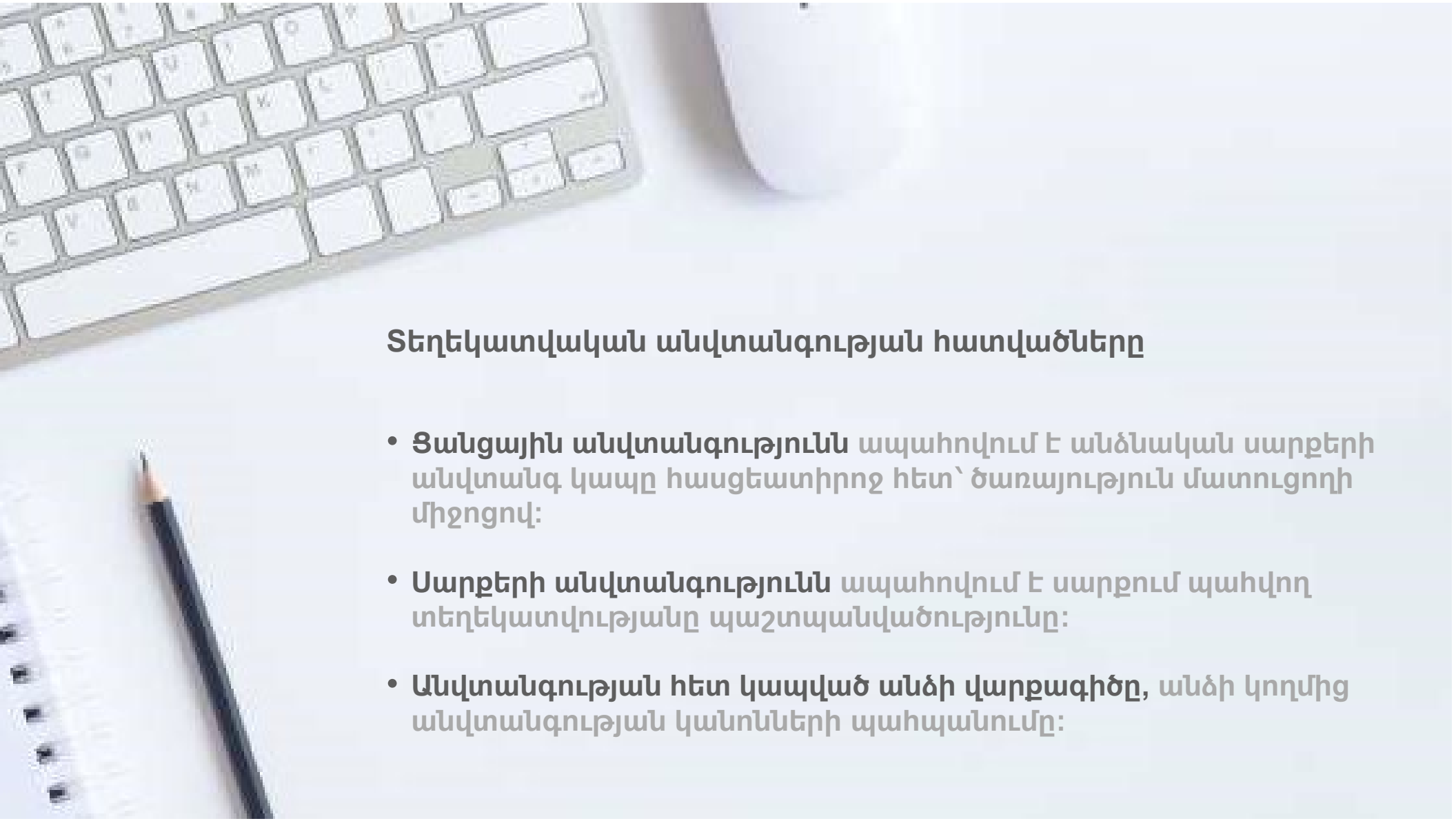
ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ

Դավիթ Սանդուխյան
Twitter: @david_sand

Տեղեկատվական անվտանգություն հասկացությունը սովորաբար ներառում է տեխնիկական, ֆիզիկական և կազմակերպչական միջոցների համալիրը, որը կոչված է ապահովել տեղեկատվության խորհրդապահությունը, ամբողջականությունը և հասանելիությունը:



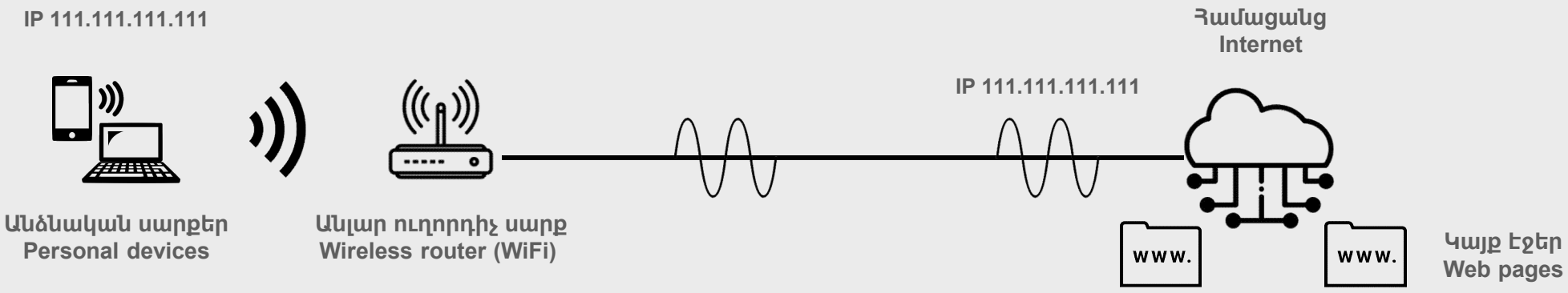
Տեղեկատվական անվտանգության հատվածները

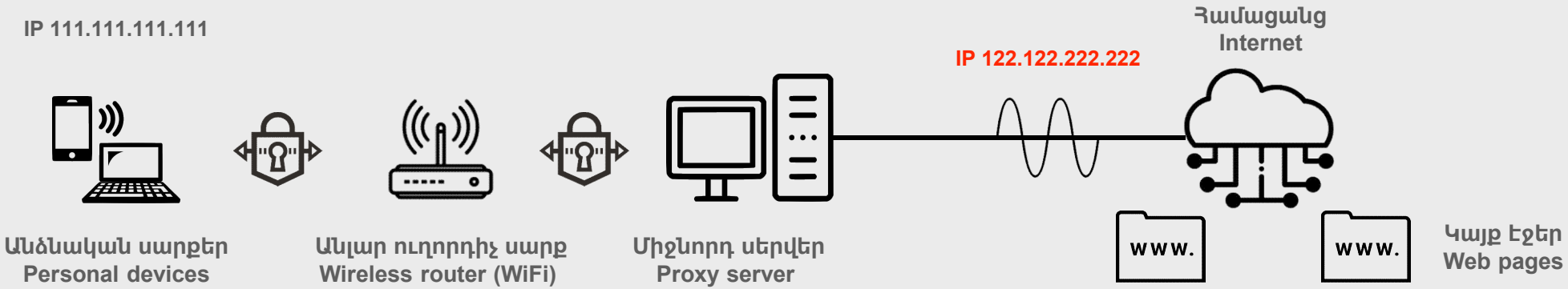
- **Ցանցային անվտանգությունն** ապահովում է անձնական սարքերի անվտանգ կապը հասցեատիրոջ հետ՝ ծառայություն մատուցողի միջոցով:
- **Սարքերի անվտանգությունն** ապահովում է սարքում պահվող տեղեկատվությանը պաշտպանվածությունը:
- **Անվտանգության հետ կապված անձի վարքագիծը,** անձի կողմից անվտանգության կանոնների պահպանումը:

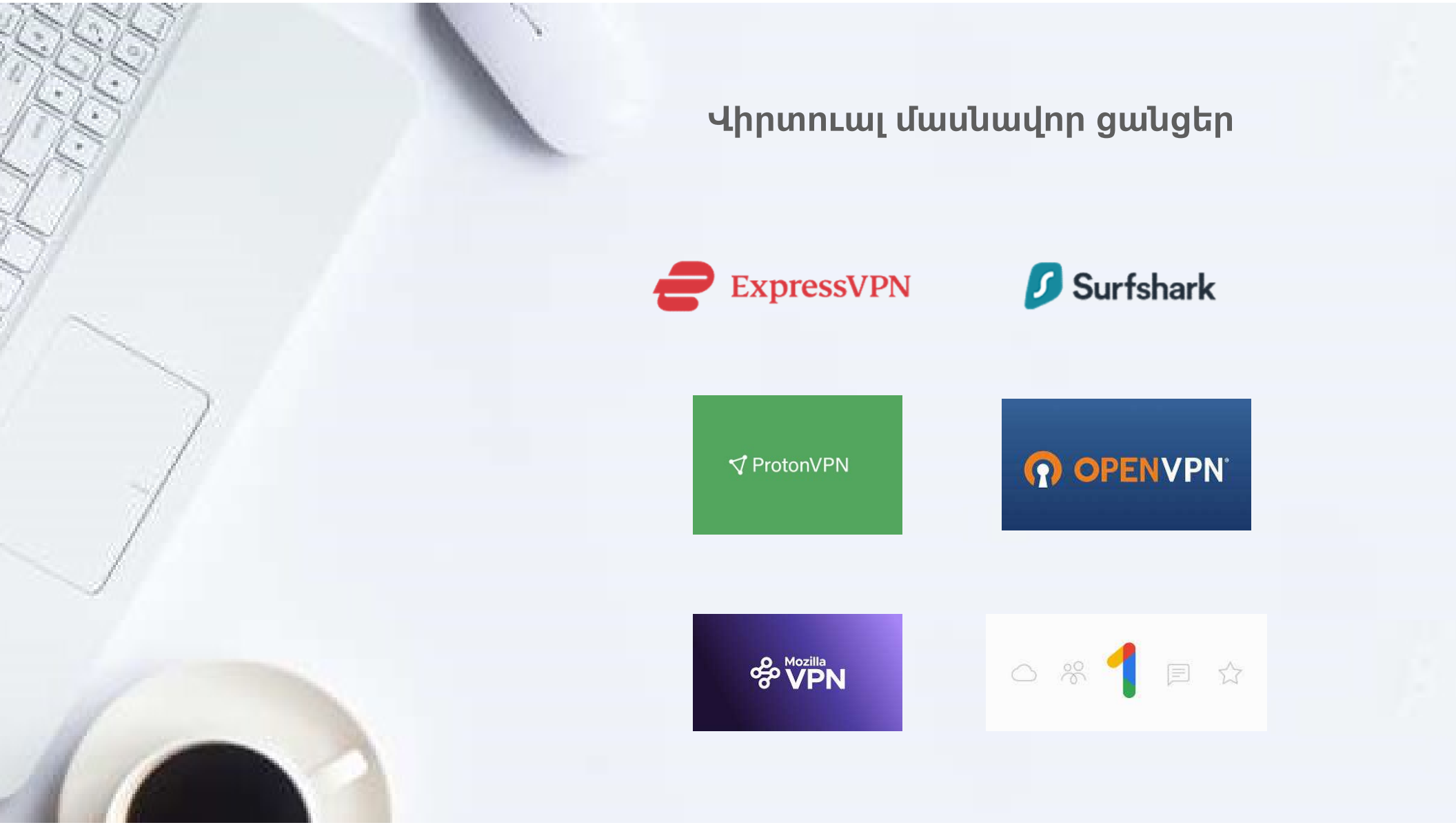
Ցանցային անվտանգություն

- Ըստ անվտանգության մակարդակի՝ առավել անվտանգ են լարային ցանցերը:
- Քիչ ավելի անվտանգ են համարվում շարժական (բջջային) կապի ցանցերը:
- Առավել թույլ պաշտպանված ցանցերից են Wi-Fi և Bluetooth տեսակի ցանցերը:

Մասնավոր վիրտուալ ցանց - Virtual Private Network





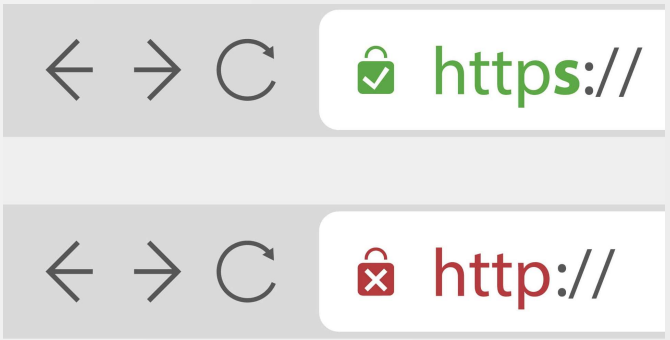

Վիրտուալ մասնավոր ցանցեր
ExpressVPN
Surfshark
ProtonVPN
OPENVPN
Mozilla VPN

Կայք էջերի անվտանգության սերտիֆիկատը և անվտանգ հաղորդակցությունը

Անվտանգ հաղորդակցության արձանագրությունը (Transport Leyer Security կամ Secure Socket Layer) ապահովում է օգտատիրոջ և կայքի միջև գաղտնագրված հաղորդակցությունը:

https կամ TLS/SSL արձանագրություններն առավել կարևոր են, երբ կայք էջին հաղորդվում են գաղտնի տվյալներ, օրինակ՝ անձնական տվյալներ, գաղտնաբառ կամ մուտք է կատարվում որևէ օգտահաշիվ (user account):

Վստահված սերտիֆիկատի (trusted certificate) առկայությունը հաստատում է, որ կայքը պատկանում է այն կազմակերպությանը, որը նշված է սերտիֆիկատում (հաստատում է սեփականատիրոջ ինքնությունը):



Գաղտնաբառեր և օգտահաշիվներ

- Գաղտնաբառերի ընտրությունը պետք է բացառի
  Բառեր (առավել ևս հաճախ օգտագործվող)
- Օգտատիրոջ անձնական տվյալները
  (անուն, ծննդյան թիվ, բնակության վայր)
- Միայն թվերի կամ միայն տառերի պարզ համադրություններ
  (օրինակ՝ aaddgg կամ 112233)
- Չպետք է կրկվեն տարբեր համակարգերում
  (օրինակ, սոց ցանցում և էլ փոստի օգտահաշվում)

Օգտահաշվի պաշտպանությունը

- Առավել անվտանգ է համարվում անվտանգության սարքի կամ ծրագրերի օգտագործմամբ նույնականացման եղանակը:
- Բարձր պաշտպանվածության աստիճան են համարվում նաև Կենսաչափական տվյալների մուտք գործելու եղանակները:
- Բազմակի (սովորաբար կրկնակի) նույնականացման եղանակները համարվում են միջին աստիճանի պաշտպանված:
- Կարճ հաղորդագրությունների միջոցով նույնականացումը համարվում է ոչ վստահելի:
- Միայն գաղտնաբառի օգտագործմամբ օգտահաշվի պաշտպանությունը համարվում է առավել չպաշտպանված, սակայն որոշ համակարգերի համար ընդունելի միջոց է:

Սարքերի անվտանգությունը - սմարթֆոններ

Կարևոր է սարքը կորցնելու կամ կողոպտելու դեպքում տեղեկությունները պաշտպանելու համար: Չի պաշտպանում հակեռական գրոհներից ու վնասաբեր ծրագրերից (վիրուսներ):

Մուտքի արգելափակում՝ գաղտնաբառի կամ կենսաչափական (մատնահետքեր, դեմքի «ճանաչում):

Սարքերի գաղտնագրում՝ ինչպես առանձին տվյալների, այնպես էլ ամբողջ սարքի պարունակության:

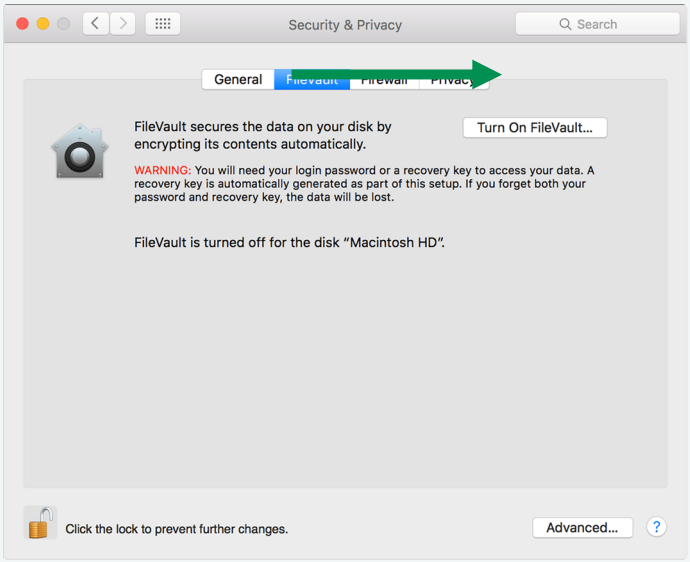
iPhone-ի բոլոր ժամանակակից համակարգերը (**iOS 8** և ավելի բարձր) ապահովում են գաղտնագրումը առանց լրացուցիչ կարգավորումների:

Android 5 և բարձր օպերացիոն համակարգերի հիման վրա աշխատող սարքերը պահանջում են լրացուցիչ կարգավորում հետևյալ բաժնում **Settings > Personal > Security > Encryption**

Սարքերի անվտանգությունը - համակարգիչներ

macOS համակարգում (MacBook)
FileVault գործիքն է կարգավորումներում

Settings > Security & Privacy > FileVault

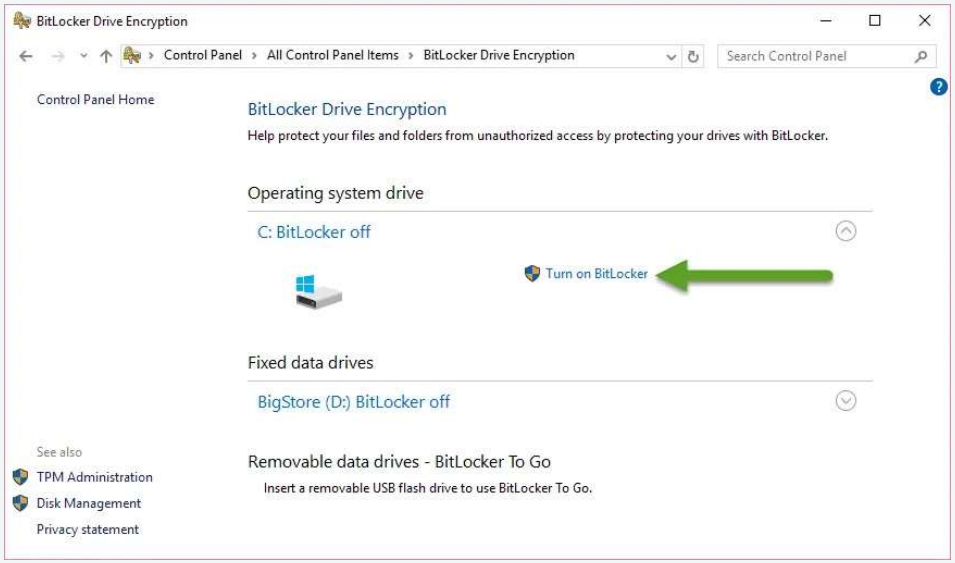


Windows 10 համակարգում գաղտնագրման գործիքը կոչվում է BitLocker և միանում է կարգավորումների համապատասխան բաժնում

Control Panel > All Control Panel Items > BitLocker Drive Encryption

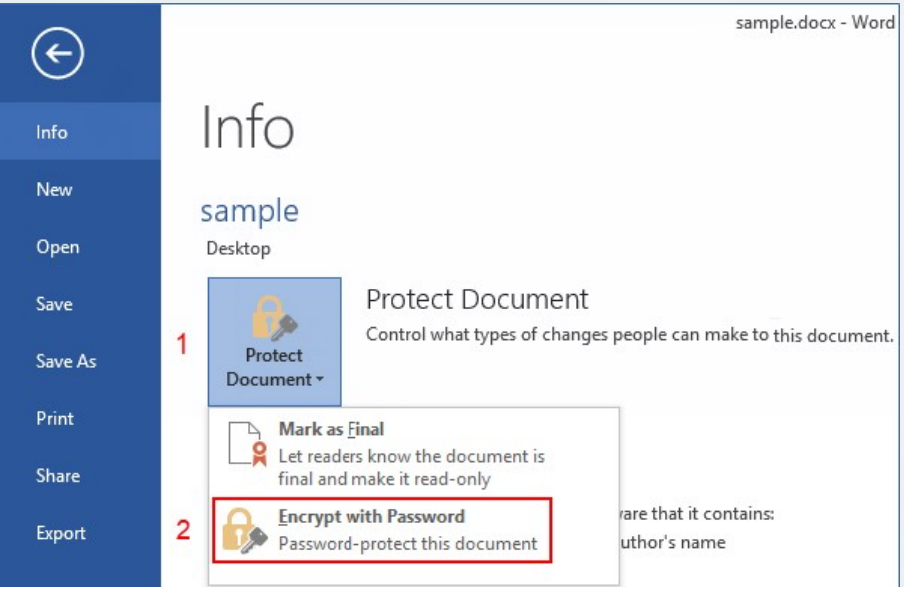
կամ (տարբեր թողարկումներ)

System and Security > BotLocker Drive Encryption

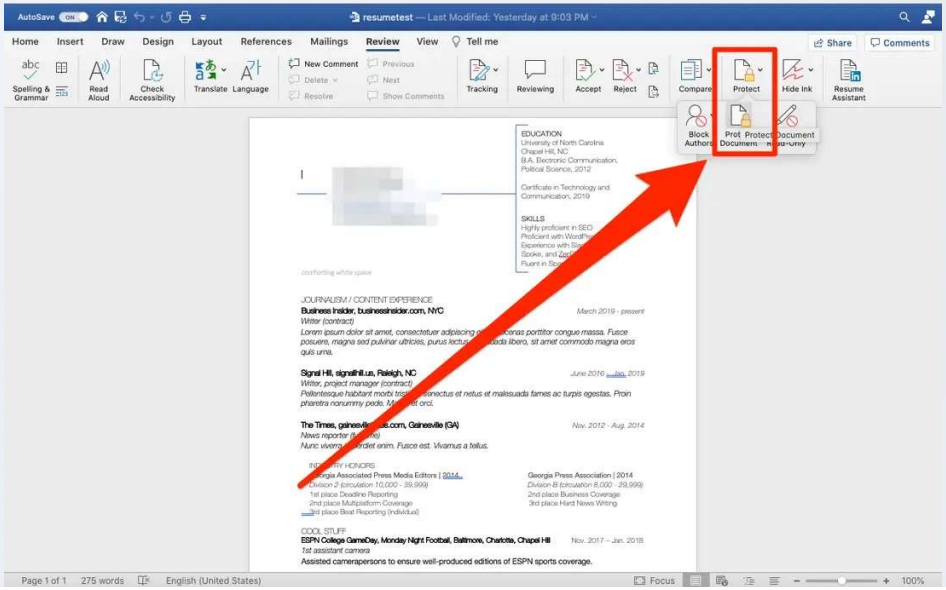


Փաստաթղթերի փաշտպանությունը

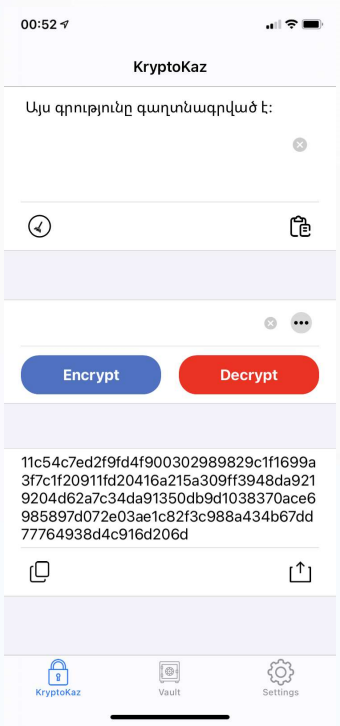
MS Word for Windows

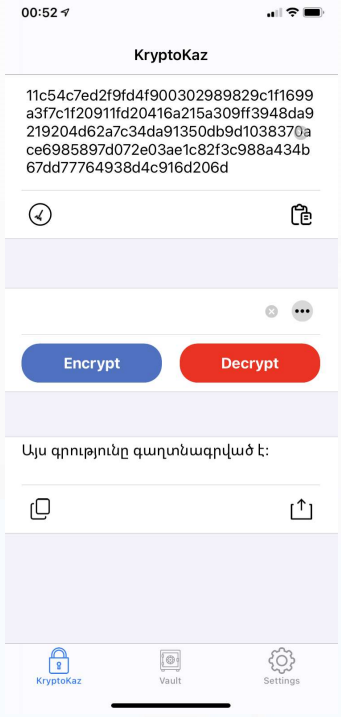


MS Word for MacOs



Փաստաթղթերի ու հաղորդագրությունների գաղտնագրում





Հաղորդակցվող կողմերը պետք է օգտվեն գաղտնագրման նույն ալգորիթմից ու նախօրոք որոշեն գաղտնաբառը:

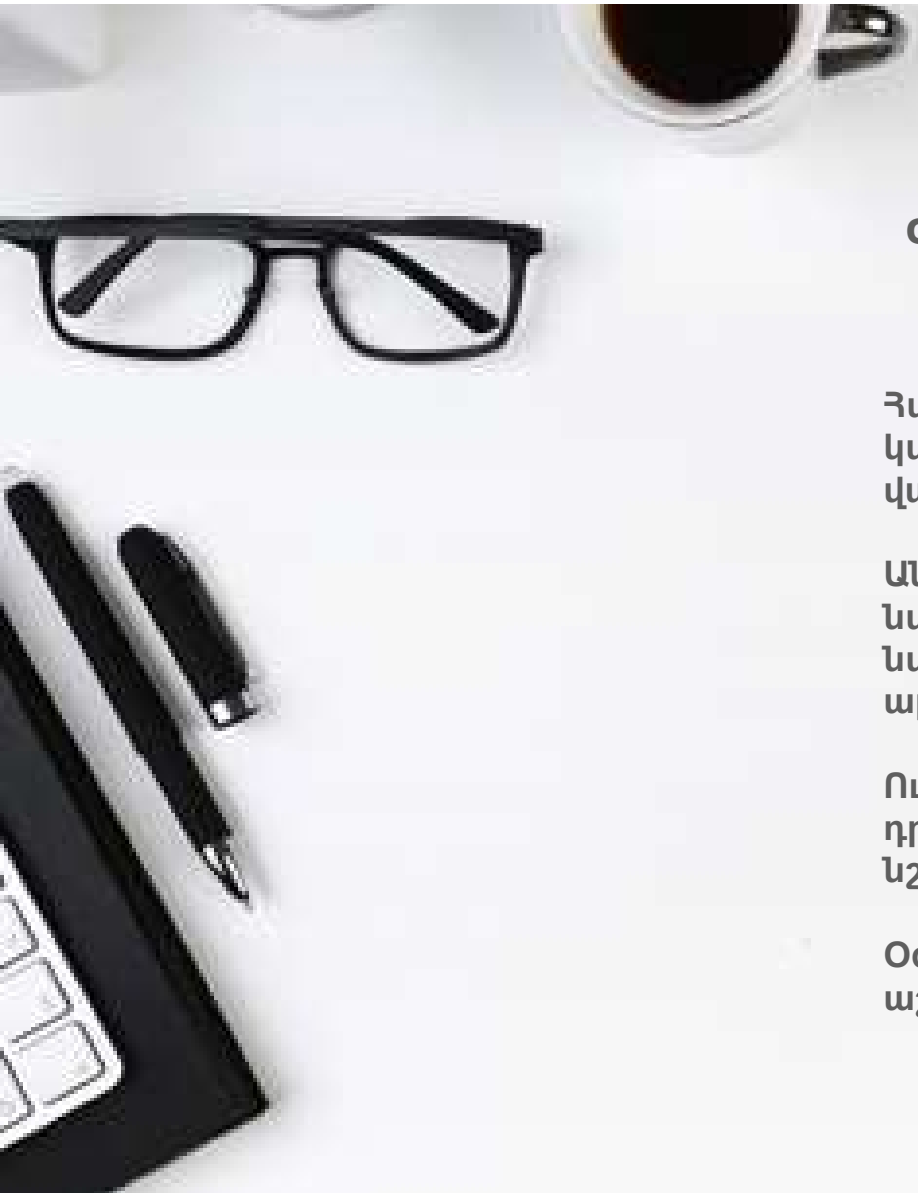
Առավել պաշտպանված գաղտնագրերն են՝ AES-256, SHA-512

Անձի վարքագիծը անվտանգության ոլորտում

Հակեռային գրոհների մեծ մասը կատարվում է այդպես կոչված սոցիալական ճարտարագիտության (social engineering) միջոցով:

Հակերները օգտագործում եմ անձանց անուշադրությունը, համակարգչային գրագիտության պակասը և պարզապես մարդկանց դասական թուլությունները:

Պետք է հիշել, որ նախքան գրոհ կազմակերպելը հակերը ուսումնասիրում է իր հնարավոր զոհի վարքը, սոցիալական կապերը, նախասիրությունները:



Գրոհի կազմակերպելու տարբերակները

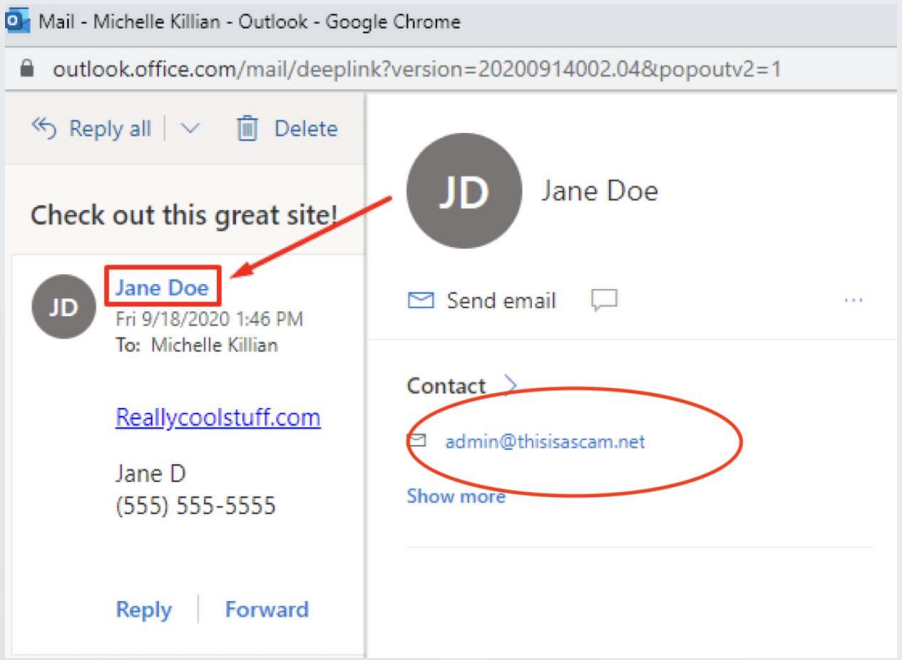
Հակերային գրոհի զոհը կարող է ստանալ էլ նամակ
կամ կարճ հաղորդագրություն, որտեղ կարող է լինել
վտանգավոր հղում (link) կամ կցված հաղորդում (attachment):

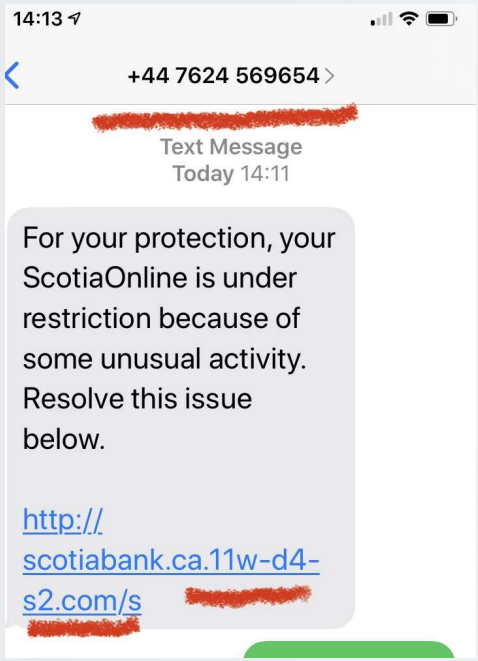
Անհրաժեշտ է խուսափել անծանոթ հասցեներից ստացված
նամակները բացելուց: Եթե կասկածելի բովանդակության
նամակ եք ստացել ծանոթ մարդուց, անհրաժեշտ է ստուգել՝
արդյո՞ք հասցեն նրանն է:

Ուշադրություն դարձնել կայքերի հասցեներին, ստուգել՝ արդյոք
դրանք համապատասխանում են կազմակերպության
նշած հասցեին:

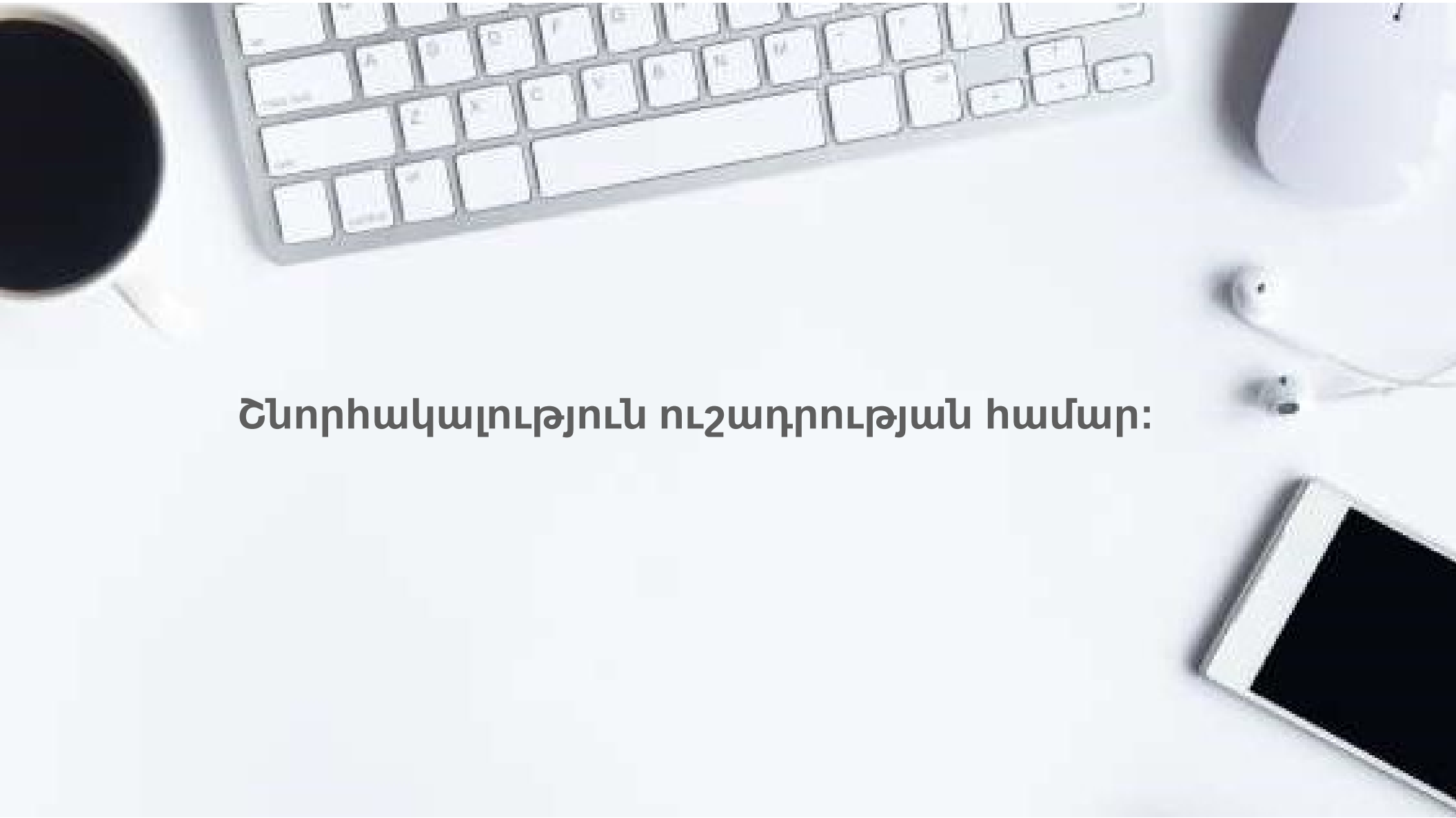
Օգտագործել մի քանի բրաուզեր սոցիալական ցանցերի,
աշխատանքային կայքերի ու վճարման համակարգեր այցելելու նպա

Շփոթություն առաջացնող մեթոդները





ՀԱՐՑԵ՞Ր



Շնորհակալություն ուշադրության համար: