4.

## ՊԱՇՏՊԱՆԵ՛Ք ՎԻՐՏՈՒԱԼ ՏԻՐՈՒՅԹՈՒՄ ՁԵՐ «ԹԱՆԿԱՐԺԵՔ ԻՐԵՐԸ»

Ինչպես որ հոգ եք տանում Ձեր տան թանկարժեք իրերի մասին, նույն կերպ էլ պետք է վարվեք այն տեղեկատվության հետ, որ պահում եք վիրտուալ տիրույթում. կլինի դա Ձեր ֆինանսական հաշվետուությունները, անձնագրի սկանը, անգամ Ձեր հասցեն համ հեռախոսի համար. մտածեք՝ որտեղ եք պահում Ձեր ամենաթանկարժեք անձնական տվյալները և ինչպես կարող եք պաշտպանել դրանք:

Կետային մաքրումը հիանալի միջոց է, եթե ցանկանում եք մաքրել սուրճից մնացած հետքը: Ձեր փոստային հասցեում կամ այլ օգտահաշիվներում որոնեք Ձեր մասին զգայուն տեղեկատվությունը և հեռացրեք այն, օրինակ՝ նույնականացման քարտի սկան, բանկային տվյալներ, առողջապահության ապահովագրություն: Եթե դա այնպիսի բան է, որ հետո Ձեզ պետք է գալու, միշտ կարող եք ներբեռնել կամ տպել այն՝ նախքան ջնջելը:

Խորը մաքրումը ավելի մանրամասն մաքրումն է, և ցանկալի է, որ դա անեք տարին մեկ անգամ: Արխիվացրե՛ք Ձեր փոստային հասցեում կամ սոցմեդիայի օգտահաշիվներում ցանկացած բան, ներբեռնե՛ք այն Ձեր համակարգչի մեջ, հեռացրե՛ք օգտահաշվի ամբողջ կոնտենտը և սկսե՛ք զրոյից:

Խորհուրդ. ոչ միայն պարզապես ջնջեք, դատարկեք նաև Ձեր trash զամբյուղը և հեռացրեք ժամանակավոր ֆայլերը:

Որոշողը Դուք եք՝ արդյուք ուզում եք Ձեր արխիվները և փաստաթղթերը տեղափոխել ամպային համակարգ, թե պահել այն կրիչի կամ արտաքին կոշտ սկավառակի վրա: Որտեղ էլ որ պահեք՝ համոզվեք, որ չեք կորցնելու այն, և որ այն պաշտպանված է ուժեղ գաղտնաբառով:

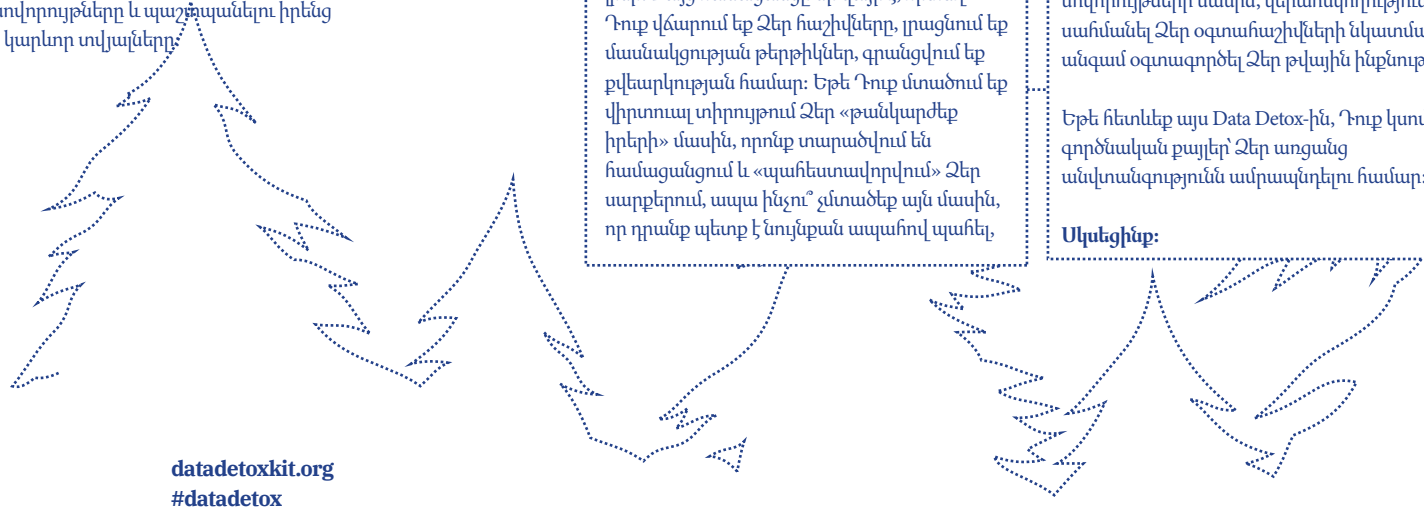
5.

## ՓՈԽԱՆՑԵ՛Ք

Մենք հաճախ մոռանում ենք, որ համացանցը իզուր չէ՝ որ «ցանց» են անվանում: Այսպես թե այնպես, մենք բոլորս կապված ենք միմյանց հետ. ոչ միայն որպես «ընկերներ» սոցիալական ցանցներում, այլև էլեկտրոնային հասցեի կոնտակտներով, մեր տարածած լուսանկարներով: Պաշտպանելով ձեր օգտահաշիվները՝ ուժեղացրեք գաղտնաբառերը և հեռացրեք անձնական տվյալները: Դրանից կշահեք ոչ միայն Դուք, այլև Ձեզ հետ կապված մարդիկ նույնպես կստանան լրացուցիչ անվտանգություն:

Մաքրելով Ձեր էլեկտրոնային փոստը կամ սոցիալական ցանցերը՝ մտածեք էլ ինչ կարող եք ներբեռնել կամ հեռացնել, ինչպես դա կարող է օգնել Ձեր ընկերներին կամ գործընկերներին. Ձեր քրոջ բանկային տվյալները, գրասենյակի մուտքի ծածկագիրը կամ երեխայի անձնագրի սկանը. այդ տվյալները, հայտնվելով ուրիշի ձեռքում, կարող են լուրջ խնդիրներ ստեղծել:

Պատմե՛ք այդ մասին: Թվային անվտանգությունն ուժեղացնելու համար բավական է մի քանի քայլ ձեռնարկել: Կիսվեք Data Detox-ի տվյալներով Ձեր ընկերների, գործընկերների և ընտանիքի անդամների հետ, որպեսզի օգնեք նրանց փոխելու իրենց սովորույթները և պաշտպանելու իրենց համար կարևոր տվյալները:



DATA DETOX KIT

# ՓՈԽԵ՛Ք ԿԱՐԳԱՎՈՐՈՒՄՆԵՐԸ

անձնական տվյալները պաշտպանելու համար

Եթե համացանցը լիներ մի վայր, որտեղ պարզապես տեղադրում են դինոզավրի համազգեստով շների նկարներ, գաղնաբառերի կարիք այդքան էլ շատ չէր լինի: Բայց համացանցը մի վայր է, որտեղ Դուք վճարում եք Ձեր հաշիվները, լրացնում եք մասնակցության թերթիկներ, գրանցվում եք քվեարկության համար: Եթե Դուք մտածում եք վիրտուալ տիրույթում Ձեր «թանկարժեք իրերի» մասին, որոնք տարածվում են համացանցում և «պահեստավորվում» Ձեր սարքերում, ապա ինչու՞ չմտածեք այն մասին, որ դրանք պետք է նույնքան ապահով պահել,

Գոյություն ունի մի պարզ միջոց, որը կարող է բարդացնել մյուսների գործը՝ հասանելիություն ստանալ Ձեր վիրտուալ «թանկարժեք իրերին». այնպես մի՛ արեք, որ նրանք հեշտությամբ գուշակեն Ձեր գաղտնաբառը: Շատ մարդկանց համար պարտադիր չէ մասնագիտացված տեխնիկական հմտություններ՝ Ձեր հաշիվներ մուտք գործելու համար. նրանք դա կարող են անել՝ պարզապես մի քանի հարցերի պատասխան գուշակելով կամ ծրագրի միջոցով:
Եվ եթե նրանց արդեն հաջողվել է մուտք գործել Ձեր հաշիվներից մեկը, նույն գաղնաբառը նրանք կարող են կիրառել այլ օգտահաշիվների վրա, տեղեկատվություն հավաքել Ձեր և Ձեր սովորույթների մասին, վերահսկողություն սահմանել Ձեր օգտահաշիվների նկատմամբ և անգամ օգտագործել Ձեր թվային ինքնությունը:

Եթե հետևեք այս Data Detox-ին, Դուք կսովորեք գործնական քայլեր՝ Ձեր առցանց անվտանգությունն ամրապնդելու համար:

**Սկսեցինք:**

արտադրանք՝
TACTICAL TECH

Աջակցում է՝
Firefox

**datadetoxkit.org**
**#datadetox**

# 1.

## ՓԱԿԵ՛Ք ՁԵՐ ԹՎԱՅԻՆ ԴՌՆԵՐԸ

Կողպե՛ք էկրանը. գաղտնաբառը, նախշերը, մատնահետքը, դեմքի նույնականացումը, որ Դուք օգտագործում եք, մի քանիսն են լավագույն պաշտպանական միջոցներից, որոնք կարող եք կիրառել նրանց դեմ, ովքեր ցանկանում են հասանելիություն ստանալ Ձեր սարքին: Բայց կան բազմաթիվ այլ միջոցներ, ուստի կարող եք դժվարանալ հասկանալ՝ որը կարող է ճիշտ լինել Ձեզ համար:

Հեռախոսի, թաբլեթի կամ համակարգչի վրա ցանկացած տեսակի «կողպեք» ունենալը Ձեզ ավելի ապահով է դարձնում, քան ընդհանրապես ոչինչ չունենալը: Եվ չնայած դրների վրա դնելու տարբեր տեսակի կողպեքներ կան, դրանց մի մասն ավելի ամուր են, քան մյուսները:

Բոլոր կողպեքներից երկար, ինքնատիպ գաղտնաբառերն ամենաուժեղն են: Դա նշանակում է, որ Ձեր գաղտնաբառը պետք է պարունակի տառեր, թվեր և հատուկ նիշեր: Օրինակ, եթե Դուք օգտագործում եք գաղտնաբառի կողպեքը, կարող եք ավելի երկար գաղնաբառ դնել: Նախշերո՞վ գաղտնաբառ եք օգտագործում: Գուցե նախշն ավելի՞ երկարացնեք: Կամ եթե օգտագործում եք 1234 PIN-ը, գուցե փոխարենը 7 անգամ զառ գցեք և 7 նիշանոց գաղտնաբա՞ռ կազմեք: Փոքրիկ փոփոխությունը կարող է երկար ժամանակ պահել վերահսկողությունը Ձեր սարքերի վրա:

# 2.

## ԸՆՏՐԵ՛Ք ՃԻՇՏԸ

Որակյալ գաղտնաբառ կազմելը հեշտ է: Դրա համար պարզապես պետք է հետևեք մի քանի հիմնական սկզբունքների: Ձեր գաղտնաբառը պետք է լինի.

Երկար. **գաղտնաբառը պետք է բաղկացած լինի առնվազն 8 նիշից: Ավելի լավը լինելու համար՝ 16-20 նիշից:**

Ինքնատիպ. **յուրաքանչյուր կայքի համար օգտագործեք տարբեր գաղտնաբառեր:**

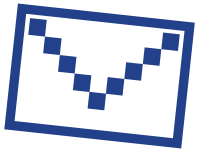
Պատահական. **Ձեր գաղտնաբառը չպետք է որոշակի տրամաբանական հաջորդականություն ունենա կամ հեշտ լինի գուշակել: Այստեղ շատ օգտակար են գաղտնաբառերի մենեջերները:**

**Ամենաուժեղ գաղտնաբառը թվերի, տառերի և հատուկ նշանների համակցությունն է:** Այս արժեքավոր խորհրդին հետևելով՝ կարող եք կազմել ավելի ուժեղ և դժվար գուշակվող գաղտնաբառ: Գաղտնաբառերի որոշ համակարգեր, ցավոք, թույլ չեն տալիս Ձեզ օգտագործել հատուկ նիշեր (օրինակ՝ @#$%-=+), բայց տառերի և թվերի երկար համակցումը ավելի լավ է, քան կարճ գաղտնաբառը:
Գաղտնաբառեր գեներացնելու կամ դրանք պահելու համար լավ կլինի օգտագործեք գաղտնաբառերի մենեջերներ, օրինակ 1Password and KeePassXC, որոնք ամենաշատն են խորհուրդ տրվում անվտանգության փորձագետների կողմից. սրանք հավելվածներ են, որոնց նպատակն է պաշտպանել Ձեր գաղտնաբառը և այլ զգայուն տվյալներ:

# 3.

## ԱՎԵԼԱՑՐԵ՛Ք ԵՐԿՐՈՐԴ ԲԱՆԱԼԻՆ

Միացրեք երկքայլ (2FA) կամ բազմաքայլ (MFA) հաստատում, ինչը նշանակում է, որ անգամ եթե որևէ մեկը գտնում է Ձեր գաղտնաբառը, Ձեր օգտահաշիվ մուտք գործելու համար նրան հասանելի չեն լինի լրացուցիչ տվյալները:



Աչքի անցկացրեք Ձեր կողմից ամենաշատ օգտագործվող կայքերի և հավելվածների անվտանգության կարգավորումները՝ տեսնելու՝ արդյոք կարող եք տեղադրել այդ լրացուցիչ բանալին: Սկսեք ամենակարևորներից՝ ֆինանսական հավելվածներ կամ փոստային հասցեների ծառայություններ, որոնք Դուք օգտագործում եք վերականգնելու Ձեր մյուս օգտահաշիվները:


Google.
**Մուտք գործեք. myaccount.google.com →**
**Անվտանգություն →**
**Երկքայլ հաստատում →**
**Միացնել**

Facebook.
**Մենյու →**
**Կարգավորումներ →**
**Անվտանգություն և Լոգին →**
**Միացնել երկքայլ հաստատում**

**Խորհուրդ.** հաստատման հաջորդ քայլը կարգավորելիս Դուք պետք է Ձեր անձը հաստատելու երկրորդ ուղի ընտրեք: Աշխատեք խուսափել SMS-ի տարբերակից (երբ տեքստային հաղորդագրություն է ուղարկվում Ձեր հեռախոսահամարին)՝ որպես երկրորդ քայլ, քանի որ կարող եք կորցնել Ձեր հեռախոսը: Էլփոստը սովորաբար ավելի հուսալի