# ***Էլեկտրոնային ապահովություն***

| Հարցեր | Հնչող պատասխաններ | Ակնկալվող պատասխաններ |
| --- | --- | --- |
| * Ի՞նչ էլեկտրոնային ծառայություններից եք օգտվու՞մ։ * Ո՞ր սոցիալական ցանցերում ունեք հաշիվներ։ |  | Էլ փոստ, Instagram, Facebook, Snapchat, TikTok․․․ , տարբեր զրուցարաններ․․․, խաղեր․․․ |
| * Ի՞նչ է գաղտնաբառ։ * Ի՞նչ կանոնների է պետք հետևել գաղտնաբառեր կազմելիս։   ՈՒՀ1  Ո՞ր դեպքում է ավելի հեշտ գուշակել դիմացինի էլեկտրոնային հաշիվների գաղտնաբառերը։  ՈՒՀ2  Արդյո՞ք ձեր անունը կամ ծննդյան տարեթիվը օգտագործել եք որպես գաղտնաբառ։ |  | Այլ անձանցից գաղտնի պահվող բառ կամ սիմվոլների հերթականություն, որն օգտագործվում է ինքնությունը կամ իրավասությունը հաստատելու համար։  Գաղտնաբառը պետք է կազմված լինի մեծատառերի և փոքրատառերի, ինչպես նաև թվերի և սիմվոլների համադրությունից։  Չպետք է պարունակի հեշտ գուշակվող տեղեկատվություն․ օրինակ՝ ծննդյան թիվը, հեռախոսահամարը, երեխաների, քույր եղբայրների անունները և այլն: |
| * Բոլո՞ր հաշիվների համար օգտագործում եք նույն գաղտնաբառը։ |  | Տարբեր հաշիվների գաղտնաբառերը երբեք չպետք է կրկնվեն։ Եթե մարդը բոլոր հաշիվների համար կիրառում է նույն գաղտնաբառը, ապա նման բացահայտումը վտանգում է նրա բոլոր գրանցումները։ |
| * Ինչ գիտեք երկփուլային վավերացման մասին։ |  | **Այսօր ամենախորացված պաշտպանության միջոցը երկփուլային մուտքի ընթացակարգն է (Two-factor authentication), որը ենթադրում է գաղտնաբառի մուտքագրումից բացի երկրորդ քայլով անընդհատ փոփոխվող կոդի մուտքագրում, որն օգտվողին տրամադրվում է կամ հատուկ բջջային հավելվածի, կամ սարքի, կամ կարճ հաղորդագրությունների միջոցով։** |



Հիմնական գաղափարներ՝

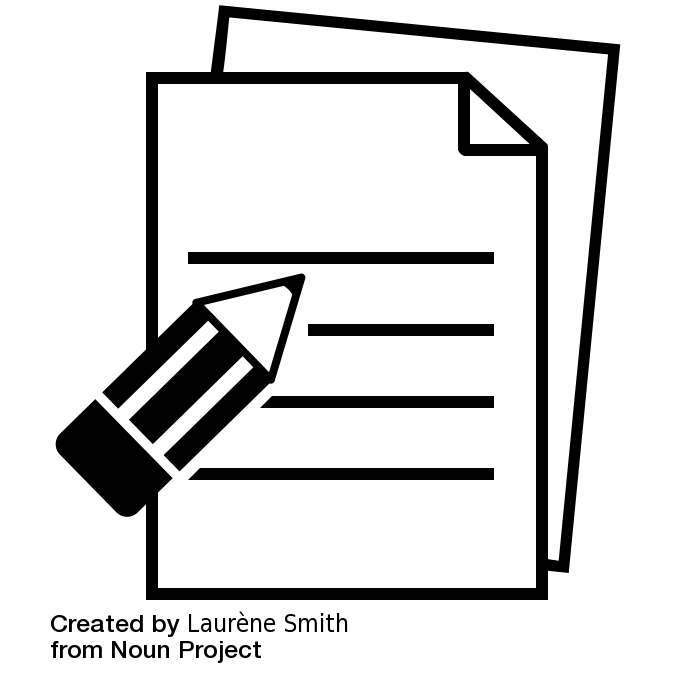
* Գաղտնաբառերը հաշիվների պաշտպանության հիմնական բանալին են։
* Օգտագործողի համար ամենահեշտ գաղտնաբառը, որը սովորաբար հեշտ է հիշվում, վնասողի համար ավելի դյուրին կռահելի կլինի։
* Գաղտնաբառերը մեր անձնական անվտանգության հարցում ամենակարևոր գործոններից են:
* Գաղտնաբառի վերաբերյալ գոյություն ունեն մի քանի հստակ սկզբունքներ, և եթե մենք դրանց պարբերաբար հետևենք, մեր հաշիվները քիչ թե շատ պաշտպանված կլինեն:
* Կարելի է օգտվել գաղտնաբառեր գեներացնող կայքերից, օրինակ՝ <https://passwordsgenerator.net/>

Բացված պատուհանում կարող ենք որոշել ծածկագրի կառուցվածքը՝

* Ծածկագրի երկարությունը(Password Length)
* Ներառել սիմվոլներ(Include Symbols)
* Ներառել թվեր(Include Numbers)
* Ներառել փոքրատառեր(Include Lowercase Characters)
* Ներառել մեծատառեր(Include Uppercase Characters)
* Բացառել նմանատիպ տառերը և թվերը շփոթություն չառաջացնելու համար(Exclude Similar Characters)
* Բացառել տարօրինակ նշանները(Exclude Ambiguous Characters)
* !Ստեղծել տվյալ սարքի վրա!(Generate On Your Device)
* Հիշել կարգավորումները հետագայում նորից օգտագործելու համար(Save My Preference)
* Ստեղծել ծածկագիրը(Generate Password)
* Երկփուլային մուտքի վավերացումը (Two-factor authentication) նշանակում է, որ եթե ուրիշն անգամ ունի ձեր գաղտնաբառը, նա չի կարող մտնել ձեր հաշիվը՝ առանց հատուկ կոդի, որն էլ անընդհատ փոխվում է։

Դիտում ենք երկփուլային վավերացման տեսանյութերից մեկը՝

[*https://youtu.be/988Db38NNew*](https://youtu.be/988Db38NNew) *Ինչպես ակտիվացնել Երկփուլային վավերացումը (Two-factor authentication)* ***Instagram****-ում*



Առաջադրանք 1 (4 րոպե )

Քայլ 1 ։ Բացել չատում տեղադրված [ֆայլը](https://docs.google.com/document/d/1HM_ZuDkyG0Cn7O7qnkcLyUJL0e697wSlhJkEDOQhaag/edit?usp=sharing).

Քայլ 2 ։ Պատասխանել հարցերին.



**Հ1 Ինչպիսի՞ գործողությունների դեպքում է հնարավոր**

**հայտնվել նման իրավիճակում։**

Հնչող պատասխաններ՝

Ակնկալվող պատասխաններ՝

Չնայած բարդ գրված գաղտնաբառի, առցանց տիրույթում որոշ անփույթ գործողությունների

պատճառով հնարավոր է կորցնել գաղտնաբառը՝

* Բացել ենք կասկածելի հղումները։
* Այլ համակարգիչներից կամ սարքերից օգտվելիս, պահպանել ենք գաղտնաբառերը։
* Պատասխանել ենք այն նամակներին և մուտք ենք գործել այնպիսի էջեր որոնք պահանջում են լրացնել իրական մուտքանունը և [գաղտնաբառը](https://hy.wikipedia.org/wiki/%D4%B3%D5%A1%D5%B2%D5%BF%D5%B6%D5%A1%D5%A2%D5%A1%D5%BC)։
* Խաղացել ենք առցանց թեստեր՝ անձնական հաշվով մուտք գործելով։



**Հ2 Ինչպե՞ս խուսափել նման իրավիճակում հայտնվելուց։**

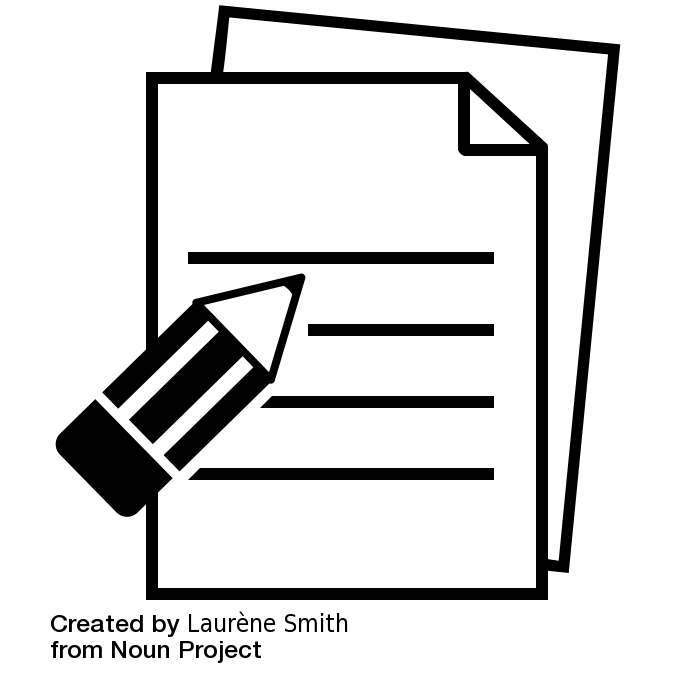
Հնչող պատասխաններ՝

Ակնկալվող պատասխաններ՝

* Չի կարելի անզգուշորեն բացել այն կասկածելի հղումները, որոնք նստացել ենք նույնիսկ մեր վստահելի ընկերներից, քանի որ հնարավոր է, որ ընկերոջ հաշիվն արդեն գտնվում է հաքերների վերահսկողության տակ, և տվյալ նամակն ինքը չի կազմել, այլ ուղարկվել է մեզ չարագործների կողմից։
* Չգայթակղվել առցանց թեստերից, դրանք վտանգավոր են և կարող են գողանալ մեր տվյալները։
* Բրաուզերում գաղտնաբառերը պատահաբար չպահպանելու համար մուտք գործել հատուկ ռեժիմով, որը չի պահպանում տվյալները պատուհանը փակելուց հետո։ Google Chrome-ի դեպքում դա միանում է որպես New Incognito Window (կամ ստեղնաշարով Ctrl+Shift+N)
* Պարտադիր ակտիվացնել երկփուլային վավերացումը։

Հիմնական գաղափար՝ 

* **Ֆիշինգը** կիբեռհանցագործության տեսակ է, որի նպատակն է ստանալ որևէ [սոցիալական կայքի](https://hy.wikipedia.org/wiki/%D5%8D%D5%B8%D6%81%D5%AB%D5%A1%D5%AC%D5%A1%D5%AF%D5%A1%D5%B6_%D5%AF%D5%A1%D5%B5%D6%84) օգտատիրոջ գաղտնի տվյալները, ծածկագիրը և ծածկանունը։ Ֆիշինգի զոհ դառնալուց խուսափելու համար հետևել վերոնշյալ գաղափարներին։
* Երբեք, ոչ մեկին չտրամադրել գաղտնաբառը, թեկուզ դա լինի ձեր բանկի լիազոր ներկայացուցիչը կամ կայքերի տեխնիկական սպասարկման թիմի անդամները․․․



Առաջադրանք 2 (4 ր)

Քայլ 1 ։ Բացել չատում տեղադրված [ֆայլը](https://docs.google.com/document/d/1JREULUvw6YpmhWBa_S3vxRY-XgeqKuXvotk-wLKRsKc/edit?usp=sharing).

Քայլ 2 ։ Պատասխանել հարցերին.



**Հ1 Ինչպիսի՞ գործողությունների դեպքում է հնարավոր հայտնվել նման իրավիճակում։**

Հնչող պատասխաններ՝

Ակնկալվող պատասխաններ՝ սոցիալական ցանցերում բոլոր նկարները և անձնական տվյալները դրված են հրապարակային ռեժիմով։ Գրանցվել ենք առցանց խաղերի, որտեղ օգտագործել ենք իրական նկարներ․․․



**Հ2 Ինչպե՞ս խուսափել նման իրավիճակում հայտնվելուց։**

Հնչող պատասխաններ՝

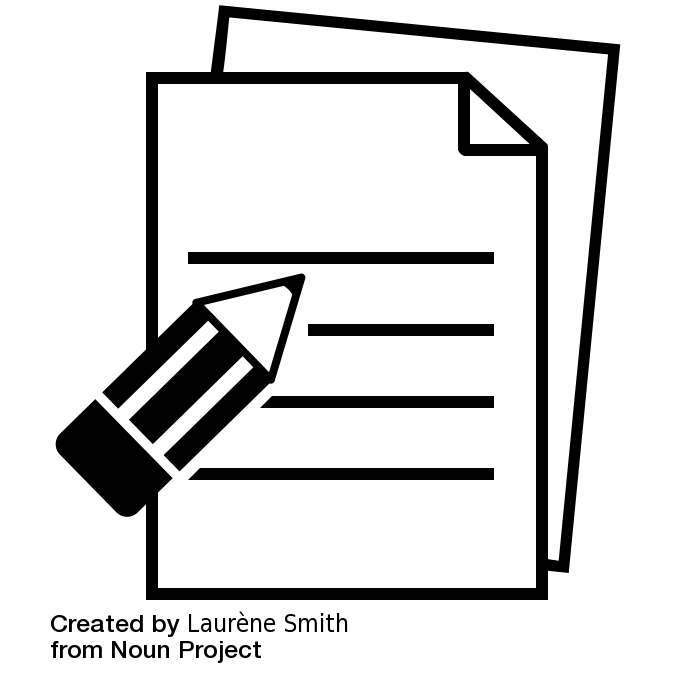
Ակնկալվող պատասխաններ՝ Զգույշ վերաբերվել անձնական տեղեկություններին: Լուսանկարները հրապարակելիս անպայման նշել «Միայն ընկերների համար» կարգավորումը։ Համակարգչային խաղեր խաղալիս ընտրել անվտանգ խաղանուն, օրինակ՝ SecretNinja99․․․, օգտագործել ավատար համացանցային տեսախցիկի փոխարեն: Տեսախցիկը շատ լավ բան է, բայց կարիք չկա, որպեսզի անծանոթներն իմանան, թե ինչ արտաքին ունենք:



Հիմնական գաղափար՝

* Սոցիալական ցանցում պետք չէ հրապարակել այնպիսի բաներ, որը չէիք ցանկանա հեռարձակվեր հանրության համար և արտացանցային աշխարհում:

* Խնդիրն այն է, որ համացանցում անձնական բնույթի տեղեկատվություն տեղադրելուն պես` մարդն այլևս ի վիճակի չէ վերահսկել, թե ով կտեսնի դա կամ ինչպես այն կօգտագործվի: Նկարները հեշտությամբ կարող են կրկնօրինակվել և սեղմակի մեկ հպումով տարածվել հազարավոր մարդկանց շրջանում: Ունենալով թվային բնույթ` նրանք կարող են  փոփոխվել կամ աղավաղվել: Նկարները կարող են նաև օգտագործվել որոնման նոր ծրագրերի կողմից` մարդկանց նույնականացնելու նպատակով (եթե անգամ նկարի կողքին չկա անունը):
* Առցանց համակարգում բոլորը չէ, որ ներկայանում են այնպիսին ինչպիսին իրականում կան:
* Համացանցային խաղերը զվարճալի են և ինտերակտիվ: Կարող եք խաղալ ընկերների և աշխարհի տարբեր ծայրերում գտնվող անձանց հետ: Սակայն համոզվեք, որ համացանցային խաղեր խաղալիս պաշտպանված եք դուք և ձեր անձնական բնույթի տեղեկությունները:



Առաջադրանք 3 (7 րոպե )

Քայլ 1 ։ Բացել չատում տեղադրված [<<Հաշիվներ>> խաղի հղումը](https://tsantsar.media.am/worlds/accounts-security)․

Քայլ 2 ։ Պատասխանել հարցերին և քննարկել պատասխանները։

Ժամանակի առկայության դեպքում ցուցադրվում է երկփուլային վավերացման տեսանյութը՝