ ԲՋՋԱՅԻՆ ՀԱՎԵԼՎԱԾԸ ՏԵՂԱԴՐԵԼԸ ՈՒՍՈՒՄՆԱՍԻՐԵՔ ԹՈՒՅԼՏՎՈՒԹՅՈՒՆՆԵՐԻ ՑՈՒՑԱԿԸ

ԽՈՐՀՈՒՐԴ 53: **ՀԱՎԵԼՎԱԾԻ ԸՆՏՐՈՒԹՅՈՒՆ**

Հաշվիչ հավելվածը ձեր բանկ հաղորդագրություն է ուղարկել՝ հրահանգելով ձեր փողերը փոխանցել անծանոթ հաշվեհամարի, հետո հղումներ է ուղարկել ձեր հեռախոսում եղած համարներին իր պատճենից: Տհաճ իրավիճակ է: Փորձեք հիշել՝ հավելվածը տեղադրելիս դուք ուսումնասիրել եք թույլտվությունների ցուցակը, որը հարցնում էր հավելվածը: Երևի՝ ոչ, հակառակ դեպքում հարց կառաջանար, թե ինչո՞ւ է հաշվիչը ուզում, որ ձեր կոնտակտները և հաղորդագրությունները հասանելի լինեն իր համար: Ցավոք, սմարթֆոնների օգտատերերը հաճախ անտեսում են հարցվող թույլտվությունների ցանկը, այսպիսով թույլ են տալիս, որ հավելվածը սարքի մեջ անի այն, ինչ ցանկանում են նրա հեղինակները: Բարեբախտաբար, թանկարժեք մեկ դասը բավական է, որ մարդիկ ուշադիր լինեն:



ԱՆՎՃԱՐ ԲՋՋԱՅԻՆ ՀԱՎԵԼՎԱԾՆԵՐԸ ԿԱՐՈՂ ԵՆ ԳՆՈՒՄՆԵՐ ԿԱՏԱՐԵԼ

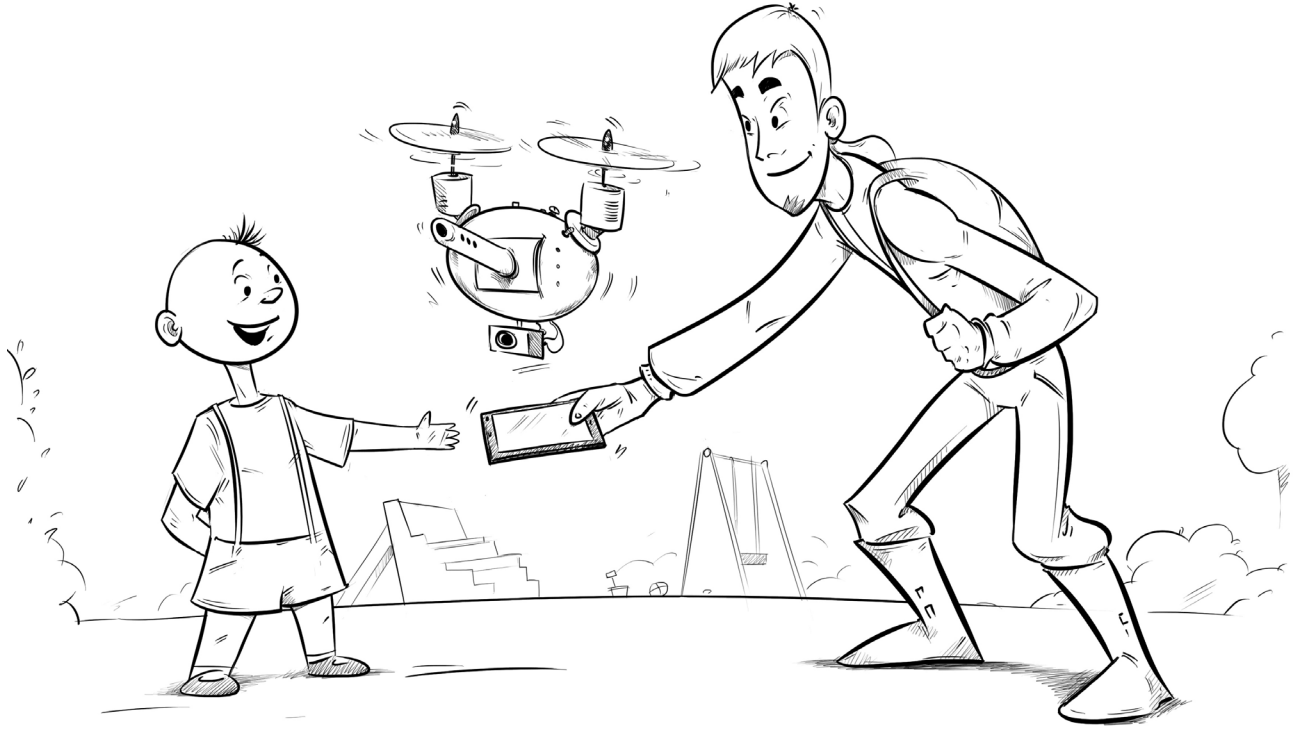
ԽՈՐՀՈՒՐԴ 54: **ԱՆՆԿԱՏԵԼԻ ԲՋՋԱՅԻՆ ՎՃԱՐՈՒՄՆԵՐ**

Բջջային հավելվածների գնի հարցը այնքան էլ պարզ չէ: Եթե հավելվածը կարելի է ներբեռնել անվճար, այդ չի նշանակում, որ դուք գումար չեք ծախսելու: Այդ անվճար հավելվածը ձեզ վրա կարող է ավելի թանկ նստել, քան վճարովին: Եթե ձեր բախտը բերի՝ հավելվածը կարող է ձեզ հոգնեցնել գովազդներ ցուցադրելով, բայց հնարավոր է, որ «քամի» ձեր բանկային քարտը հավելվածի ներսում գնումներ անելով: Բջջային հավելվածներ վաճառող խանութներ ունեցող ընկերությունների կարծիքով այդ գնումները օրինական են, քանի որ օգտատերերից շատերը պատրաստ են մեկ-երկու դոլար վճարել իրենց սիրելի խաղում նոր թուր ունենալու համար: Պետք է այնպես անել, որ գնումը կատարվի բացահայտ, բայց արագ և անցավ: Իսկ հավելված մշակողները նախընտրում են ստեղծել այնպիսի հավելվածներ, որոնք ինքնուրույն կարող են գնումներ կատարել:

ՊԵՏՔ ՉԷ ՍԵՂՄԵԼ SMS-ՈՒՄ ԱՆԾԱՆՈԹ ՀՂՈՒՄՆԵՐԸ

ԽՈՐՀՈՒՐԴ 55: ՎՏԱՆԳԱՎՈՐ SMS ՀԱՂՈՐԴԱԳՐՈՒԹՅՈՒՆՆԵՐ

Հաճա՞խ եք ձեր ընկերներին SMS ուղարկում հետաքրքիր նյութի հղումով: Դժվար թե: Հանցագործները շատ են սիրում վնասատու հղումներով հաղորդագրություններ ուղարկել և տեքստ, որը մղում է սեղմել հղումը: Նրանք կարող են այնպես անել, որ վնասատու հաղորդագրություն ուղարկվի ձեր ընկերոջ հեռախոսահամարից: Պետք չէ կարծել, որ ձեր ընկերը համաձայնվել է նրանց հետ հանցավոր ճանապարհով գումար վաստակել: Պարզապես հղումը մի փոքր ավելի շուտ է հասել նրան և նա սեղմել է: Հիմա ձեր ընկերոջ սմարթֆոնը վարակված է վնասատու ծրագրով, որը սկսել է հղումներ ուղարկել ինքն իր վրա կոնտակտների ցուցակում եղածներին:



ՄԻ ՄՈՌԱՑԵՔ ԵՐԵԽԱՆԵՐԻ ԲԶԶԱՅԻՆ ՍԱՐՔԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԱՍԻՆ

ԽՈՐՀՈՒՐԴ 56: **ՄԱՆԿԱԿԱՆ ՍՄԱՐԹՖՈՆԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ**

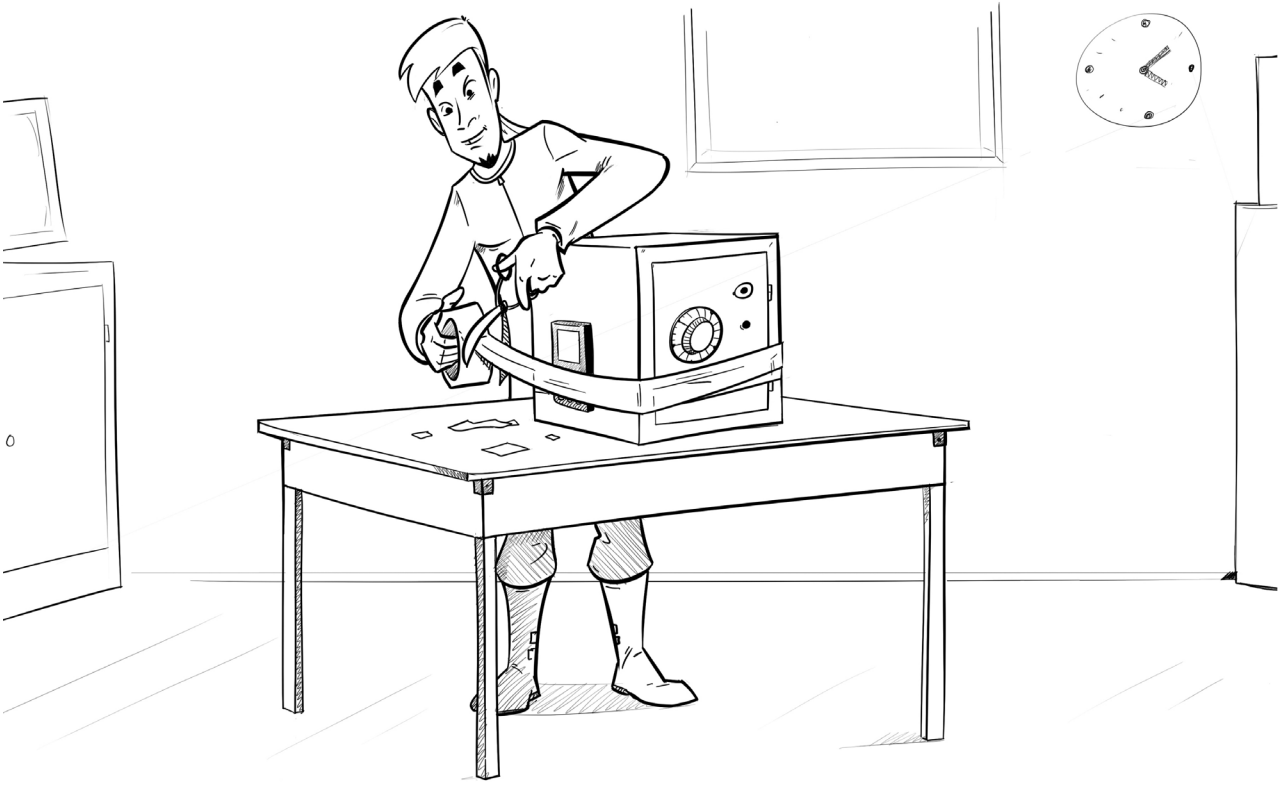
Ձեր սմարթֆոնը ունի հուսալի պաշտպանություն, բայց ձեր բանկային քարտից անընդհատ գումար է պակասում «Google Play»-ում կասկածելի գնումների պատճառով: Իհարկե «Google»-ը մտադիր չէ ձեզ գաղտնի կողոպտել, սա հարգելի ընկերության սկզբունքներին հակառակ է: Ժամանակն է հիշել, որ դուք ձեր երեխայի հեռախոսին փոխանցել եք ձեր քարտի տվյալները մանկական մի քանի խաղ գնելու համար: Հիմա բջջային վարակը հասել է ձեր երեխայի հեռախոսին և կամաց-կամաց ձեր քարտից գումար է գողանում: Պետք է դադարեցնել վիրուսի գործողությունները և սմարթֆոնի մեջ տեղադրել բջջային հակավիրուս: Երեխաների տեխնիկական սարքավորումները չպետք է մնան անպաշտպան:

ՄՈՒՏՔԸ ԼԻԱԶՈՐԵ՛Ք ԸՍՏ ՄԱՏՆԱՀԵՏՔԻ

ԽՈՐՀՈՒՐԴ 57: **ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՆՈՐ ՏԵԽՆՈԼՈԳԻԱՆԵՐ**

Գեղարվեստական ֆիլմերում կան տեսարաններ, որտեղ կողպեքները բացում են մատնահետքով: Մատնահետքը որպես պաշտպանության միջոց ավելի հուսալի է, քան քառանիշ թվային կոդը կամ գրաֆիկական բանալին, որոնք ցանկության դեպքում կարելի է տեսնել: Հատկապես անհուսալի են պարզ պաշտպանական կոդերը, եթե «հանցագործը» ձեր երկրորդ կեսն է, ով ուզում է կարդալ ձեր սմարթֆոնի SMS հաղորդագրությունները: Մատնահետքը հարմար է օգտատիրոջը և անհարմար է հանցագործի համար:

ՄԻԱՑՐԵՔ ԲԱՆԿԱՅԻՆ ՔԱՐՏՈՎ ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐԻ ՄԱՍԻՆ ՀԱՅՏՆՈՂ SMS-ԾԱՆՈՒՑՈՒՄՆԵՐԻ ԾԱՌԱՅՈՒԹՅՈՒՆԸ



ԽՈՐՀՈՒՐԴ 58: **ՈՎ ԻՐԱՁԵԿՎԱԾ Է, ՆԱ ՉԻՆՎԱԾ Է**

Բանկոմատները, առցանց գնումները, ինտերնետ և բջջային բանկինգը և ֆինանսական այլ տեխնոլոգիաները գողերի լավագույն բարեկամներն են: Դրանք ձեր լավագույն բարեկամներն էլ են, բայց գողերի համար եկամտի աղբյուր են, իսկ ձեզ համար՝ հարմարավետություն: Հանցագործները շատ են սիրում կողոպտել՝ չմոտենալով զոհին՝ ինչն արագ է, հեշտ է, անվտանգ է: Պաշտպանվել այսպիսի կողոպուտից ավելի հեշտ է մի պայմանով՝ եթե դուք գիտեք, որ ձեզ կողոպտում են: Եթե բոլորը ամեն օր չեն կարող նայել բանկային քարտից քաղվածքները, ապա բանկային գործողությունների մասին SMS-ծանուցումներ ստանալը դժվարություն չէ: Եթե տեսնում եք ծանուցում անծանոթ գնումների մասին՝ շտապեք բանկ և արգելափակեք քարտը: Անկանխիկ փողերը կարելի է վերադարձնել:

ՕԳՏԱԳՈՐԾԵՔ ԵՐԿՖԱԿՏՈՐ ՎԱՎԵՐԱԿԱՆՈՒԹՅՈՒՆԸ

ԽՈՐՀՈՒՐԴ 59: **ՓՈՂԵՐԻ ԿՐԿՆԱԿԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ**

Հմուտ ցանցահենը կարող է գողանալ ցանկացած գաղտնաբառ: Այնպես որ, եթե ձեզ համար կարևոր սերվերը առաջարկում է երկֆակտոր վավերակա-նացում՝ անպայման համաձայնվեք: Պաշտպանության լրացուցիչ մակարդակը, օրինակ՝ SMS-ով մեկանգամյա գաղտնաբառ ուղարկելը, կապահովագրի ձեր հաշվագրանցումը: Լավ տարբերակ է նաև հատուկ USB-տոկենի բանալու տեսքով կրիչի կիրառումը՝ եթե այն դրված չէ համակարգչի USB-մուտքի մեջ՝ բանկը կամ պաշտպանվող ծառայության կայքը հասանելի չեն:

ՉՊԱՇՏՊԱՆՎԱԾ ԲԱՆԿՈՄԱՏԸ ԿԱՐՈՂ Է ԴԱՌՆԱԼ ԿԻԲԵՌՀԱՆՑԱԳՈՐԾՆԵՐԻ ԳՈՐԾԻՔԸ

ԽՈՐՀՈՒՐԴ 60: **ՎՏԱՆԳԱՎՈՐ ԲԱՆԿՈՄԱՏ**

Ցավոք, բանկերը քարտերի վրա չեն գրում կարճ, բայց տարողունակ նշանաբան՝ «Նայիր՝ ուր ես մտցնում»: Այս նշանաբանը կօգներ կանխել բազմաթիվ խաբեություններ: Բանկային քարտերը վճարման հարմար միջոց են, միաժամանակ ձեր բանկային հաշիվը կողոպտելու պարզ և անվտանգ մեթոդ: Սովորական մարդը նայելով չի կարող որոշել բանկոմատը մաքուր է, թե տեղադրված է սկիմեր՝ քարտի տվյալները գողանալու համար սարք: Հանցագործները (նրանց կոչում են կարդեր) սովորել են վարպետորեն թաքցնել բանկոմատի վրա տեղադրված իրենց սարքավորումները: Ինժեներական խմբերը ստուգում են բանկոմատները ամիսը մեկ կամ ավելի ուշ, իսկ հանցագործները այդ ժամանակաընթացքում կարող են գողանալ հարյուր-հազարավոր մարդկանց բանկային քարտերի տվյալները:

ԱՄԵՆԱԱՆՎՏԱՆԳ ԲԱՆԿՈՄԱՏԸ ԲԱՆԿԻ ՄԱՍՆԱՃՅՈՒՂՈՒՄ Է

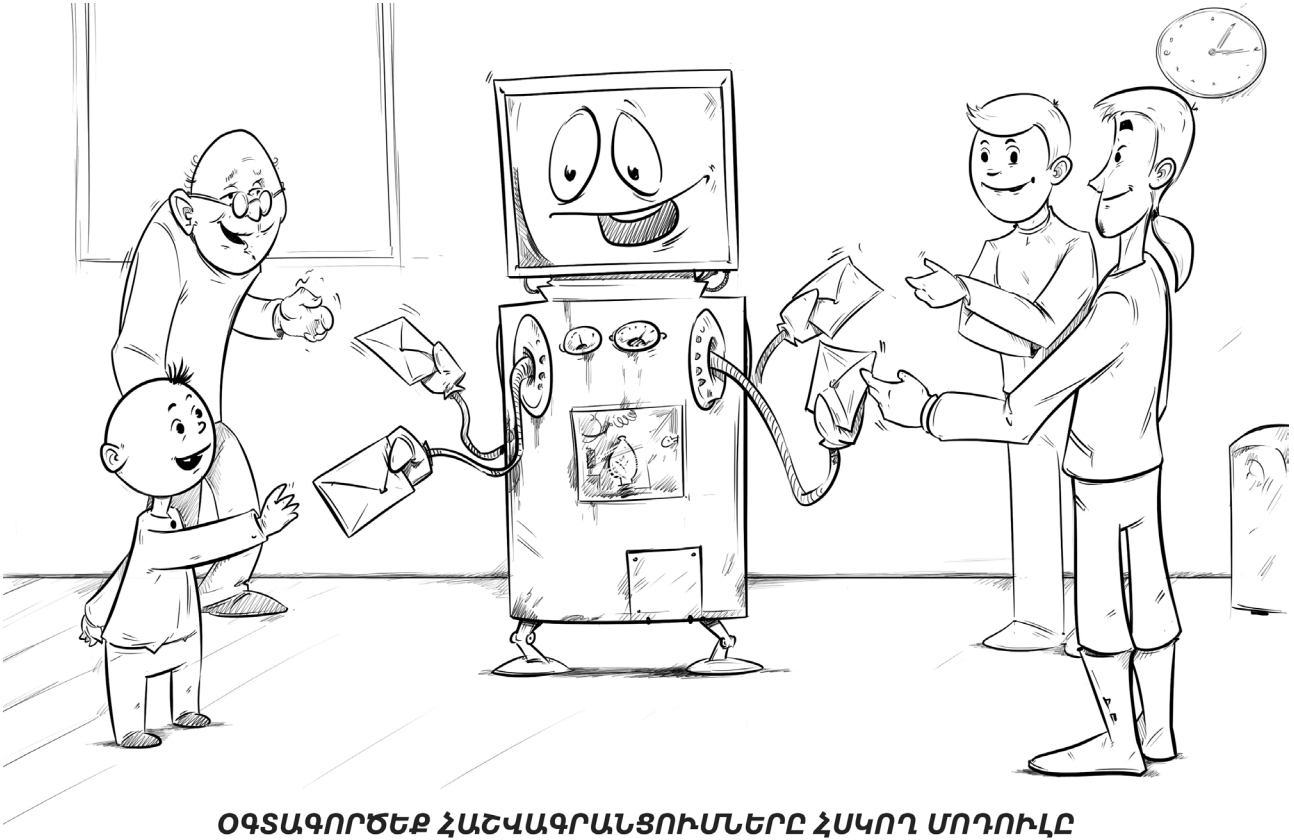
ԽՈՐՀՈՒՐԴ 61: **ԲԱՆԿՈՄԱՏԻ ԸՆՏՐՈՒԹՅՈՒՆԸ**

Ոչ բոլոր բանկոմատներն են հավասարապես վտանգավոր: Հանցագործ-կարդերները սիրում են իրենց գործը անել մեկուսի՝ տեղադրել կամ հանել իրենց սարքավորումները առանց վկաների: Մեկուսի տեղ կարող է լինել բանուկ առևտրի կենտրոնը՝ գնումներով ծանրաբեռնված մարդկանց բազմությունը և կիսաքնած պահակները հնարավորություն են տալիս, որ հանցագործը անի իր «սև գործը» և հեռանա փողերով կամ քարտերի տվյալներով, որոնց մեջ կարող է լինել ձեր քարտը: Լավ բանկոմատն այն է, որը տեղադրված է բանկի բոլոր կողմերից տեսանելի, պահպանվող և տեսախցիկներով դիտարկելի տեղում:

NFC-ՈՎ ՏՎՅԱԼՆԵՐԻ ՓՈԽԱՆՑՈՒՄԸ ԿԱՐՈՂ Է ՕԳՏԱԳՈՐԾՎԵԼ ՎԻՐՈՒՍԻ ՆԵՐԲԵՌՄԱՆ ՀԱՄԱՐ

ԽՈՐՀՈՒՐԴ 62: **ԲԱՐՁՐՏԵԽՆՈԼՈԳԻԱԿԱՆ ՍՊԱՌՆԱԼԻՔ**

Երբեմն այն տպավորությունն է ստեղծվում, որ կապի բոլոր տեսակները մարդիկ ստեղծել են ինչ-որ մեկին վնաս տալու համար: Համացանցը լի է կիբեռսպառնալիքներով, դեռ հնում փոստային աղավնիները փորձում էին կեղտոտել հասցեատիրոջ գլխին, հեռախոսով այսօր էլ հիմար կատակներ են անում, իսկ Հայաստանի Փոստային ծառայությունը ներառել է նախնիների հարուստ փորձը: Թվում էր, թե NFC տեխնոլոգիան («Near Field Communication» - կարճ տարածության վրա գործող կապ) պետք է որ անվնաս լինի, քանի որ գործում է մի քանի սանտիմետր հեռավորության վրա: Ավաղ, արդեն հայտնվել են մեթոդներ, որոնցով հնարավոր է NFC-ով փոխանցվող տվյալները ձեռք գցել կամ վարակել բջջային սարքը: Պետք է հետևել, թե ինչին և ում եք հենում ձեր սմարթֆոնը:



ՕԳՏԱԳՈՐԾԵՔ ՀԱՇՎԱԳՐԱՆՑՈՒՄՆԵՐԸ ՀՍԿՈՂ ՄՈԴՈՒԼԸ

ԽՈՐՀՈՒՐԴ 63: **ՊՐՈՖԻԼՆԵՐ ՕԳՏԱՏԵՐԵՐԻ ՀԱՄԱՐ**

Օգտատերերի հաշվագրանցումները հսկող մոդուլը օգտակար գործիք է, որը հետևում է գործարկված հավելվածների գործողություններին և երբ հայտնաբերում է վտանգավոր ակտիվություն կանգնեցնում է ծրագիրը և էկրանին դուրս է բերում թույլտվության հարցում: Այս մոդուլի միջոցով ընտանիքի անդամների համար կարելի է ստեղծել օգտատերի հաշվագրանցում, ինչը կհեշտացնի նրանց շփումը համակարգչի հետ, իսկ տարբեր վիրուսների համար՝ կդժվարացնի: Եթե անգամ օգտատիրոջ հաշվագրանցումը վարակվի, վիրուսը ադմինիստրատորի իրավունքներ չի ստանա և լուրջ վնաս չի հասցնի:

ՀԱԿԱՎԻՐՈՒՍԸ ԿՄԱՔՐԻ ԴԵՊԻ ԳԻՏԵԼԻՔԸ ՏԱՆՈՂ ՃԱՆԱՊԱՐՀԸ

ԽՈՐՀՈՒՐԴ 64: **ՈՒՍՈՒՄՆԱՌՈՒԹՅՈՒՆԸ ՊԱՇՏՊԱՆՎԱԾ Է**

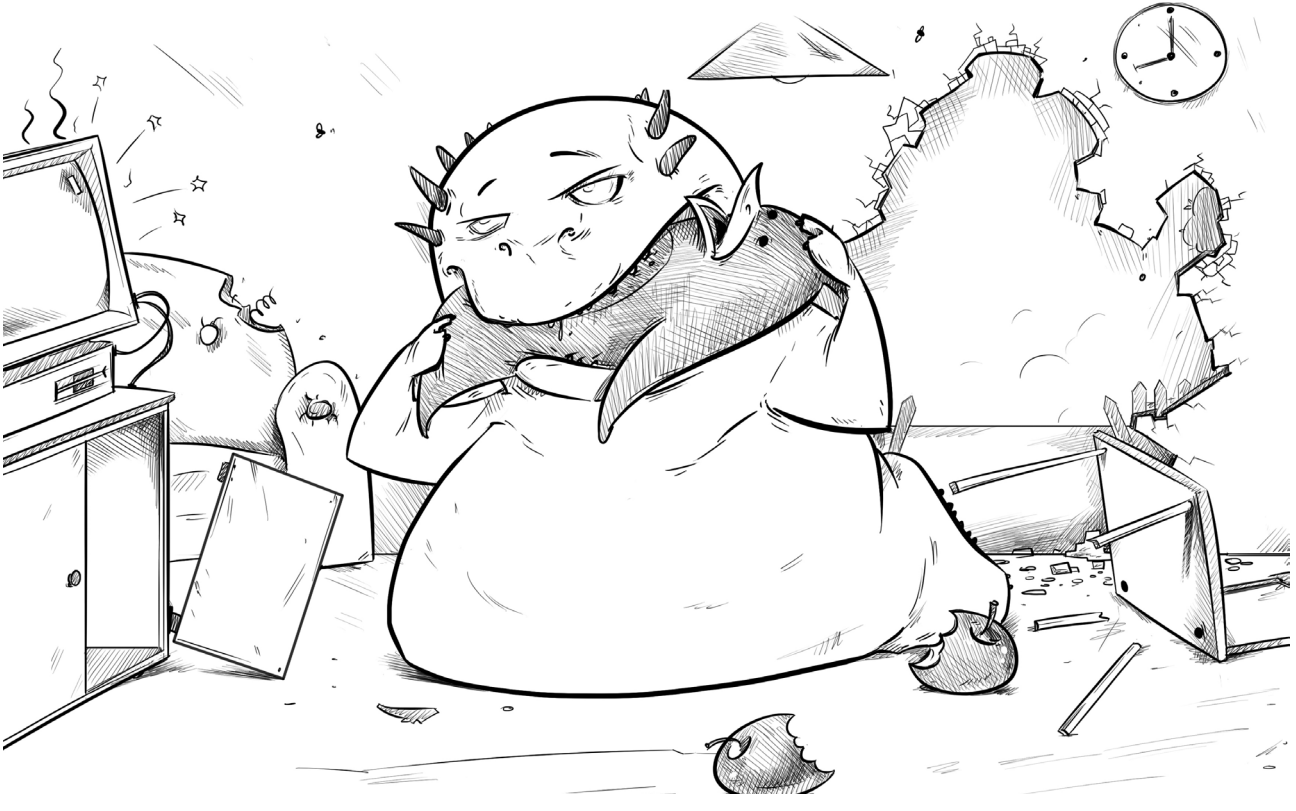
Երբ պատանի Միխայիլ Լոմոնոսովը Ռուսաստանի մի ծայրից գնում էր մյուս ծայրը գիտելիք ստանալու, չար մարդկանցից պաշտպանվելու համար նա միացավ ձուկ տանող գումակին: Անցել է 300 տարի, դեպի գիտելիքը տանող ճանապարհը դարձել է ավելի պարզ և հեշտ, բայց ոչ անվտանգ: Համացանցը շատ արագ պրպտող ուղեղին կտրամադրի ցանկացած ինֆորմացիա, բայց այնտեղ ապրող կիբեռսպառնալիքները հընթացս անախորժություններ կպատճառեն: Անցանկալի գովազդը, անձնական տվյալներ գողանալը, կոշտ սկավառակի ծածկագրումը փող կորզելու նպատակով՝ նվազագույն վնասներն են, որոնցից կարելի է տուժել համացանցում: Ապահովեք երեխայի համակարգչի պաշտպանությունը:

ՄԻ ԹՈՂԵՔ ԵՐԵԽԱՅԻՆ ՄԻԱՅՆԱԿ ՀԱՄԱԿԱՐԳՉԻ ԱՌԱՋ

ԽՈՐՀՈՒՐԴ 65: **ՄԱՆԿԱԿԱՆ ՀԵՏԱՔՐՔՐԱՍԻՐՈՒԹՅՈՒՆ**

Երեխաները շատ հետաքրքրասեր են, այդ պատճառով համակարգչի նման բազմաֆունկցիոնալ սարքը նրանց շատ է հետաքրքրում (ճիշտ այնպես, ինչպես ձեր մեքենան կամ հրացանը, բայց դրանք նրանց համար այնքան էլ հասանելի չեն): Լավ է, որ երեխան նոութբուքով ոչ մեկին չի կարող սպանել, բայց սարքը կարող է տուժել: Տվեք երեխային նրա ռադիոկառավարվող մեքենան և վերցրեք նոութբուքը:

ԻՄԻՋԻԱՅԼՈՑ, ՀԱԿԱՎԻՐՈՒՍԸ ՊԵՏՔ Է ՈՉ ՄԻԱՅՆ WINDOWS-ՕԳՏԱՏԵՐԵՐԻՆ



ԽՈՐՀՈՒՐԴ 66: **ՍՊԱՌՆԱԼԻՔ ԲՈԼՈՐ ՀԱՄԱԿԱՐԳԵՐԻ ՀԱՄԱՐ**

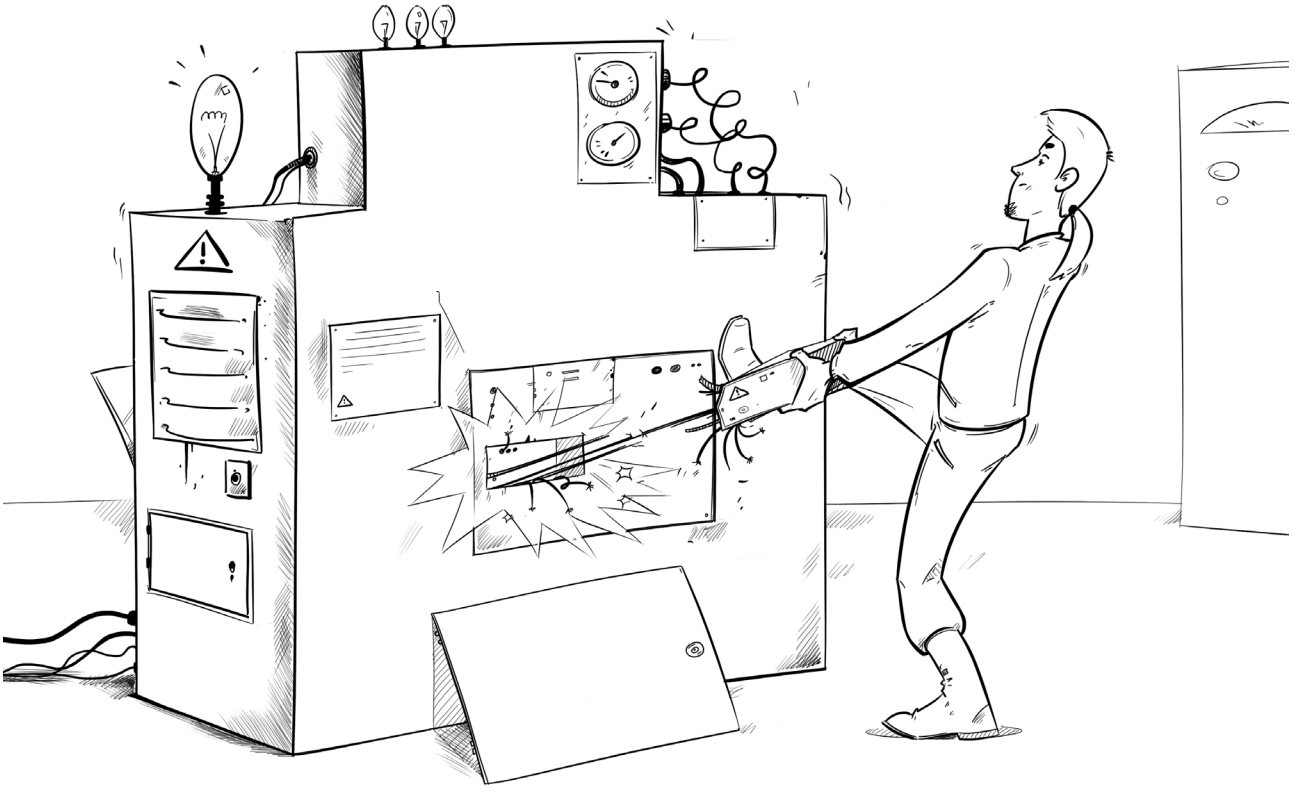
Տարածված է այն կարծիքը, թե վնասատու ծրագրերը գրվում են միայն «Windows»-ի համար, իսկ մյուս հարթակները վտանգված չեն: Այս կարծիքը ճիշտ է այն օպերացիոն համակարգերի համար, որոնք ոչ մեկին պետք չեն: «Linux»-ը և «Mac OS»-ը ունեն լայն տարածում, այդ ծրագրերի օգտատերերը անտեսում են հակավիրուսային ծրագրային ապահովումները և պաշտպանական այլ միջոցառումները և դառնում են ցանցահենների համար թիրախ: Ինչքան էլ քիչ վնասատու ծրագրեր լինեն ձեր օպերացիոն համակարգի համար, մեկ վնասատու ծրագիրը բավական է համակարգչի աշխատանքը խափանելու և արժեքավոր ինֆորմացիա կորզելու համար:

ԱՆՋԱՏԵՔ ԿՐԻՉՆԵՐԻ ԻՆՔՆԱԳՈՐԾԱՐԿՈՒՄԸ

ԽՈՐՀՈՒՐԴ 67: **ՎՏԱՆԳԱՎՈՐ ԿՐԻՉՆԵՐ**

Մենք սովորեցնում ենք շներին գետնից ոչինչ չվերցնել, որպեսզի նրանք չթունավորվեն կամ չխեղդվեն: Մոտավորապես նույն բանը պետք է անի համակարգչի տերը այդ սարքի նկատմամբ: Կրիչի կամ DVD-սկավառակի վրա եղած ֆայլերի ավտոմատ գործարկումը նպաստելու է համակարգչի վարակմանը, եթե այդ ֆայլերում կա վնասատու ծրագրային ապահովում: «Windows»-ի նոր տարբերակներում այդ ֆունկցիան անջատված է, բայց եթե դուք օգտվում եք «Windows XP»-ից՝ պետք է այնպես անել, որ համակարգը մոռանա այդ վատ սովորությունը:

ՀԱՆԵՔ ՍԱՐՔԸ ԱՆՎՏԱՆԳ



ԽՈՐՀՈՒՐԴ 68: **ՏՎՅԱԼՆԵՐԻ ՊԱՀՊԱՆՈՒՄ**

Կրիչի վրա փոխանցել եք ֆայլերը և կրիչը հանել եք համակարգչից: Պատրաստ եղեք այն բանին, որ ֆայլերը այլևս չլինեն համակարգչում: Որքան էլ տարօրինակ է, բայց դա արված է օգտատերերի հարմարության համար: Բանն այն է, որ կրիչը ավելի դանդաղ է գրի առնում տվյալները, քան դրանք հաղորդում է համակարգիչը: Այդ պատճառով փոխանցման պրոցեսի վրա երկար ժամանակ չծախսելու համար «Windows»-ը արձանագրում է հաղորդվող տվյալները հիշողության հատուկ տիրույթում (բուֆեր), որտեղից էլ դրանք աստիճանաբար փոխանցվում են կրիչին: Բուֆերում ինֆորմացիայի վերջին մասը գրանցելուց հետո «Windows»-ը էկրանից հեռացնում է ֆայլերի պատճենման պատուհանը, բայց այդ չի նշանակում գրանցումը ավարտվել է: Եթե պետք է կրիչը շտապ հանել՝ կօգնի սարքը անվտանգ հանելու ֆունկցիան, որի կիրառումից հետո գրառումը հաստատապես կավարտվի:

ՎԵԲ-ՏԵՍԱԽՑԻԿԸ ԿԱՐՈՂ Է ՕԳՏԱԳՈՐԾՎԵԼ ԼՐՏԵՍԵԼՈՒ ՀԱՄԱՐ

ԽՈՐՀՈՒՐԴ 69: **ԱՆՆԿԱՏԵԼԻ ԼՐՏԵՍ**

Վեբ-տեսախցիկը մեծագույն հայտնագործություն է հատկապես նրանց համար, ում ընկերները և հարազատները գտնվում են շատ հեռու: Միջոցներ ձեռնարկեք, որպեսզի ձեր սարքերի տեսախցիկները հանցագործներին չպատմեն ձեր անձնական կյանքի մանրամասները: Ցանցահենները այդ մանրամասները կարող են տարբեր կերպ օգտագործել՝ վաճառել պոռնոկայքերին կամ էլ շանտաժի ենթարկել նկարահանված մարդկանց: Եթե չեք ուզում անհարմար դրության մեջ հայտնվել՝ օգտվեք պաշտպանական միջոցներից, այսօրյա հակավիրուսները կարողանում են հսկել վեբ-տեսախցիկների հասանելիությունը:

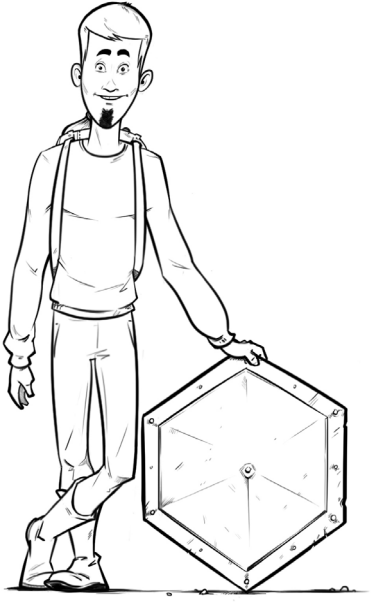
WINDOWS-Ի ՏԵԽՕԳՆՈՒԹՅԱՆ ԱՇԽԱՏԱԿՑԻ ԿԵՐՊԱՐԸ ՇԱՏ ԵՆ ՍԻՐՈՒՄ ԽԱԲԵԲԱՆԵՐԸ

ԽՈՐՀՈՒՐԴ 70: **ԽԱԲԵԲԱՅՈՒԹՅՈՒՆ ՀԵՌԱԽՈՍՈՎ**

«Բարև ձեզ, ես «Windows»-ի տեխ. օգնության աշխատակիցն եմ: Ձեր համակարգչում վտանգավոր վիրուս է հայտնաբերված»: Այսպես ձեզ կարող են դիմել հեռախոսով ձեզ զանգահարած խաբեբաները: Խաբեության սխեման պարզ է՝ հանցագործը համոզում է օգտատիրոջը, որ նրա համակարգիչը վարակված է և խնդրում է կատարել որոշ գործողություններ, որոնք իբր կազատեն վարակից: Իրականում հանցագործի հրահանգները կատարելուց հետո հայտնվում է վնասատու ծրագիրը: Հիշեք՝ ինչքան էլ վիրուս լինի ձեր համակարգչում՝ «Microsoft»-ից ձեզ չեն զանգահարի:

Եթե դուք ուշադիր կարդացիք մեր խորհուրդները, ուրեմն դուք տեղեկացված եք և կարող եք դիմադրել ինֆորմացիոն սպառնալիքներին: Բայց սեփական անվտանգության մեջ համոզվելու համար պետք է զինված լինել՝ տեղադրելով հակավիրուսային ծրագրային ապահովում, օրինակ՝ մեր «Kaspersky Total Security», որի փորձնական տարբերակը կարելի է ներբեռնել https://survival.kaspersky.ru

Խաբեբայական նոր հղումների, կիբեռհանցագործների արդիական օպերացիաների, վիրուսների բնակության և տրոյան ձիերի արածելու տեղերի մասին փնտրեք https://blog.kaspersky.ru մեր բլոգում:



Վիրուսներ, ֆիշինգ, «նիգերիական սպամ»... Մեզ շրջապատում են բազմաթիվ տեղեկատվական սպառնալիքներ, որոնցից պաշտպանվելը գնալով ավելի դժվար է դառնում:

Սակայն «Կասպերսկի Լաբորատորիա»-ի մասնագետները վստահ են, որ յուրաքանչյուրը կարող է յուրացնել տեղեկատվական անվտանգության հիմունքները:

Այս գիրքը պարզ խորհուրդների ժողովածու է, որոնց հետևելը կօգնի հետ մղել թվային գիշատիչներին, որոնք թաքնվում են համացանցում: