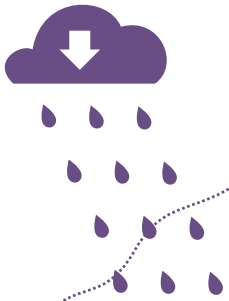
4.

ՄԱՔՐԵ՛Ք ՀԵՏՔԵՐԸ

Ձեր հեռախոսի բրաուզերը պահպանում է հսկայական քանակությամբ տեղեկատվություն՝ Ձեր գտնվելու վայրը, ինչ որոնում եք կատարել, ինչ կայքերից եք օգտվում, և կարող է «բաց թողնել» այդ տեղեկատվությունը: Դուք կարող եք որոշակի վերահսկողություն հաստատել այդ տեղեկատվության նկատմամբ՝ կատարելով մի քանի փոփոխություններ:
Հեռախոսներում, թաբլեթներում և համակարգիչներում սովորաբար տեղադրված են լինում բրաուզերներ, որոնց համար Ձեր գաղտնիությունը առաջնահերթություն չէ: Փոխարենը, Դուք կարող եք ներբեռնել և օգտագործել բրաուզերներ, որոնք Ձեր ցանցային գործունեությունը առավել գաղտնի են պահում և կարող են հեռու պահել Ձեզ թրեքերներից:
«Լրտեսությունից» զերծ մնալու համար Դուք կարող եք ավելացնել որոշ անվտանգության ուժեղացման ֆունկցիաներ՝ add-on-ներ կամ extension-ներ, (գոյություն ունեն հեշտությամբ ներբեռնվող մինի-ծրագրեր Ձեր բրաուզերների համար, որոնք կարող են Ձեր առցանց գործունեությունն ավելի գաղտնի դարձնել):

Լրտեսական գովազդներն ու անտեսանելի թրեքերներն արգելափակելու համար ներբեռնեք **uBlock Origin** (Chrome-ի, Safari-ի, Firefox-ի համար) կամ **Privacy Badger** (Chrome-ի, Firefox-ի և Opera-ի համար):

Որպեսզի համոզվեք, որ Ձեր կապերը կայքերում հնարավորինս անվտանգ են, ներբեռնեք HTTPS Everywhere: դա բրաուզերի extension է, որպեսզի Ձեր հաղորդակցությունը բազմաթիվ խոշոր կայքերի հետ գաղտնագրվի և պաշտպանված լինի: Եթե Դուք Safari-ի օգտատեր եք և ցանկանում եք օգտվել սրանից, Ձեր հիմնական որոնման համակարգ դարձրեք ոչ-Google պրոդուկտ, օրինակ DuckDuckGo, որն ավտոմատ կերպով Ձեզ կուղղորդի դեպի գաղտնագրված կապեր:



DATA DETOX KIT

ՎԵՐԱՀՍԿԵՔ ՁԵՐ ՍՄԱՐԹՖՈՆԻ ՏՎՅԱԼՆԵՐԸ

ցանցում գաղտնիություն պահելու համար

Երբեմն կարող եք մտածել՝ իսկ ինչ պիտի պատմեն Ձեր տվյալները Ձեր մասին, թվում է՝ մի մեծ բան չէ. ում է պետք, թե Դուք ինչ երաժշտություն եք լսում, ինչ կոշիկ եք գնում, կամ արդյոք Ձեր արձակուրդը մեկ տարի առաջ եք սկսում պլանավորել:

Խնդիրն այն է, թե ինչ է տեղի ունենում Ձեր տվյալների հետ: Ժամանակի ընթացքում դրանց համակցությունից ձևավորվում է թվային պատկեր՝ Ձեր նախասիրությունները, տեղաշարժերը, հավատալիքները, սովորույթները, և այդ տվյալները կարող են հասանելի դառնալ նրանց, ովքեր վերլուծում են դրանք և օգուտ ստանում, օրինակ բիզնես ընկերություններին և տվյալների բրոկերներին:

Եթե հետևեք այս Data Detox-ին, կտեսնեք՝ ինչու և ինչպես է այդ ամենը կատարվում և գործնական քայլեր կձեռնարկեք վերահսկելու Ձեր տվյալները համացանցում:

Սկսեցինք:

5.

ՀԵՌԱՑՐԵ՛Ք ԹԵԳԵՐԸ ՁԵՐ ԵՎ ՈՒՐԻՇՆԵՐԻ ՎՐԱՅԻՑ

Նախկինում երբևէ նպաստե՞լ եք Ձեր ընկերների տվյալների ավելացմանը՝ նրանց պիտակելով նկարներում և հրապարակումներում:

Թեթևացրեք նրանց տվյալների ծանրաբեռնվածությունը հնարավորինս բոլոր նկարների և հրապարակումների վրայից՝ հանելով նրանց թեգերը:

Փոխանակվե՛ք. Խրախուսեք Ձեր ընկերներին, ընտանիքի անդամներին և գործընկերներին միանալ Ձեզ՝ վերահսկելու «ազատ» տեղեկատվությունը: Եթե մենք բոլորս միասին աշխատենք մեր տվյալների հետքերը վերահսկելու ուղղությամբ՝ ավելի լավ արդյունքի կարող ենք հասնել:

արտադրանք՝
TACTICAL TECH

Աջակցում է՝
Firefox

datadetoxkit.org
#datadetox

1.

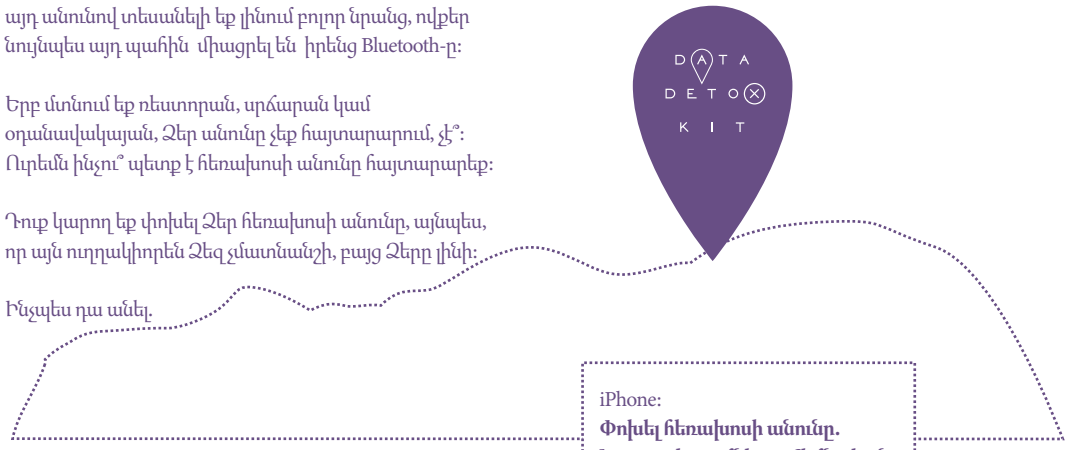
ՓՈԽԵ՛Ք ՍԱՐՔԻ ԱՆՈՒՆԸ

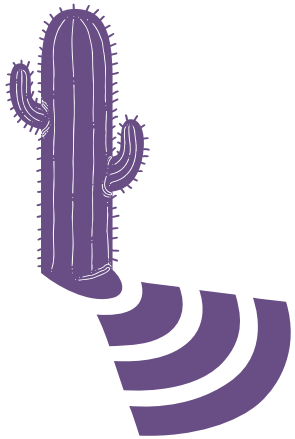
Ինչ-որ պահի Դուք Ձեր Wi-Fi-ին, Bluetooth-ին (կամ երկուսին էլ) անուն եք դրել, գամ գուցե անունն ավտոմատ կերպով է գերներացվել կարգավորումների ժամանակ: Դա նշանակում է, որ Wi-Fi-ի ցանցի սեփականատիրոջ մոտ Դուք երևում եք որպես “Alex Chung’s Phone” (Ալեքս Չանգի հեռախոս), կամ եթե Ձեր Bluetooth-ը միացված է, այդ անունով տեսանելի եք լինում բոլոր նրանց, ովքեր նույնպես այդ պահին միացրել են իրենց Bluetooth-ը:

Երբ մտնում եք ռեստորան, սրճարան կամ օդանավակայան, Ձեր անունը չեք հայտարարում, չէ՞: Ուրեմն ինչու՞ պետք է հեռախոսի անունը հայտարարեք:

Դուք կարող եք փոխել Ձեր հեռախոսի անունը, այնպես, որ այն ուղղակիորեն Ձեզ չվատնանշի, բայց Ձերը լինի:

Ինչպես դա անել.





iPhone:
Փոխել հեռախոսի անունը.
Կարգավորումներ → Հիմնական→
Այս սարքի մասին → Անուն

Android:
Փոխել Wi-Fi-ի անունը
Կարգավորումներ→
Wi-Fi → Մենյու →
Ընդլայնված կարգավորումներ /
Լրացուցիչ→
Wi-Fi ուղիղ → Վերանվանել սարքը
Փոխել Bluetooth-ի անունը.
Կարգավորումներ→ Bluetooth →
Միացնել Bluetooth-ը, եթե այն
անջատված է → Մենյու→
Վերանվանել սարքը→
Միացրեք Bluetooth-ը

2.

ՋՆՋԵ՛Ք ՏԵՂԱՇԱՐԺԻ ՀԵՏՔԵՐԸ

Եթե Ձեզ թվում է, որ Ձեր տեղաշարժի մասին տվյալները պարզապես տեղեկատվության խառը կտորներ են, համակցության մեջ դրանք կարող են կարևոր տեղեկություն բացահայտել Ձեր և Ձեր սովորույթների մասին, օրինակ՝ որտեղ եք ապրում, աշխատում և որտեղ եք սիրում ժամանակ անցկացնել ընկերների հետ: Բազմաթիվ ընկերությունների և դատա-բրոկերների համար դա մեծ պահանջարկ ունեցող տեղեկություն է:

Դրա համար անցեք Ձեր հավելվածների թույլտվությունների վրայով և անջատեք գտնվելու վայրի ծառայությունները: Գտեք այն հավելվածները, որոնց համար այդ ծառայությունը պարտադիր չէ (իսկապե՞ս կարևոր է, որ այդ խաղն իմանա Ձեր գտնվելու վայրը) և նրանք, որոնք Դուք չեք ցանկանում, որ ունենան այդ տվյալը:

3.

ՄԱՔՐԵ՛Ք ՀԱՎԵԼՎԱԾՆԵՐԸ

Ձեր սոցմեդիա հավելվածները, խաղերը և եղանակի տեսության հավելվածները հետաքրքրված են Ձեր տվյալներով... և գուցե արդեն հավաքել են դրանք:

Ձեր հեռախոսում այսպիսի պատահական հավելվածներից հրաժարվելը, որոնք անգամ չեք էլ օգտագործում, կարող է հզոր միջոց լինել Ձեր թվային հետքերը վերացնելու գործում:

Բացի այդ, դրա արդյունքում Դուք կարող եք տեղ ազատել Ձեր հեռախոսում և երկարաձգեք մարտկոցի կյանքը:

Android:
Կարգավորումներ →
Հավելվածներ → Գտնվելու վայր

iPhone:
Կարգավորումներ →
Գաղտնիություն → Գեոլոկացիայի
ծառայություններ → Յուրքանչյուր
հավելվածի գտնվելու վայրի

Android:
Կարգավորումներ →
Հավելվածներ →
Ընտրեք այն հավելվածը, որից
ուզում եք ազատվել → Հեռացնել

iPhone:
Սեղմեք և սեղմած պահեք տվյալ
հավելվածը, մինչև որ բոլոր
հավելվածները կսկսեն թրթռալ և
նրանց բոլորի վերևի ձախ
անկյունում կերևա փոքրիկ խաչ:
Հավելվածը հեռացնելու համար
սեղմեք տվյալ հավելվածի վրայի
խաչը:
Հետո կարող եք վերադառնալ
նախկին վիճակին:

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:

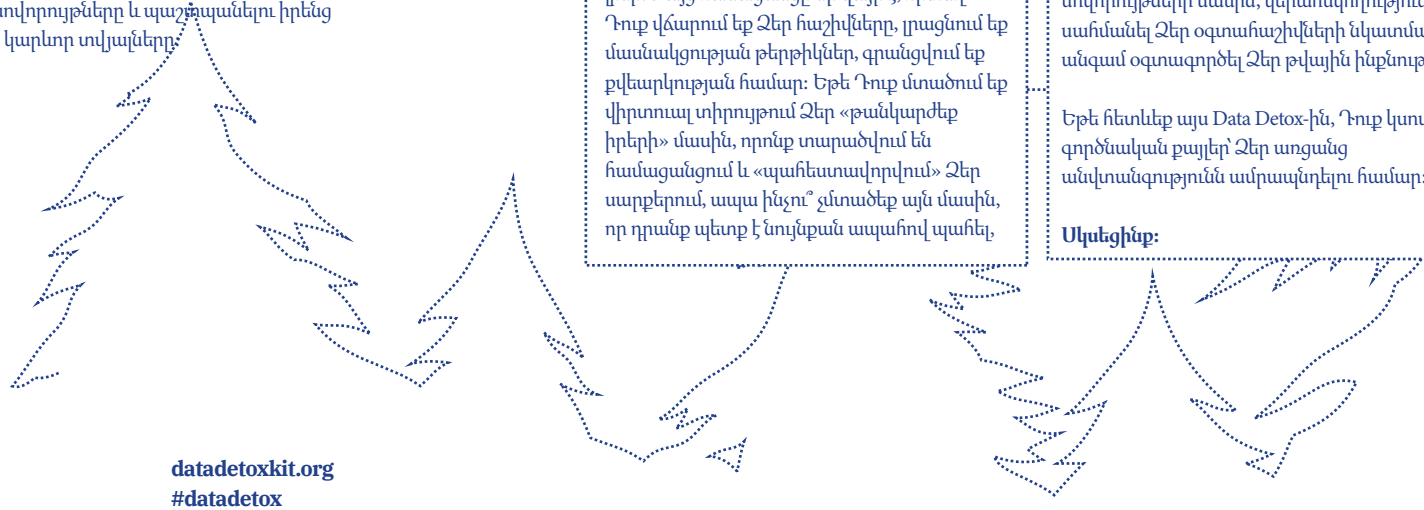
5.

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:**

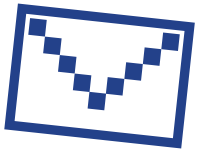
Պատահական. **Ձեր գաղտնաբառը չպետք է որոշակի տրամաբանական հաջորդականություն ունենա կամ հեշտ լինի գուշակել: Այստեղ շատ օգտակար են գաղտնաբառերի մենեջերները:**

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

4.

ՉԵՋ ԼՍԵԼԻ՛ ԴԱՐՁՐԵՔ

Եթե Ձեզ դուր չի գալիս Ձեր կողմից շատ այցելվող/օգտագործվող կայքերի կամ հավելվածների կպչուն դիզայնը կամ սխալ տեղեկատվություն եք տեսնում, Դուք կարող եք նրանց էլհասցեին նամակ գրել, թվիթ անել և նրանց տեղյակ պահել, որ համաձայն չեք դրա հետ: Եթե ընկերությունների վրա ճնշում է գործադրում նրանց ամենաարժեքավոր ակտիվը՝ օգտատերերը, կա հավանականություն, որ նրանք կփոխվեն:

Եթե Ձեզ թվում է, որ Ձեր արձագանքը տեղ չի հասել, ավելի հզոր բան կա, որ կարող եք անել. օգտվեք այլ հավելվածից կամ կայքից: Եթե Դուք տեղյակ եք պահել, որ տվյալ կայքում կամ հավելվածում ինչ-որ բան Ձեզ դուր չի գալիս և հետո դադարել եք դրանից օգտվել, և եթե բավարար չափով մարդիկ դա անեն, նրանք կնկատեն:

5.

ԽՈՍԵ՛Ք ԱՅԴ ՄԱՍԻՆ

Փոխանցեք: Այս խորհուրդը հեշտությամբ կարող եք մոռանալ, բայց այն կարող է մեծ ազդեցություն ունենալ: Պատմեք Ձեր ընկերներին, ընտանիքի անդամներին, գործընկերներին այն ամենը, ինչ նկատում եք, և անգամ խնդրեք նրանց միանալ Ձեզ և դետոքսիկացվել: Բոլորն էլ պայքարում են իրենց հեռախոսային սովորույթները կարգավորելու հարցում: Կարևորն այն է, որ Դուք գտնեք այն ուղին, որը Ձեզ համար ճիշտ կլինի, և որը համապատասխանում է Ձեր կենսակերպին: Փորձարկումներ արեք, մինչև որ գտնեք՝ որն է Ձեզ համապատասխանում, հետո թարմացրեք Ձեր սովորույթները, քանի որ ժամանակի ընթացքում Ձեր կարիքները փոխվում են:

Եվ վերջապես, Ձեր տեխնիկական նախընտրությունների մասին տեղյակ պահեք Ձեր շրջապատին: Օրինակ, եթե Դուք որոշել եք, որ ժամը երեկոյան 8-ից հետո անհասանելի եք լինելու մեսենջերով, այդ մասին հայտնեք Ձեր ընտանիքի անդամներին, որպեսզի նրանք փոխարենը Ձեզ զանգահարեն: Այդ երկխոսությունը բաց պահեք, հարցեր տվեք և կարող եք ունենալ առավել հավասարակշռված առցանց կյանք, որը համապատասխանում է Ձեզ:

DATA DETOX KIT

ԽՈՒՍԱՓԵ՛Ք «ԼՌԵԼՅԱՅՆ»-ԻՑ

Ձեր թվային բարեկեցությունն ամրապնդելու համար

Որքան ժամանակ է, որ դուք կտրվել եք համացանցից և ամբողջ օրվա ընթացքում թեկուզ և մեկ ժամ չեք մոտեցել Ձեր սարքերին: Եթե Դուք մշտապես առցանց եք, իմացեք՝ Դուք մենակ չեք: Ինչպե՞ս կարող եք վստահ լինել, որ սմարթֆոնն օգտագործում եք ի շահ Ձեզ:

Նշենք, որ սարքերի նկատմամբ Ձեր անհաղթահարելի ձգտումը Ձեր մեղավորությունը չէ: Հավաքում եք, թե ոչ՝ Ձեր բոլոր սիրելի հավելվածները և կայքերը մշակված են այնպես, որ յուրաքանչյուր գործառույթ, գոյն կամ ձայն «օպտիմիզացվել են»՝ Ձեզ կառչած պահելու համար: Վաճառքով հետաքրքրված ընկերությունները շահագրգռված են, որպեսզի օգտատերերը մշտապես վերադառնան՝ ավելի շատ ինֆորմացիա ստանալու համար:

Ցանկանու՞մ եք հավասարակշռություն գտնել Ձեր օնլայն և օֆլայն կյանքի միջև: Հենց այդպիսի նպատակ է դրել Data Detox-ը:

Սկսեցինք:

արտադրանք՝
TACTICAL TECH

Աջակցում է՝
Firefox

datadetoxkit.org
#datadetox

1.

ԱՊՐԵՔ ԱՅՍՏԵՂ ԵՎ ԱՅՍ ՊԱՀԻՆ

Այս խորհուրդն ավելի դաժան է, քան թվում է: Մշտապես կենտրոնացած լինելը ամենօրյա ջանք է պահանջում: Դա նման է ուղեղի մկանի, որը պետք է պարբերաբար մարզել, որպեսզի կարողանաք հույս դնել դրա վրա: Կարող եք սկսել նրանից, որ նկատեք Ձեր հարաբերություններն այն տեխնոլոգիաների հետ, որոնք օգտագործում եք:

Որքա՞ն ժամանակ եք ծախսում հեռախոսի մեջ

Եթե պատասխանը Ձեզ դուր չի գալիս, կան կարգավորումներ և ռազմավարություններ, որոնց կարող եք հետևել՝ Ձեր տեխնիկայի վրա վերահսկողություն սահմանելու համար:

Եթե Ձեր նպատակն է ավելի քիչ ժամանակ ծախսել Facebook-ում, Instagram-ում կամ Snapchat-ում, փոխեք այդ հավելվածների կարգավորումներն ու թույլտվություններն այնպես, որ Ձեզ համար հարմար տարբերակով աշխատեն:
Որոշ հավելվածներ, օրինակ Instagram-ը անգամ տարբերակ ունեն, երբ հավելվածը Ձեզ հիշեցնում է, որ Դուք հասել եք Ձեր օրվա առավելագույնին:

Instagram:
Պրոֆայլ → Մենյու → Կարգավորումներ→ Օգտահաշիվ→ Ձեր գործունեությունը→ Սահմանել օրական հիշեցում

Եթե կարծում եք, որ Ձեր հեռախոսը փչացնում է իրական կյանքում Ձեր զրույցները դռռոցով, զնգոցով կամ լույսով, կարող եք այն ժամանակավորապես դնել լուռ ռեժիմի վրա, «դեմքով» դեպի սեղանը, և անգամ թողնել պայուսակում կամ գրպանում՝ աչքից հեռու:

2.

ՈՒՇԱԴՐՈՒԹՅՈՒ՛Ն ԴԱՐՁՐԵՔ ԴԻԶԱՅՆԻ ՀՆԱՐՔՆԵՐԻ ՎՐԱ

Համոզիչ դիզայնը, որը նաև անվանում են «մութ նախշեր» (dark patterns) հիմնված է մարդկային հոգեբանության վրա, որի նպատակն է ստիպել Ձեզ մուտք գործել, գնել ինչ-որ բան կամ տրամադրել ավելի շատ անձնական տվյալներ, քան նախատեսում էիք:
Ընդհանուր դիզայնի գործիքները կարող են ներառել որոշակի գույներ, կոճակներ, ոչ հստակ տեքստ կամ ոչ լիարժեք տեղեկատվություն: Երբեմն այս հնարքներն ակնհայտ են, բայց երբեմն դրանք դժվար է նկատել:
Դրանց մի մասը գուցե Դուք նկատել եք առցանց առևտրի կայքերում գրանցվելիս կամ բաժանորդագրվելիս:
Պատճառը, որ Դուք ամենուր տեսնում եք դիզայնի այս հնարքները, այն է, որ դրանք աշխատում են. դրանք ստիպում են մեզ սեղմել, բաժանորդագրվել, ավելի հաճախ գնել և կրկին ու կրկին վերադառնալ: Որքան շատ իմանաք Ձեր կողմից օգտագործվող կայքերում ներդրված նուրբ հիշեցումների և մանիպուլյացիաների մասին, այնքան ապահով և տեղեկացված կդառնաք:

Գոյություն ունեն մի շարք հնարքներ, որոնց միջոցով կարող եք հիմարացնել Ձեր հավելվածներին:

Իմացեք՝ երբ են Ձեզ «գայթակղում». առաջին բանը, որ կարող եք անել՝ պարզապես իմացեք, որ Ձեր նկատմամբ կիրառվում է այս տեխնիկան:

Սքրինշո՛թ արեք և տարածե՛ք. ամեն անգամ, երբ հանդիպում եք համոզիչ դիզայնի տարրերի, սքրինշոթ արեք և տարածեք Ձեր ընկերների շրջանում (բնականաբար ջնջելով անձնական տվյալները (գաղտնիությունն ամենակարևորն է)): Կարող եք նաև դիմել ընկերությանը՝ դա փոխելու առաջարկով:

Հանգստություն պահպանեք. Եթե առևտրային էջում հետհաշվարկի ժամացույց կա, հարց տվեք ինքներդ Ձեզ՝ արդյոք սա իսկապես հրատապ է: Եթե Ձեզ բռնեցնում եք այն մտքի վրա, որ սեղմեցիք կոճակը, չնայած որ չէիք ուզում, մտածեք՝ ինչ բառեր է օգտագործել ծառայությունը այդ կոճակի վրա, կամ ինչ գույն ունի այն: Եթե մտահոգվեցիք, պետք չէ անմիջապես մտածել, որ Դուք եք մեղավոր. հաշվի առեք կայքի կամ հավելվածի կողմից օգտագործվող ձևակերպումները, քանի որ դրանք կարող են ոչ հստակ լինել:

3.

ԵՂԵ՛Ք ՄԵԴԻԱԳՐԱԳԵՏ

Եթե Դուք կարող եք հիմարացնել այդ հնարքներն ու դիզայնի տարրերը, որոնց նպատակն է Ձեզ ստիպել անվերջ ներքև իջնել և սեղմել, ապա Դուք կարող եք նաև ավելի խելացի գտնվել՝ հայտնաբերելու այն հրապարակումներն ու պատկերները, որոնց նպատակը Ձեզ մոլորեցնելն է:

Մինչ այժմ Դուք թերևս լսել եք «ապատեղեկատվության» և «կեղծ լուրերի» մասին: Դուք կարող եք ավելի խելացի գտնվել ապատեղեկատվությունից, եթե Ձեզ համար սովորություն դարձնեք քննադատական հարցեր տալը ցանկացած տեղեկատվության մասին, որը սպառում եք, հատկապես եթե այն զարմացնող է, տարօրինակ կամ չափազանց լավը՝ ճիշտ լինելու համար:

Եվ վերջում, Դուք կցանկանաք ստուգել՝ որ լուրն է ճիշտ, որը կեղծ. հատկապես եթե Դուք ցանկանում եք այն տարածել Ձեր ընկերների կամ ընտանիքի անդամների շրջանում:

**Ի՞նչ կայք է հրապարակել:
Ո՞վ է գրել այն (և ե՞րբ):
Ինչի՞ մասին է ամբողջ հոդվածը՝ վերնագրից բացի: Ի՞նչ աղբյուրներ են վկայակոչվում:**

Եթե Դուք կարծում եք, որ դա ապատեղեկատվություն է և ցանկանում եք դադարեցնել դրա տարածումը, կան բազմաթիվ հարթակներ, որտեղ կարող եք բողոքել այդ հրապարակումից: Հետո արդեն կարող եք որոշել՝ շարունակում եք արդյոք հետևել այն օգտահաշվին, որը հրապարակել է դա:

5.

ՓՆՏՐԵՔ ՃՇՄԱՐՏՈՒԹՅՈՒՆԸ ՀԱՄԱՑԱՆՑՈՒՄ

«Կեղծ լուր» (ֆեյք նյուզ) եզրն օգտագործվում է բնութագրելու ոչ ճշգրիտ կամ մոլորեցնող տեղեկատվությունը, այդ թվում սատիրան, ոչ լիարժեք հետազոտված կամ ստուգված կոնտենտը, սուտը, խաբեությունը: Կեղծ լուրը, միշտ չէ, որ տարածվում է չարամտորեն, բայց անկախ նրանից, թե ինչ պատճառով է այն տարածվում, արդյունքը հիմնականում նույնն է. մարդիկ այն ստանալով՝ հավատում են, որ այն ինչ սխալ է, իրականում ճիշտ է, կամ որ պատահել է մի բան, որն իրականում չի եղել:

Լավագույն դեպքում դա կարող է լինել հումորային մեմ: Վատագույն դեպքում՝ առողջությանը վերաբերող ոչ ճշգրիտ տեղեկատվություն կամ քաղաքական բնույթի կեղծ ինֆորմացիա:

Անգամ ինքնուրույն հետազոտելու և քննդատական հարցեր տալու դեպքում էլ հնարավոր է, որ խճճվեք: Բայց իմացեք, այդ հարցում Դուք միայնակ չեք:

Ամեն ինչ պատրաստ
Քանի որ կայքերը չեն ընդունում իրենց սխալները, դա չի նշանակում, որ նրանք սխալներ չեն անում: Փաստացի, ամենավստահելի հրապարակումները նրանք են, որոնք չափազանց զգույշ են փաստերում, և ունենում են մարդիկ, կամ մի ամբողջ բաժին, որոնց գործը միայն փաստեր ստուգելն է:

Փնտրե՛ք այնպիսի աղբյուրներ, որոնք ուղղումներ են կատարում, երբ սխալվում են: Ավելի լավ է, երբ ուղղումը դրվի տեքստի ամենավերևում և տարածվի սոցմեդիայով, որպեսզի կարիք չլինի երկար փնտրել:

6.

ԴՈՒ՛ՐՍ ԵԿԵՔ ՏԵՂԵԿԱՏՎԱԿԱՆ ՊՂՊՋԱԿԻՑ

Երբ կայքերն ու հավելվածները ստեղծում են պրոֆիլ, որով Դուք հետաքրքրված եք, Դուք կարող եք հայտնվել ֆիլտրված պղպջակում: Սա այն դեպքն է, երբ ծառայությունները Ձեզ ցույց են տալիս ավելի շատ հրապարակումներ՝ նման նրանց, որոնց վրա արդեն սեղմել եք: Ինչպե՞ս է դա սահմանափակում կամ փոխում այն, ինչի մասին լսում եք:

Հայտնվելով ֆիլտրված պղպջակում՝ մարդիկ կարող են տեսնել միանգամայն այլ պատմություններ, այլ վերնագրեր, հոդվածներ, գովազդներ, ինչպես որ ցույց է տրված Կապույտ լրահոս, Կարմիր լրահոս (Blu Feed, Red Feed) ինտերակտիվ հոդվածում (graphics.wsj.com/blue-feed-red-feed):

Եթե Դուք տեսնում եք ալգորիթմներով «լավ խնամված» կոնտենտ, որի դիզայնը, թվում է, հատուկ Ձեզ համար է, հարց բարձրացրեք՝ ինչպես կարողք եք դուրս գալ ֆիլտրված պղպջակից:

Փոխեք ուղղությունը և ստեղծեք Ձեր լրահոսը
Ֆիլտրված պղպջակից դուրս գալու լավ միջոց է բաժանորդագրվել այնպիսի ծառայությունների, որոնք հավաքում են լուրեր տարբեր աղբյուրներից, ցույց են տալիս տարբեր տեսակետներ: RSS-ալիքները, տարբեր ֆորումները, որտեղ ներկայացված է մտքերի լայն սպեկտր, կօգնեն Ձեզ տեսնել՝ ինչ է կատարվում պղպջակից դուրս: Կարելի է սկսել Global Voices-ից (globalvoices.org) և Syllabus-ից (the-syllabus.com):

Հավելվածները, կայքերը և առցանց մեդիան կարող են հիմնական գործիքը լինել տեղեկություն ստանալու, զվարճանքի և լայֆհեքերի համար: Բայց այդ ամբողջ կոնտենտում կարող է բարդ լինել չտրվել շեղող գործոններին և գտնել այն, ինչ իսկապես փնտրում եք: Ավելին, կարող է դժվար լինել հասկանալ ճշմարտության և հորինվածի տարբերությունը, երբ առցանց հանդիպում եք տեսանյութի, նկարի կամ հոդվածի:

Անձնավորված ալգորիթմները, որոնք փորձում են Ձեզ պրոֆիլավորել, ցնցող վերնագրերը, խմբագրված լուսանկարներն ու տեսանյութերը կարող են Ձեզ համոզել միանգամայն այլ իրականություն: Այն, ինչ Դուք տեսնում եք առցանց, միշտ չէ, որ արտացոլում է իրականությունը:
Data Detox-ի այս հատվածում մենք կպատմենք ապատեղեկատվության ամենահայտնի թեմաների և վիրուսային բառերի մասին: Սկսենք Ձեր պատասխանատվության վերլուծությունից, որից հետո կուսումնասիրենք առավել լայն պատկեր և խորհուրդներ կտանք, թե ինչպես կողմնորոշվել վիրտուալ ապատեղեկատվության աշխարհում:

Սկսեցինք:

6 ԽՈՐՀՈՒՐԴ՝ ԶԵՐԾ ՄՆԱԼՈՒ ԱՊԱՏԵՂԵԿԱՏՎՈՒԹՅՈՒՆԻՑ ԱՌՑԱՆՑ ՏԻՐՈՒՅԹՈՒՄ

DATA DETOX KIT

datadetoxkit.org #datadetox

արտադրանք՝ TACTICAL TECH

Աջակցում է՝ Save the Children 100 ANNI IFLA

Ֆինանսավորվում է Եվրամիության կողմից.

1.

ԳԻՏԱԿՑԵ՛Ք ՁԵՐ ՈՒԺԸ

Հավանելը, տարածելը, ռեթվիթը և վերահրապարակումը գործողություններ են, որոնք նկարագրում են, թե որքանով եք Դուք կապված այն ամենի հետ, ինչ տեսնում եք օնլայն, և Ձեր այդ փոխազդեցությունները կարող են մեծ նշանակություն ունենալ: Եթե բավարար թվով մարդիկ են արձագանքում լուսանկարին, տեսանյութին կամ հրապարակմանը, այն արագ տարածվում է և դառնում «վիրուսային»:

Մի պահ ինքներդ Ձեզ հարց տվեք. «Ո՞րն է իմ ազդեցությունն օնլայն տիրույթում»: Վերջին անգամ ե՞րբ է եղել, երբ տեսել եք շոկային կամ զվարճալի հոդված, վերնագիր, տեսանյութ կամ լուսանկար և վայրկյանների ընթացքում արդեն այն ուղարկել եք Ձեր ընկերներին: Հետազոտողները կարծում են, որ վիրուսային դարձող հոդվածները կամ նկարները նրանք են, որոնք Ձեր մեջ առաջացնում են վախ, զզվանք, տագնապ, զայրույթ և բարկություն: Եթե Դուք հենց այսօր առավոտյան նման բան եք արել, պետք չէ վատ զգալ դրանից:

Տարածելը խրախուսվում է

Տարածելը մասնակցության ձև է: Երբ տարածում եք ինչ-որ բան (ցանկացած բան), Դուք մեծացնում եք դրա՝ վիրուսային դառնալու հավանականությունը: Եթե պարզվում է, որ այն ֆեյք է, կուզե՞ք, որ Ձեր անունը կամ հեղինակությունը կապվեր դրա հետ: Նախքան հղումը տարածելը, մտածեք՝ գուցե տարածում եք կեղծ բան, վնասակար կամ թունավոր:

2.

ՄԵ՛Կ ԱՆԳԱՄ ԷԼ ՄՏԱԾԵՔ՝ ՆԱԽՔԱՆ ԱՅԴ ԹԵՍՏՆ ԱՆՑՆԵԼԸ

Վերջին անգամ ե՞րբ է եղել, երբ տեսել եք թեստ (տեքստային կամ լուսանկարի տեսքով) նմանատիպ վերնագրով.

Ո՞ր տասնամյակն եք Դուք
Ո՞րն է Ձեր հոգու կենդանին
Ո՞րն է Ձեզ համար կատարյալ արձակուրդը
... ցանկը շարունակվում է

Չնայած կա հավանականություն, որ այս հարցաշարի նպատակն իսկապես Ձեզ զվարճացնելն է, հնարավոր է նաև, որ հարցերը զգուշորեն այնպես են կառուցված, որ տեղեկատվություն հավաքեն Ձեր մասին և դասակարգեն Ձեր ինքնությունը՝ հիմնված այսպես կոչված հոգեմետրիկ երանգների վրա:

Օրինակ, «Սիմփսոնների ո՞ր կերպարն եք Դուք» թեսթի պատասխանը՝ Ձեր բրաուզերում կամ հավելվածներում երևացող մի շարք այլ սովորույթների հետ կարող են տվյալների վերլուծաբաններին պատկերացում տալ՝ ինչ տեսակի մարդ եք Դուք, ինչն է Ձեզ համար կարևոր, և ինչպես ազդել Ձեզ վրա, որպեսզի, օրինակ գնեք կոշիկ... կամ անգամ կարող են կազմել Ձեր պրոֆիլը, որպեսզի որոշեն՝ ինչպես կարելի ներազդել Ձեզ վրա՝ հաջորդ ընտրություններում այս կամ այն կերպ քվեարկելու համար:

Ավելի շատ գաղտնիքներ

Երբ ասում են անձնական տվյալներ, առաջինը մտաբերում եք գաղտնաբառերը, նույնականացման քարտը, բանկի հաշվեհամարը: Բայց Ձեր մասին մանրամասները, օրինակ, ինչն է Ձեզ վախեցնում, զայրացնում, կամ ինչ ձգտումներ ունեք, խիստ անձնական են: Այս տվյալները կարող են արժեքավոր լինել տվյալների վերլուծաբանների համար՝ լույս սփռելով այն բանի վրա, թե ինչպես կարելի է Ձեզ ցանցը գցել: Մեկ անգամ էլ մտածեք՝ նախքան կփորձեք հարցման կամ թեստի միջոցով «բաց թողնել» այդ բնույթի տեղեկատվությունը:

3.

ԿՈՒԼ ՄԻ՛ ՏՎԵՔ ԽԱՅԾԸ

Քլիքբեյթ եզրն օգտագործվում է սենսացիոն, անազնիվ և հորինված վերնագրերը նկարագրելու համար, որոնք նպատակ ունեն ստիպել մարդուն սեղմել վերնագիրը կամ հղումը: Որքան շատ ուշադրության է արժանանում հոդվածը, տեսանյութը կամ լուսանկարը, այնքան շատ գումար այն կարող է հավաքել: Դա նշանակում է, որ այն ստեղծողները շահագրգռված են ասել ցանկացած բան, որը կստիպի Ձեզ սեղմել հղումը կամ տարածել այդ կոնտենտը:

Ձեր կողմից օգտագործվող հարթակները (օրինակ Facebook-ը կամ Instagram-ը) Ձեր շուրջ կառուցված ինքնության պրոֆիլի հիման վրա կարող են Ձեզ առաջարկել պատվիրված վերնագրեր, որոնց նպատակն է շարժել Ձեր էմոցիաները՝ ստիպելով Ձեզ սեղմել:

Քլիքբեյթ վերնագրերի տակ կարող եք գտնել ապատեղեկատվություն, բայց միշտ չէ, որ դա այդպես է: Հենց սկսեք տարբերել քլիքբեյթ վերնագրերը, դրանք կսկսեք նկատել YouTube-ում, բլոգերում և տապլոիդներում:

Հասե՛ք սկզբնաղբյուրին

Երբ հանդիպում եք քլիքբեյթի, վերնագրով մի՛ բավարարվեք: Եթե հղումն անվտանգ է երևում, բացե՛ք հոդվածը և փորձե՛ք գտնել՝ ով է նյութի հեղինակը, երբ է այն հրապարակվել, և ինչ աղբյուրների է վկայակոչում: Դա կարող եք գտնել հոդվածում, կարող է լինել ծանուցում, որ դա վճարովի կոնտենտ է կամ գովազդ, կամ գուցե այն տեղադրված է Կարծիքներ բաժնում: Այս մանրամասները կարող են Ձեզ օգնել հասկանալ՝ արդյոք այն արժե Ձեր ծախսած էներգիան:

4.

ԶԳՈՒՇԱՑԵՔ ԿԵՂԾԻՔԻՑ

Դիփ ֆեյքերը այն տեսանյութերն են, ձայնագրությունները կամ լուսանկարները, որոնք թվային փոփոխության են ենթարկվել, հիմնականում՝ ինչ-որ մեկի դեմքը կամ շարժումները մյուսի վրա դնելու, նրանց խոսքը փոխելու միջոցով: Չնայած «դիփ ֆեյքը» նոր եզր է, այդ տեխնիկան երկար ժամանակ է, ինչ այս կամ այն կերպ օգտագործվում է:

Շատ ավելի հեշտ է ստեղծել այսպես կոչված չիփ ֆեյք (էջան ֆեյք)՝ մոլորեցնող կոնտենտ, որը չի պահանջում նուրբ տեխնոլոգիա, այլ պարզապես կարող է կառուցվել տեսանյութի կամ լուսանկարի վրա սխալ վերնագիր դնելով, կամ օգտագործելով հին կոնտենտ՝ ներկայի դեպքերը նկարագրելու համար:

Ֆեյքերի դեմ պայքարելը երբեմն անիրական է թվում, բայց կա մի բան, որ կարող եք անել... ուշադիր եղեք:

Ուշադիր եղեք, փորփրեք

Ինչպես քլիքբեյթերի դեպքում, այս դեպքում էլ այդքան հեշտությամբ մի հավատացեք: Եթե լուսանկարը, տեսանյութը Ձեզ անիրատեսական են թվում կամ չափազանց շոկային են, Ձեզ հարց տվեք՝ ինչ կարող է լինել այդ տեղեկատվության հետևում: Հակառակ դեպքում, եթե նկատում եք, որ միևնույն լուսանկարը ողողել է Ձեր լրահոսը, և այն Ձեզ ուղարկում են ընկերները, գուցե փորձեք սկզբնաղբյու՞րը գտնել:
Դա հենց այդ դեպքն է, երբ պետք է հարցեր ինչեցնել. Ո՞վ է այն հրապարակել (Ի՞նչ կայք է, ո՞վ է հեղինակը): Ե՞րբ է հրապարակվել: Եթե դա լուսանկար է, TinEye (tineye.com) հավելվածի միջոցով ստուգեք՝ երբ է առաջին անգամ հրապարակվել:
Ստուգեք լուրերի այլ աղբյուրներ, նախքան դրան հավատալը և ընկերների ու մերձավորների շրջանում այն տարածելը: