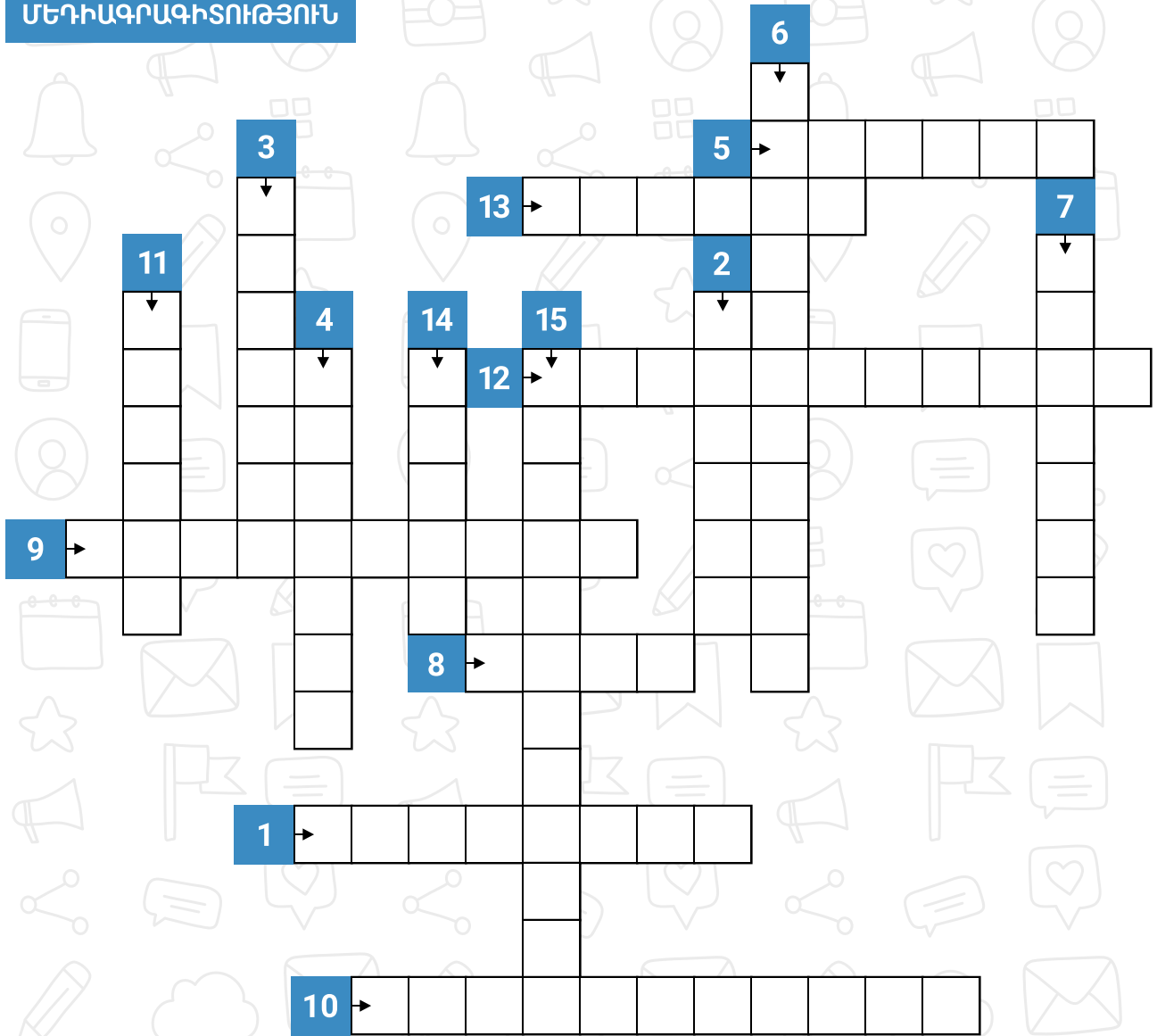


ՄԵԴԻԱԽԱՉԲԱՌ

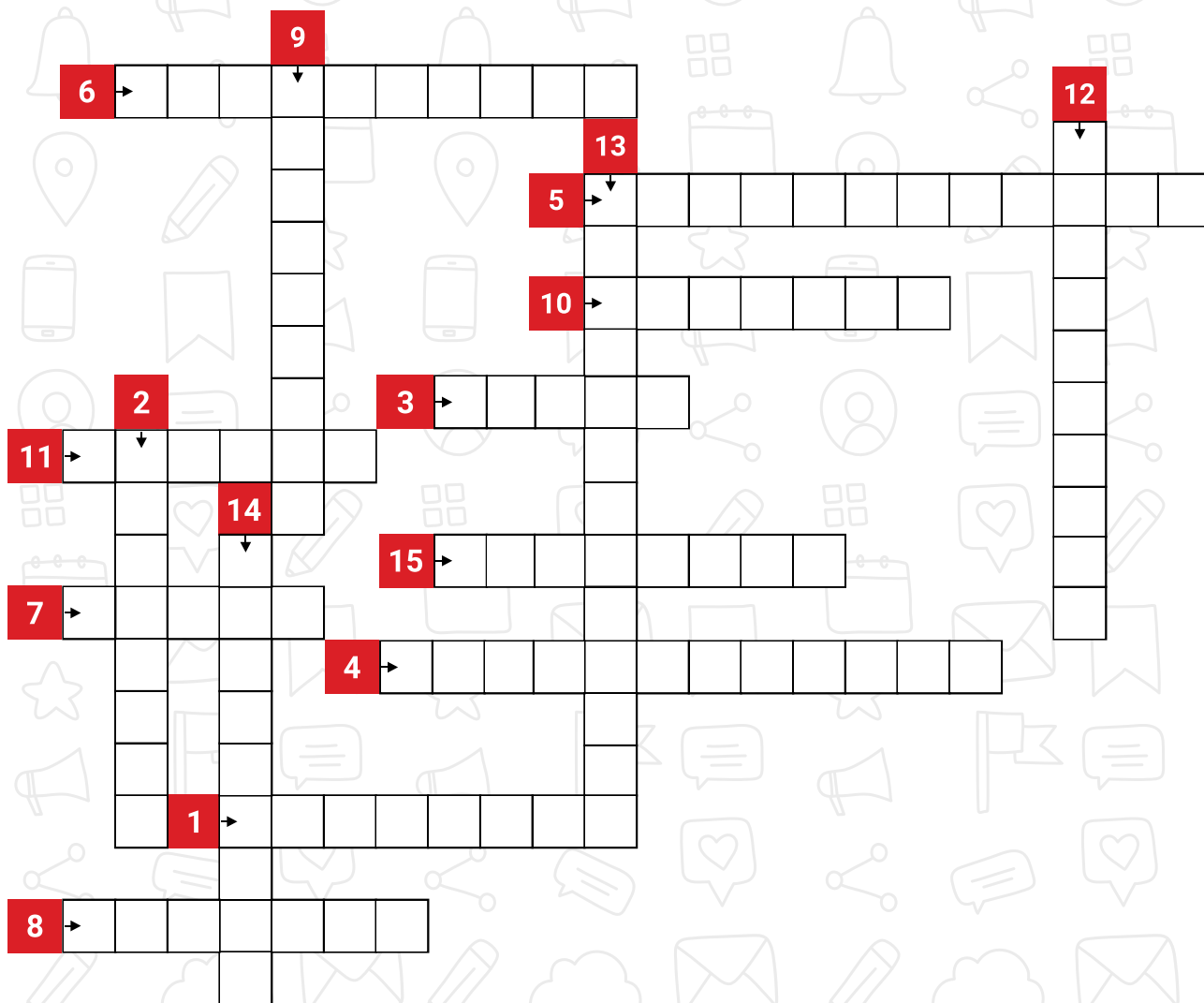
Եկե՛ք միասին լուծենք մեդիագրագիտության խաչբառը՝ ծանոթանալով մեդիաաշխարհի հասկացություններին, անձնական տվյալների պաշտպանության, թվային անվտանգության և գրագիտության կանոններին:



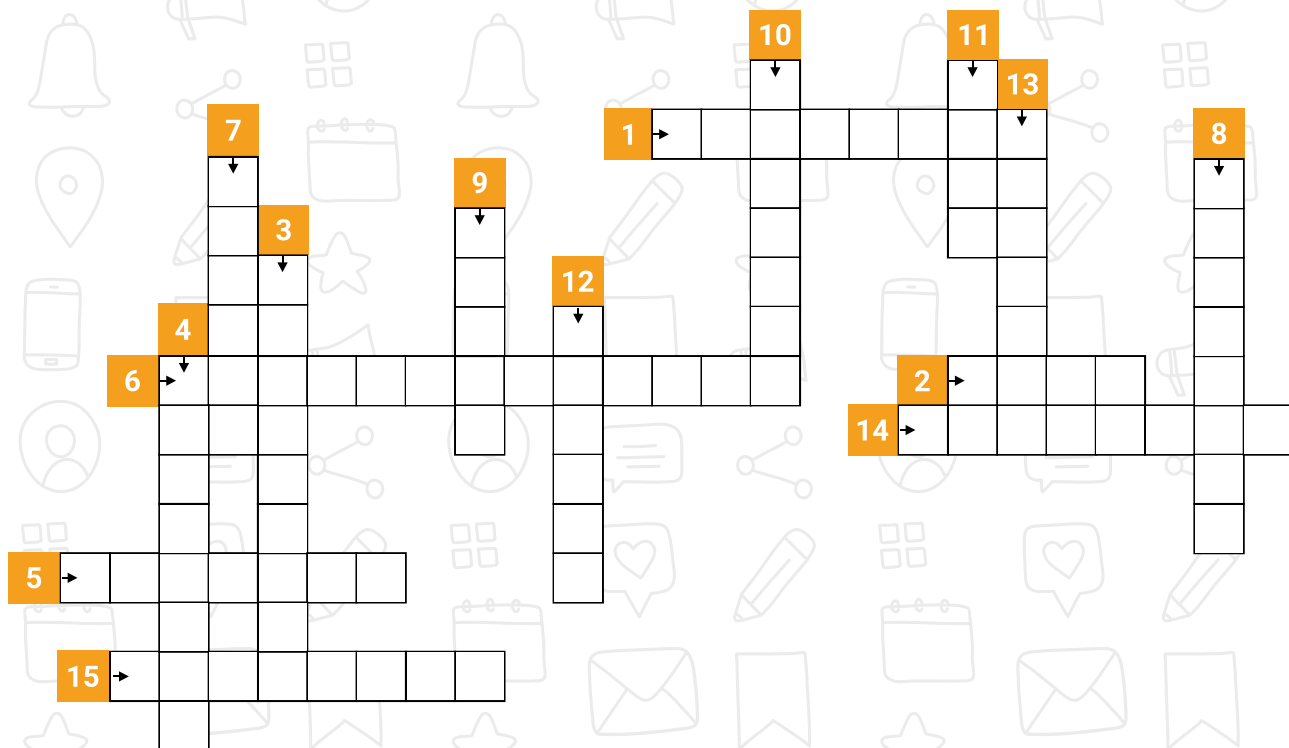
Մեդիախաչբառը մշակվել է «Մեդիագրագիտություն հասարակության խոցելի մեծահասակների համար 2.0» ծրագրի շրջանակում: Ծրագիրն իրականացվում է ԴԻ-ՎԻ-ՎԻ Ինթերնեյշնալի հայաստանյան գրասենյակի և Հանրային լրագրության ակումբի կողմից Գերմանիայի Դաշնային Հանրապետության արտաքին գործերի նախարարության աջակցությամբ:



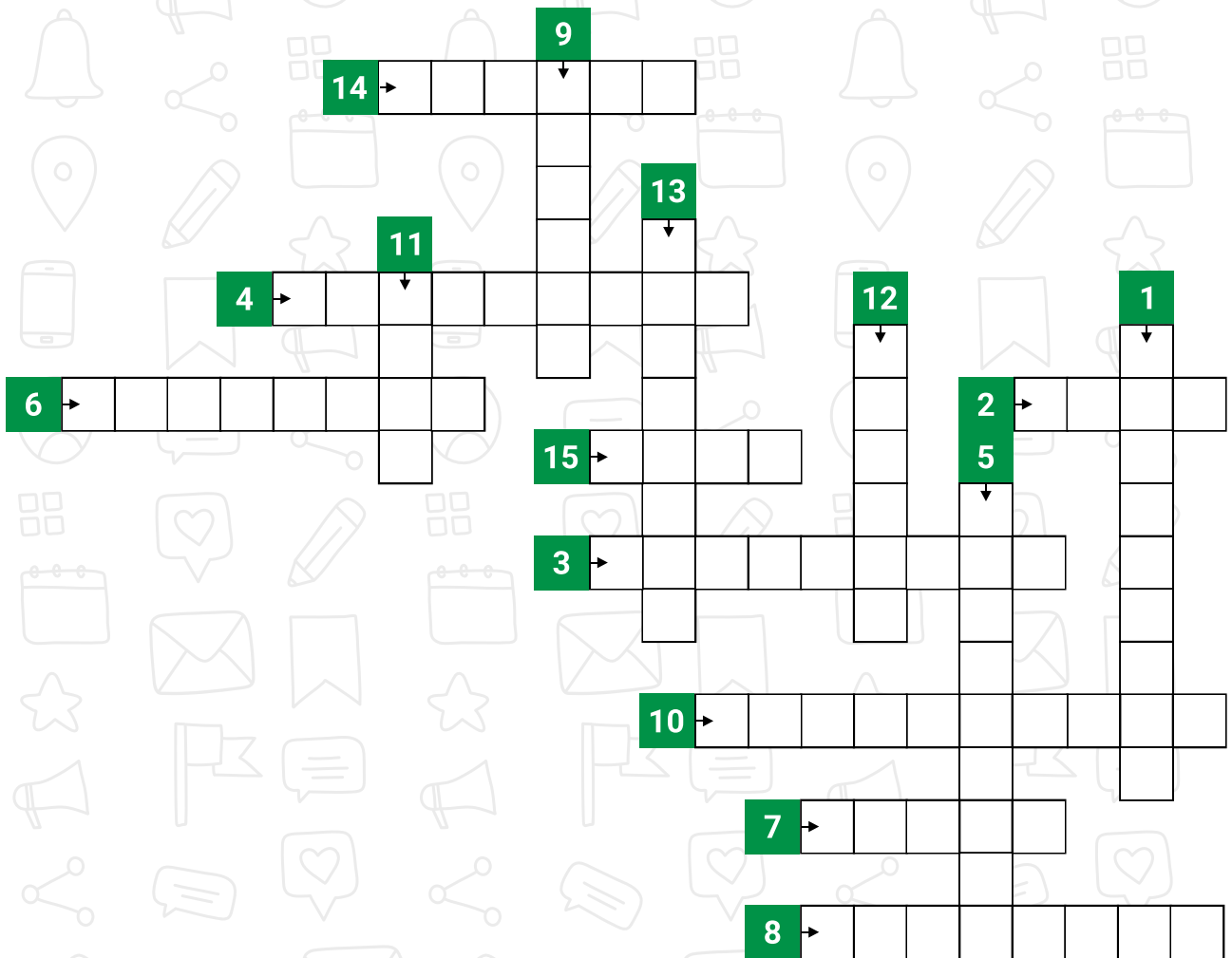
1. Նորության ո՞ր հատվածն են մարդիկ ավելի հաճախ կարդում:
2. Սոցիալական ո՞ր մեդիայի հավելվածն է ամենաշատը ներբեռնվել Հայաստանում 2022 թվականին:
3. Ինչպե՞ս է կոչվում այն բովանդակությունը, որը հաղորդվում է միայն ձայնի միջոցով, բայց ավանդական մեդիա չէ:
4. Սովորաբար ո՞ւմ ստորագրությունն է դրվում մեդիանյութի վերջում կամ սկզբում:
5. Նորություններն ընթերցելիս ի՞նչն է անհրաժեշտ տարանջատել փաստից, որպեսզի եզրահանգումը ճիշտ լինի:
6. Ինչի՞ն պետք է հղում անի լրատվամիջոցը մեջբերումներ անելիս:
7. Ինչպե՞ս է կոչվում այն գործընթացը, որի ընթացքում սաղորում և հետապնդում են օգտատիրոջը սոցիալական մեդիայում, վիրավորում և փորձում են հանել հունից:
8. Որոնողական ո՞ր համակարգն է ամենատարածվածը Հայաստանում:
9. Ինչպե՞ս է կոչվում այն մեդիանյութը, որը պարունակում է և՛ ձայն, և՛ պատկեր, և՛ տեքստ:
10. Ինչպե՞ս է կոչվում մարդուն ուղղված սուտ մեղադրանքը:
11. Ինչպե՞ս է կոչվում հայտարարությունը, հոդվածը, որը ժխտում է նախորդիվ ասվածը և/կամ հրապարակվածը:
12. Ինչպե՞ս են կոչվում այն մարդիկ, որոնք միայն կարդում, լսում և դիտում են նորությունները, բայց իրենք նորություն չեն հաղորդում:
13. Ինչպե՞ս է կոչվում նորությունների ժապավենում հայտնվող բովանդակությունը, որի էջին մենք չենք հետևում, բայց որը կարող է մեզ հետաքրքրել:
14. Թվային աշխարհում ինչպե՞ս է կոչվում որևէ կայքի հասցեն՝ հղումը:
15. Ինչպե՞ս է կոչվում մեդիաբովանդակության խեղաթյուրումը, որը լսարանին մոլորեցնելու միտում ունի:



1. Ինչպե՞ս է կոչվում անձը հաստատող հիմնական փաստաթուղթը:
2. Ինչպե՞ս է կոչվում գործընթացը, որի ժամանակ անձնական տվյալները ոչ նպատակային եղանակով հայտնվում են երրորդ կողմի մոտ:
3. Ընտանիքի այն անդամը, որին հարկավոր է հետևողական պաշտպանվածություն անձնական տվյալների հարցում:
4. Ո՞րն է անձնական այն տվյալը, որը ստեղծում ենք մենք, և որն արտացոլվում է անձնագրում:
5. Ինչպե՞ս է կոչվում այն տիրույթը, որտեղ պահպանվում է հեռախոսահամարների և զանգերի ցուցակը:
6. Ինչպե՞ս է կոչվում երևույթը, երբ առանց իրազեկելու և ծանուցելու հետևում են մարդու հեռախոսագրույցին:
7. Ինչպե՞ս են անվանում չարագործին, որը կարող է թվային միջավայրում ապօրինի եղանակով ձեռք բերել անձնական տվյալներ:
8. Ինչպե՞ս է կոչվում այն գործողությունը, որով տեղեկացնում են քաղաքացուն իր անձնական տվյալները հավաքելու և մշակելու մասին:
9. Ինչպե՞ս է կոչվում անձնական տվյալների հավաքումը և մշակումը հանրային վայրերում, որն իրականացվում է տեսախցիկի միջոցով:
10. Ինչպե՞ս է կոչվում ՀՀ կենտրոնական ընտրական հանձնաժողովի անձնական տվյալների շտեմարանը՝ ընտրելու իրավունք ունեցող քաղաքացիների վերաբերյալ:
11. Ինչի՞ միջոցով է հնարավոր ստանալ անձնական տվյալներ պետությունից, եթե դա հիմնավորված է և չի հակասում օրենքին:
12. Անձնական ո՞ր տվյալի միջոցով են հաճախ սմարթֆոնները նույնականացնում իրենց սեփականատերերին:
13. Անձնական ո՞ր տվյալի մուտքագրումն է պահանջում սոցիալական մեդիան՝ օգտահաշվի անվտանգությունն ապահովելու և վերականգնելու նպատակով:
14. Անձնական ի՞նչ տվյալ է հավաքում և մշակում GPS (ՋիՓիէս) սարքավորումը:
15. Ինչպե՞ս է կոչվում սոցիալական մեդիայում ամենից շատ հրապարակվող վիզուալ անձնական տվյալը:



1. Ինչպե՞ս է կոչվում հեռախոսը, որն աշխատում է օպերացիոն համակարգով:
2. Ինչպե՞ս են մեր օրերում անվանում կեղծ տեղեկությունը և կեղծ օգտահաշիվը սոցիալական մեդիայում:
3. Ինչպե՞ս է կոչվում համացանցային ամենատարածված էլեկտրոնային հանրագիտարանը:
4. Ինչպե՞ս են կոչվում արագ հաղորդակցության գործիքները մեր օրերում, որոնք հաճախ համակցված են սոցիալական ցանցերին:
5. Ինչպե՞ս է կոչվում գործարար կապեր գտնելու և հաստատելու համար նախատեսված սոցիալական մեդիան:
6. Ինչպե՞ս է կոչվում սոցիալական մեդիայում որևէ գրառման տակ գրված կարծիքը:
7. Առցանց ի՞նչ գործիքով է հնարավոր ստուգել որևէ վայրի տեղակայումը, ռելիեֆը, տեսարանը և այլ մանրամասներ:
8. Ինչպե՞ս է կոչվում այն բանաձևը, որի հիման վրա սոցիալական մեդիայում օգտատիրոջն առաջարկվում է գովազդ և հետաքրքրող բովանդակություն:
9. Ի՞նչ զգացմունք են հաճախ արտահայտում սոցիալական մեդիայում և մեսենջերներում «ճ» «Դ» նիշերը:
10. Ինչպե՞ս է կոչվում սոցիալական մեդիայի մեր էջը, որտեղ տեսնում ենք նորություններ և հրապարակումներ մեր ընկերներից, երբեմն գովազդ և այն ամենը, ինչին հետևում ենք:
11. Էլեկտրոնային ռ՞ի գործիքն է կիրառվում աշխատանքային և անձնական նամակագրությունների և հաղորդակցության համար:
12. Ինչպե՞ս է կոչվում տեսանյութերի համար նախատեսված ամենամեծ հարթակը:
13. Ինչպե՞ս են կոչվում ցանցային վարվեցողության և վարքագծային կանոնները, որոնք պետք է պահպանել:
14. Ինչպե՞ս են կոչվում ծրագրային ապահովումները, որոնք նախատեսված են վեբ-կայքեր մուտք գործելու, դիտելու, հարցումներ ուղարկելու համար:
15. Ինչպե՞ս է կոչվում համացանցային հաղորդակցությունը ծայնի և պատկերի միջոցով:



1. Ինչպե՞ս է կոչվում ծրագրային ապահովումը, որի նպատակն է հայտնաբերել վնասակար ծրագրեր և չեզոքացնել դրանք:
2. Ինչպե՞ս է կոչվում էլեկտրոնային փոստի գովազդային նամակը կամ փոստային աղբը:
3. Ի՞նչը պետք է պարունակի ն լատինական տառեր, ն թվեր, ն նիշեր:
4. Ինչպե՞ս է կոչվում Գուգլ Զբոմ դիտարկչում անվտանգ որոնում իրականացնելու էջը, որտեղ չի գրանցվում որոնումների պատմությունը:
5. Ո՞րն է այն կենսաչափական անձնական տվյալը, որով հնարավոր է բլոկավորել հեռախոսի էկրանը:
6. Ինչպե՞ս են կոչվում շարժական և թեթև համակարգիչները:
7. Ինչպե՞ս են անվանում հարձակման այն տեսակը, որը տեղի է ունենում թվային/առցանց միջավայրում:
8. Բացի գաղտնաբառից՝ էլ ի՞նչ է հարկավոր որևէ սոցիալական օգտահաշիվ մուտք գործելու համար:
9. Ինչպե՞ս է կոչվում ժառանգություն ստանալու կամ համացանցային մրցույթում հաթող ճանաչվելու վերաբերյալ կեղծ նամակը:
10. Ինչպե՞ս է կոչվում տեղեկությունների գաղտնիության ապահովմանն ուղղված կոդավորման գործընթացը:
11. Ինչպե՞ս են կոչվում տվյալների պահպանման արտաքին սարքերը:
12. Ո՞րն է առցանց հաղորդակցության համար ամենաանվտանգ մեքենայներից մեկը:
13. Ինչպե՞ս է կոչվում տվյալների հավաքման բազան, որտեղ տվյալները ենթարկվում են վերլուծությունների:
14. Ինչպե՞ս է կոչվում տեղեկության հոսքը, որը ևս պետք է պաշտպանել:
15. Բանկային ի՞նչ գործիքով ենք կատարում առցանց գնումներ:

1. Վերնագիր - Շատ հաճախ մարդիկ կարդում են Նորությունների վերնագրերը և չեն ծանոթանում բուն բովանդակությանը: Հարկավոր է իմանալ, որ երբեմն վերնագրերը խեղաթյուրվում և մանիպուլացվում են լսարանին մոլորեցնելու նպատակով: Այս պատճառով սոցիալական մեդիայում շրջանառվող լուրերի տակ կարելի է տեսնել բազմաթիվ իրարամերձ մեկնաբանություններ ամբողջ նյութը ընթերցած և միայն վերնագիրը կարդացած օգտատերերի միջև:

2. Տիկտոկ - 2022 թվականին Հայաստանում ամենաշատ ներբեռնված հավելվածը եղել է Տիկ-Տոկը: Սոցիալական այս մեդիա հարթակը նաև տարբերվում է իր լսարանի տարիքային կազմով, այստեղ շատ են երեխաները և դեռահասները: Տիկ-Տոկը հարթակ է, որտեղ մարդիկ ստեղծում, մշակում և հրապարակում են կարճ տեսանյութեր: Ի տարբերություն այլ սոցիալական մեդիաների՝ այս հարթակի ալգորիթմը կարող է հրապարակվող տեսանյութը հասանելի դարձնել միլիոնավոր մարդկանց, եթե անգամ օգտատիրոջը շատ քչերն են հետևում: Այն ստեղծվել է 2016 թվականին Մյուզիքլի անվանումով: Այս պահին (2022թ.) հավելվածը հասել է ավելի քան 1 միլիարդ օգտագործողի 150 երկրից:

3. Փողքաստ - Փողքաստ անվանում են աուդիոձայնագրությունները, որոնք լուսավորական, կրթական, ժամանցային և այլ բնույթի բովանդակություններ են: Եթե համեմատենք ավանդական մեդիայի հետ, ապա այն իր ձևաչափով նման է ռադիոյին: Սակայն, ի տարբերություն ռադիոյի, հրապարակվում է համացանցում, մասնավորապես փոքրաստների համար նախատեսված հարթակներում և սոցիալական մեդիայում: Փողքաստները հարմար է լսել ճանապարհին՝ աշխատանքի կամ դասի գնալիս:

4. Հեղինակ - Առհասարակ, երբ խոսում ենք մեդիայի վստահելիության և արժանահավատության մասին, գիտենք, որ նման դեպքերում օբյեկտիվ լրատվություն հայտնող ԶԼՄ-ների կայքերում հոդվածների սկզբում կամ վերջում կարելի է տեսնել հեղինակի ստորագրությունը: Ստորագրություն ասելով նկատի ունենք հեղինակի՝ լրագրողի անունը և ազգանունը: Հեղինակի անունը պարզելուց հետո միայն կարելի է անել եզրակացություններ:

5. Կարծիք Նորություններն ընթերցելիս մշտապես անհրաժեշտ է փաստերն ու կարծիքները տարանջատել միմյանցից: Երբեմն մեդիաների հրապարակած նյութերում կարծիքները ներկայացվում են փաստերին զուգահեռ՝ որպես իրողություն, և կասկածի չեն ենթարկվում: Կարծիքները ոչ շոշափելի և արքայական ձևակերպումներ են, որոնք հնարավոր չէ որևէ կերպ ստուգել, մինչդեռ փաստերը ապացուցելի են, և դրանք հնարավոր է ստուգել:

6. Սկզբնաղբյուր - Մեքերումներ կատարելիս լրատվամիջոցը, նյութի հեղինակը պարտադիր պետք է հղում անեն սկզբնաղբյուրին, որտեղից ստացվել է տեղեկությունը, և որտեղ կարելի է ստուգել դրա իսկությունը: Երբեմն մեդիաները հղում չեն անում սկզբնաղբյուրին՝ ելնելով տեղեկատվության աղբյուրի անվտանգությունից և լավագույն շահի սկզբունքից այն դեպքերում, երբ աղբյուրի հրապարակումը պարունակում է իրական ռիսկեր և կարող է անձի համար վտանգ պարունակել: Սակայն հաճախ ոչ արժանահավատ մեդիաները օգտվում են առիթից և «Մի վնասիր սկզբունք»-ի ներքո հրապարակում կեղծ տեղեկություններ՝ սկզբնաղբյուրի վերաբերյալ հիշատակման բացակայությունը հիմնավորելով որպես անձի անվտանգության ապահովման երաշխիք:

7. Թրոլինգ - Ժամանակակից մեդիայում կա «թրոլինգ» հասկացությունը: Սա այն գործընթացն է, երբ սոցիալական մեդիայում որևէ օգտատեր սադրում, հետապնդում և վիրավորում է այլ օգտատերերի՝ փորձելով նրանց հունից հանել և ստեղծել կոնֆլիկտային իրավիճակ: Այս օգտատերերին անվանում են թրոլ: Թրոլների նպատակն է ստեղծել իրարամերժ կարծիքների միջավայր և էմոցիոնալ ճնշումների միջոցով համացանցային վեճի համար նպաստավոր պայմաններ:

8. Գուգլ - Հայաստանում և առհասարակ աշխարհում ամենատարածված որոնողական համակարգը Գուգլն է: Գուգլը ստեղծվել է որպես Սթենֆորդի համալսարանի ուսանողներ Լարի Փեյջի և Սերգեյ Բրինի ուսումնական նախագիծ: Նրանք 1996 թվականին աշխատում էին BackRub որոնման համակարգի վրա, իսկ 1998 թվականին դրա հիման վրա ստեղծեցին Նոր Գուգլ որոնման համակարգը: Ամենաշատ գործածվող որոնողական համակարգն է (79.65 %): Ամսական ընդունում է ավելի քան 41 միլիարդ 345 միլիոն հարցում:

9. Մուլտիմեդիա - Այսօր մուլտիմեդիա կարելի է անվանել և՛ մեդիաներին, և՛ առանձին վերցված մեդիանյութերը: Մուլտիմեդիա ասելով հասկանում ենք, որ այն պարունակում է մեդիաբովանդակության տարբեր ձևաչափեր՝ տեքստ, լուսանկար, տեսանյութ, ձայնագրություն, շարժապատկեր, անիմացիա, գրաֆիկական լուծումներ և այլն: Մեր օրերում այս ձևաչափը շատ տարածված է և ընդունված, քանի որ տեքստին կամ պատկերին զուգահեռ առկա են նյութի ներկայացման բազմաթիվ այլ ձևաչափեր, որոնք նյութի ընկալումը դարձնում են առավել մատչելի:

10. Ջրպարտություն - Մարդուն ուղղված սուտ մեղադրանքը կոչվում է զրպարտություն: Հարկ է նշել, որ զրպարտությունը Հայաստանում դատապարտելի երևույթ է և կարող է պատժվել օրենքով սահմանված կարգով: Իրավականորեն այն բացատրվում է այսպես՝ անձի պատիվն ու արժանապատվությունը նվաստացնող կամ համբավն արատավորող ակնհայտ սուտ տեղեկությունների տարածում:

11. Հերքում - Բոլորն էլ սխալվում են: Սխալվում են նաև վստահելի և արժանահավատ մեդիաները: Սակայն լրագրության էթիկական սկզբունքները հստակորեն ընդգծում են. լրատվամիջոցը պետք է հեռացնի իր տարածած տեղեկությունը, եթե պարզվել է, որ այն սխալ է, և հրապարակի դրա վերաբերյալ հերքում՝ տալով ճշգրտված տեղեկությունը, որպեսզի լսարանն իրեն չզգա խաբված և մանիպուլացված: Անձի մասին տարածված սուտ տեղեկությունը նույնպես պետք է հերքվի, հակառակ դեպքում տուժողը կարող է դատական կարգով հերքում պահանջել, որի դեպքում բովանդակության հեղինակին առաջադրվում է մեղադրանք զրպարտության մասին հոդվածով:

12. Մեդիասպառող - Սովորաբար մեդիայի հետ առնչություն ունեցող մարդկանց բաժանում են երկու խմբի՝ մեդիասպառողներ և մեդիաարտադրողներ: Մեդիաարտադրողներն այն մարդիկ են, որոնք ստեղծում և տարածում են բովանդակություն: Մեդիասպառողները նրանք են, որոնք առավելապես կարդում, լսում կամ դիտում են մեդիաբովանդակությունները, սակայն չեն ստեղծում որևէ նոր բովանդակություն և/կամ չեն տարածում արդեն իսկ եղածները ուղեկցող այլ բովանդակությունների ստեղծմամբ:

13. Գովազդ - Սոցիալական մեդիայում նորությունների ժապավենը թերթելիս կարող են հայտնվել գովազդներ: Գովազդները գումարի միջոցով առաջխաղացվող բովանդակություններն են: Շատերը սոցիալական մեդիայում նշում են իրենց սեռը, տարիքը, բնակության վայրը, որոնումներ են կատարում իրենց հետաքրքրող բաների մասին: Այս տեղեկությունները համապատասխան ձևով վերլուծության են ենթարկվում ալգորիթմների կողմից, ինչի արդյունքում հաճախ օգտատիրոջ նորությունների ժապավենում հայտնվում են գովազդներ, որոնք տվյալ անձի հետաքրքրությունների սահմաններում են:

14. Դոմեն - Դոմենը որևէ կայքի հղումն է: Դոմենները երբևէ չեն կարող կրկնվել, ինչպես բնակարանների հասցեները: Սովորաբար դրանք ունենում են նույն անվանումը, ինչ կայքը, կայքում ներկայացված կազմակերպությունը, նախաձեռնությունը կամ ծառայություններ մատուցող ընկերությունը: Դոմենի միջոցով հնարավոր է այցելել տվյալ կայքը: Այն նույնականացված է և օգնում է հեշտորեն կոդմուրոշվելու համացանցում:

15. Մանիպուլյացիա - Հաճախ մեդիայում տեղեկությունը խեղաթուրվում է և լսարանին մոլորեցնելու նպատակ ունի: Նման գործընթացը մենք անվանում ենք մանիպուլյացիա: Մանիպուլյացիան հոգեբանական և էմոցիոնալ ներգործություն է ունենում մարդու վրա և առաջխաղացում է կեղծ տեղեկոյթներ և խոսույթներ: Մանիպուլյացիա կարող են համարվել, օրինակ, համատեքստից դուրս միտքը, կիսաճշմարտություն արտահայտելը, կարծրատիպեր կիրառելը և այլն:

1. Անձնագիր - Անձը հաստատող հիմնական փաստաթղթերից մեկը անձնագիրն է: Անձնագիրը պարունակում է բազմաթիվ անձնական տվյալներ, որոնց միջոցով հնարավոր է նույնականացնել անձին, օրինակ՝ լուսանկար, ստորագրություն, ծննդյան ամսաթիվ, բնակության վայր, անձնագրի սերիա և այլն: Հաճախ այս տվյալների միջոցով հնարավոր է իրականացնել գործարքներ: Այս պատճառով հարկավոր է ուշադիր և զգայուն լինել անձնական տվյալների հանդեպ:

2. Արտահոսք - Անձնական տվյալների արտահոսք կոչվում է այն գործընթացը, երբ անձնական տվյալներն առանց անձի համաձայնության, գիտության կամ ցանկության հայտնվում են երրորդ կողմի մոտ: Եթե դիտարկենք սոցիալական ցանցերը, ապա անձը՝ որպես տեղեկության տիրապետող, առաջին կողմն է, սոցիալական ցանցը, որի միջոցով շրջանառվել է տեղեկությունը, դիտարկվում է որպես երկրորդ կողմ, իսկ այլ օգտատերը, որի մոտ հայտնվել է այդ տեղեկությունը, երրորդ կողմն է: Անձնական տվյալը տնօրինողը պարտավոր է ապահովել տվյալների գաղտնիությունն ու անվտանգությունը և նվազագույնի հասցնել դրանց՝ երրորդ կողմի մոտ հայտնվելու հավանականությունը:

3. Երեխա - Երեխաներն ընտանիքի ամենախոցելի անդամներն են անձնական տվյալների պահպանման տեսանկյունից: Այս առումով նրանց վերաբերող անձնական տվյալները՝ լուսանկարները, տեսանյութերը, ֆիզիկական և առողջական վիճակին վերաբերող տեղեկությունները, համարվում են զգայուն, և դրանց արտահոսքը կամ հանրային հրապարակումը կարող է բացասաբար անդրադառնալ նրանց կյանքի որակի, ինչպես նաև հետագա՝ չափահաս տարիքում ծավալվող գործունեության վրա:

4. Ստորագրություն - Ստորագրությունն անձի ստեղծած անձնական տվյալ է, որի միջոցով հնարավոր է կատարել անձի նույնականացում, աշխատանքային և ֆինանսական գործարքներ: Ստորագրությունը նույնպես պետք է պահպանվի զգուշորեն, չփոխանցվի այլ անձանց, քանի որ դրա արտահոսքը կարող է հանգեցնել որոշակի նյութական, ֆինանսական և այլ տեսակի վնասների:

5. Հեռախոսագիրք - Հեռախոսագրքում պահպանվում են տեղեկություններ անձի կոնտակտային շրջանակի վերաբերյալ: Այստեղ հնարավոր է պահպանել հեռախոսահամարներ, էլեկտրոնային փոստի հասցեներ, աշխատանքի և կրթության վերաբերյալ տվյալներ, բնակության հասցեն, տարիքը, սեռը և այլն: Կան բազմաթիվ հեռախոսային հավելվածներ, որոնք մուտքի թույլտվություն են հարցնում հեռախոսագրքից, որպեսզի կարողանան անխոչընդոտ աշխատել և թույլ տալ անձին կիրառել հավելվածն ամբողջությամբ: Սակայն երբեմն այդ հավելվածների ֆունկցիոնալ նպատակը որևէ առնչություն չունի հեռախոսագրքի հետ: Այս դեպքերում պետք է առավել ուշադիր լինել և չտալ համապատասխան թույլտվություն:

6. Գաղտնալսում - Գաղտնալսումն առանց անձի թույլտվության անձի խոսակցություններին և հեռախոսագրույցներին հետևելն է, դրանք ձայնագրելը: Ավելի ուշ այս գործողությունը կարող է տանել այլ գործընթացների և, օրինակ՝ ձայնագրության արտահոսքի կազմակերպման և հրապարակման, ինչը կարող է հանգեցնել բարոյական և սոցիալական մի շարք խնդիրների, ինչպես նաև փոխել հանրության վերաբերմունքը տվյալ անձի նկատմամբ:

7. Հաքեր - Հաքերները, այլ կերպ ասած՝ ցանցահեղինները, մարդիկ են, որոնք թվային միջավայրում տիրապետում են բազմաթիվ գործիքների և մեթոդների, ունեն որոշակի փորձ և կարող են կոտրել անձի սոցիալական հաշիվները, հասանելիություն ձեռք բերել անձի անձնական տվյալներին և դրանք կիրառել այլ նպատակներով: Ընդ որում՝ ցանցահեղի նպատակը կարող է լինել ոչ միայն կոնկրետ մեկ մարդու վնաս հասցնելը, այլև մի խումբ մարդկանց տվյալների հասանելիություն ստանալու միջոցով այդ խմբին խոցելի դարձնելը:

8. Ծանուցում - Անձնական տվյալներ մշակողը կամ լիազորված անձը պարտավոր է տվյալների սուբյեկտի գրավոր համաձայնությունը ստանալու նպատակով տվյալների սուբյեկտին ծանուցել տվյալներ մշակելու մտադրության մասին: Այս ամենն ամրագրված է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով, որտեղ նաև նշվում է, թե ինչ պետք է պարունակի ծանուցումը, մասնավորապես՝ ծանուցման մեջ նշվում են՝ 1) տվյալների սուբյեկտի ազգանունը, անունը, հայրանունը, 2) անձնական տվյալների մշակման իրավական հիմքերը և նպատակը, 3) մշակման ենթակա անձնական տվյալների ցանկը, 4) անձնական տվյալներով կատարման ենթակա գործողությունների ցանկը, որոնց համար հայցվում է տվյալների սուբյեկտի համաձայնությունը, 5) այն անձանց շրջանակը, որոնց կարող են փոխանցվել անձնական տվյալները, 6) անձնական տվյալների սուբյեկտի համաձայնությունը հայցող մշակողի կամ նրա ներկայացուցչի անվանումը (ազգանունը, անունը, հայրանունը, պաշտոնը) և գտնվելու կամ հաշվառման (փաստացի բնակության) վայրը, 7) տվյալների սուբյեկտի կողմից անձնական տվյալների ուղղում, ոչնչացում, տվյալների մշակման դադարեցում պահանջելու կամ մշակմանն առնչվող այլ գործողություն կատարելու վերաբերյալ տեղեկություններ, 8) հայցվող համաձայնության գործողության ժամկետը, ինչպես նաև համաձայնությունը հետ կանչելու կարգը և դրա հետևանքները:

9. Տեսահսկում - Հանրային վայրերում տեսախցիկների միջոցով տվյալների հավաքումը կոչվում է տեսահսկում: Տեսահսկում իրականացնողը պարտավոր է քաղաքացիներին տեղեկացնել տեսահսկման մասին, հակառակ դեպքում այն համարվում է «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի խախտում: Նույնը ձայնագրությունների դեպքում է. ձայնագրողը պարտավոր է անձին ծանուցել ձայնագրման մասին:

10. Ռեգիստր - ՀՀ կենտրոնական ընտրական հանձնաժողովն ունի ընտրելու իրավունք ունեցող քաղաքացիների ցանկ-շտեմարան, որը կոչվում է ՀՀ ընտրողների ռեգիստր: Ռեգիստրում ներառված են անձի անունը, ազգանունը, հայրանունը, ծննդյան ամսաթիվը, գրանցման հասցեն, ինչպես նաև նույն հասցեի ներքո գրանցված այլ անձանց համանման տվյալները: Ռեգիստրի նպատակն է նվազագույնի հասցնել կամ բացառել ընտրախախտումները լցոնումների տեսքով՝ պայմանավորված միևնույն հասցեից բազմաթիվ ընտրողների ներգրավմամբ:

11. Հարցում - «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը սահմանում է, որ տվյալների սուբյեկտին անձնական տվյալները տրամադրվում են տվյալ անձի կամ լիազորագրով հանդես եկող ներկայացուցչի կամ օրինական ներկայացուցչի գրավոր հարցման հիման վրա: Հարցումը կարող է ներկայացվել էլեկտրոնային եղանակով՝ հաստատված էլեկտրոնային թվային ստորագրությամբ: Համաձայն օրենքի՝ տվյալների սուբյեկտն իրավունք ունի տեղեկություն ստանալու իր անձնական տվյալների մշակման վերաբերյալ, այդ թվում՝ 1) անձնական տվյալները մշակելու փաստը հաստատելու և մշակելու նպատակի վերաբերյալ, 2) անձնական տվյալները մշակելու եղանակների վերաբերյալ, 3) այն սուբյեկտների վերաբերյալ, որոնց տրամադրվել կամ կարող են տրամադրվել անձնական տվյալները, 4) մշակվող անձնական տվյալների ցանկի և դրանք ձեռք բերելու աղբյուրի վերաբերյալ, 5) անձնական տվյալները մշակելու ժամկետների վերաբերյալ, 6) անձնական տվյալները մշակելու հետևանքով տվյալների սուբյեկտի համար առաջացող հնարավոր իրավական հետևանքների վերաբերյալ:

12. Դիմապատկեր - Հաճախ սմարթֆոններն իրենց սեփականատերերին նույնականացնում են դիմապատկերի (Face ID) միջոցով: Այս գործառնության նպատակն է ապահովել առավելագույն անվտանգություն, ինչպես նաև հեշտացնել հեռախոսի էկրանի ապաբլոկավորումը: Դիմապատկերը և դրա միջոցով տեղեկությունների հավաքումը՝ նույնականացման նպատակով, ևս համարվում է անձնական տվյալ, որի արտահոսքը կարող է մեծ վնասներ հասցնել:

13. Հեռախոսահամար - Հեռախոսահամարն այն անձնական տվյալն է, որի մուտքագրումը և պահպանումը սոցիալական հաշիվների կարգավորումներում շատ կարևոր է, քանի որ դրա միջոցով հնարավոր է իրականացնել անձի նույնականացումը, ինչը թույլ կտա, օրինակ, գաղտնաբառը մոռանալու դեպքում այն հեշտությամբ վերականգնել կամ բլոկավորված հաշիվը հեշտությամբ ապաբլոկավորել:

14. Տեղակայում - GPS սարքավորումը, որը ներկայում օգտագործվում է ժամանակակից տեխնոլոգիաներում՝ համակարգիչներում, դյուրակիր համակարգիչներում, սմարթֆոններում, խելացի ժամացույցներում, հավաքում և մշակում է անձի տեղակայման վայրի վերաբերյալ տվյալները: Այդ տվյալները հետագայում օգտագործվում են եղանակի տեսության, խցանումների, գովազդների արդյունավետ իրացման նպատակով:

15. Լուսանկար - Սոցիալական մեդիայում ամենից շատ հրապարակվող անձնական տվյալը լուսանկարն է: Ընդ որում՝ շատ կարևոր է մեծ ուշադրություն դարձնել լուսանկարում արտացոլված դետալներին, որոնք կարող են արտացոլել բազմաթիվ անձնական տվյալներ, մասնավորապես՝ գտնվելու վայրի, ժամի, նկարում հայտնված փաստաթղթի վերաբերյալ տեղեկություններ: Շատ կարևոր է նաև իմանալ, որ լուսանկարները պարունակում են մետատվյալներ՝ տվյալներ լուսանկարի վայրի, ամսաթվի, ծավալի և այլ մանրամասների վերաբերյալ:

1. Սմարթֆոն - Օպերացիոն համակարգով աշխատող հեռախոսները կոչվում են սմարթֆոն, այլ կերպ ասած՝ խելացի հեռախոս: Սմարթֆոնները պարունակում են ժամանակակից տեխնոլոգիաների ֆունկցիոնալ մի շարք հնարավորություններ՝ տեսալուսանկարահանման, տեղակայման, համաժամանակյա աշխատանքի, տեղեկությունների շրջանառման, հավելվածների միջոցով աշխատանքներ իրականացնելու համար: Այս ամենին զուգահեռ մեծանում են նաև վտանգները, քանի որ սմարթֆոնները պարունակում են մեծածավալ զգայուն տվյալներ, ինչպիսիք են, օրինակ, մատնահետքը, դիմապատկերը, հեռախոսագիրքը, փաստաթղթեր, սոցիալական մեդիայի հաշիվներ, գաղտնաբառեր, լուսանկարներ, աուդիո և վիդեո ձայնագրություններ և այլն:

2. Ֆեյք - Մեր օրերում կեղծ տեղեկությունը և կեղծ օգտահաշիվը սոցիալական մեդիայում անվանում են ֆեյք: Այս արտահայտությունն այնքան է կիրառվել առօրյայում, որ այն անգամ հնչում է այնպիսի բարձր ամբիոններից, ինչպիսիք են Կառավարությունը, Ազգային ժողովը և այլն: Ֆեյքերը, սովորաբար, անանուն կամ կեղծ անվան ներքո չնույնականացվող օգտատերեր են, որոնք գործում են քաղաքական, սոցիալական, տնտեսական որևէ շահի հետապնդող խմբի կողմից: Ֆեյքերը հաճախ նպաստում են հասարակության շրջանում կեղծ պատումների տարածմանը և խթանում են խոսույթների շրջանառմանը, որոնք կարող են հանգեցնել կեղծ պատկերացումների, առաջխաղացնել դավադրապաշտական տեսությունները և այլն:

3. Վիկիպեդիա - Համացանցային ամենալայն տարածում ունեցող ազատ հանրագիտարանը Վիկիպեդիան է: Վիկիպեդիան հանրագիտարանային հարթակ է, որտեղ ցանկացած ոք կարող է գրանցվել և ստեղծել հոդվածներ, խմբագրել արդեն ստեղծված հոդվածները: Ցանկացած նոր բովանդակություն, որը ստեղծում, մշակում է առավել նոր՝ կրտսեր խմբագիրը, ստուգում են նաև ավագ խմբագիրները: Այդուհանդերձ, այն չի կարելի համարել տեղեկություն ստանալու արժանահավատ աղբյուր: 2022 թվականի դրությամբ Վիկիպեդիայում կան շուրջ 300000 հայերեն հոդված և շուրջ 400 ակտիվ խմբագիր:

4. Մեսենջեր - Սոցիալական ցանցերին համակցված, ինչպես նաև անկախ գործող արագ հաղորդակցության գործիքները կոչվում են մեսենջեր: Մեսենջերների նպատակն է խթանել սոցիալական ցանցերի ստեղծումը, մարդկանց անսահմանափակ հաղորդակցությունը: Դրանց միջոցով հնարավոր է շրջանառել ոչ միայն տեքստեր, այլև լուսանկարներ, տեսանյութեր, ձայնագրություններ: Մեսենջերներում հնարավոր է ստեղծել խմբեր՝ բաղկացած համապատասխան մեսենջերը կիրառող օգտատերերից, կատարել զանգեր և տեսազանգեր:

5. Լինկդին - Լինկդինը սոցիալական ցանց է, որի նպատակն է խթանել գործարար աշխարհի զարգացումն ու ցանցերի ստեղծումը: Այս հարթակում օգտատերերը մուտքագրում են տեղեկություններ իրենց ֆորմալ և ոչ ֆորմալ կրթության, աշխատանքային փորձի վերաբերյալ, կարող են զետեղել կարողությունների, հմտությունների և գիտելիքների վերաբերյալ տեղեկություններ, որոնց միջոցով հարթակը ստեղծում է կապեր տվյալ ոլորտի այլ մասնագետների հետ: Այս ցանցում առավել հաճախ կարելի է տեսնել աշխատանքի հայտարարություններ տեղական և միջազգային շուկաներից:

6. Մեկնաբանություն - Սոցիալական մեդիայում օգտատերերը կարող են հրապարակել գրառումներ: Գրառումների տակ կա կարծիք և միտք արտահայտելու դաշտ, որը կոչվում է մեկնաբանությունների դաշտ: Որոշ սոցիալական մեդիաներում կան կարգավորումներ, որտեղ օգտատերն ինքն է որոշում՝ թույլ տալ իր ընկերներին, իրեն հետևողներին և այլ օգտատերերի մեկնաբանել հրապարակումը, թե ոչ: Երբեմն մեկնաբանությունների դաշտում գրվում են իրարամերժ կարծիքներ, և առաջանում է կոնֆլիկտ, սակայն մեդիագրագետ մարդիկ փորձում են խուսափել նման իրավիճակներից: Որքան շատ են գրառման մեկնաբանությունները, այնքան ավելի շատ մարդ է տեսնում տվյալ գրառումը:

7. Քարտեզ - Համացանցում կան բազմաթիվ ընկերություններ, որոնք ունեն առցանց՝ էլեկտրոնային քարտեզներ և առաջարկում են օգտվել իրենց ծառայություններից: Ընդ որում՝ այդ ծառայությունների մեծ մասն անվճար է: Ամենատարածված քարտեզը Գուգլի թողարկած Google Maps և Google Earth գործիքներն են, որոնց միջոցով կարելի է տեսնել հասցեները, օբյեկտների տեղակայման վայրերը, այդ տարածքներից հրապարակված լուսանկարները և այլն:

8. Ալգորիթմ - Սոցիալական մեդիաների համար ծրագրավորողները մշակել են բանաձև, որը կոչվում է ալգորիթմ: Ալգորիթմը մաթեմատիկական հաշվարկների վրա հիմնված և տրամաբանական քայլերի հաջորդականությունը սահմանող բանաձև է, որը հավաքված տեղեկությունների հիման վրա ձևավորում է օգտատիրոջ միջավայրը: Օրինակ՝ հավաքում է տվյալներ օգտատիրոջ տարիքի, սեռի, բնակության վայրի, հետաքրքրությունների, հրապարակած նյութերի, որոնողական համակարգերի միջոցով փնտրած տեղեկության, դիտած տեսանյութերի, հավանումների, մեկնաբանությունների վերաբերյալ, վերլուծում և առաջարկում է համանման բովանդակություններ, իրացնում է գովազդ, որի սպառման հավանականությունն օգտատիրոջ կողմից մեծանում է:

9. Ծիծաղ - Հաճախ սոցիալական մեդիայի օգտատերերն իրենց ժպիտը և ծիծաղն արտահայտելիս գրում են «Գ;» «Դ;»: Լատինատառ ստեղծաշարում նույն ստեղծների ներքո գտնվում են հետևյալ նիշերը «;» «D;»: Եթե սոցիալական մեդիայում կիրառվի Նշված նիշերի համադրումը և ուղարկվի որևէ մեկին, ապա հաստատման կոճակը սեղմելուց հետո դրանք կվերածվեն ժպիտի և ծիծաղի էմոջիների: Այլ կերպ ասած՝ էմոջիները փնտրելու և գտնելու փոխարեն օգտատերերն արագորեն հավաքում են այդ նիշերը և հաղորդում իրենց զգացողությունը:

10. Ժապավեն - Սոցիալական մեդիայում յուրաքանչյուր օգտատեր ունի Նորությունների ժապավեն: Նորությունների ժապավենը սոցիալական մեդիայի այն հատվածն է, որտեղ արտացոլվում են օգտատիրոջ ընկերների գրառումները, շրջանառված հրապարակումները, օգտատիրոջն ավտոմատ առաջարկվող գովազդը և հետաքրքրող այլ բովանդակություններ:

11. Փոստ - Աշխատանքային և անձնական Նամակագրություններն առավել պրոֆեսիոնալ վարողներն օգտվում են էլեկտրոնային փոստերից: Էլեկտրոնային փոստերը նույն մեյլերն են, որոնք առանձնահատուկ են և չկրկնվող: Էլեկտրոնային փոստերի միջոցով հնարավոր է վարել գործնական Նամակագրություններ, ուղարկել և ստանալ տարբեր ձևաչափերի ֆայլեր: Շատ կարևոր է էլեկտրոնային փոստի ծառայությունն ընտրելիս դիտարկել առաջարկվող պայմաններն ու հնարավորությունները, որպեսզի այն լինի պարզ, մատչելի, ապահով և անվտանգ:

12. Յուրթյուր - Յուրթյուրը համացանցում տեսանախագծային կայք է, որի օգտատերերը և այցելուները կարող են հրապարակել, դիտել և տարածել տեսանյութեր: Յուրթյուրի գրասենյակը Սան Բրունոյում է և ստեղծվել է 2005 թվականի փետրվարին: 2006 թվականի նոյեմբերի 13-ին Գուգլը այն գնել է 1,6 միլիարդ ԱՄՆ դոլարով: 2020 թվականի մայիսին Յուրթյուրը ունեցել է 41,9 միլիոն ալիք և ընդհանուր առմամբ 5 միլիարդ տեսանյութ:

13. Նեթիկետ - Նեթիկետը ցանցային վարվեցողության կանոնների ընդհանրությունն է: Բառի հիմքում էթիկան է՝ էթիկետը, սակայն քանի որ այն ցանցային էթիկայի մասին է, անգլերենում կոչվում է նեթվորք էթիկետ (անգլ. net «ցանց» + ֆրանս. etiquette «էթիկետ») և ժամանակի ընթացքում փոխակերպվել է այնքան, մինչև հայերենում ամրապնդվել է նեթիկետ արտահայտությունը: Ահա մի քանի կանոն ցանցային էթիկետից.

1. Հիշե՛ք, որ դուք մարդու հետ եք խոսում:
2. Հետևե՛ք վարվեցողության նույն կանոններին, ինչ իրական կյանքում:
3. Հիշե՛ք, թե կիրառարարության որ մասում եք: Նեթիկետը յուրաքանչյուր համակարգչում տարբեր է:
4. Հարգե՛ք դիմացինի ժամանակն ու հնարավորությունները:
5. Պահե՛ք սեփական դեմքը, արժանապատվությունը:
6. Եթե կարող եք, օգնե՛ք ուրիշներին:
7. Մի՛ մտեք կոնֆլիկտի մեջ:
8. Հարգե՛ք դիմացինի անձնական հաղորդակցման իրավունքը:
9. Ձեր հնարավորությունները մի՛ չարաշահեք:
10. Սովորե՛ք ներել ուրիշների սխալները:

14. Դիտարկիչ - Դիտարկիչը՝ նույն բրաուզերը, ծրագրային ապահովում է, որը նախատեսված է վեբ-կայքեր դիտելու, այսինքն՝ վեբ կայքերին դիմելու, դրանցից ստացված տեղեկությունը վերամշակելու, կայքը արտածելու և մի էջից մյուսն անցնելու համար: Համաշխարհային ցանցի ստեղծման օրվանից ցանցային դիտարկիչներն անընդհատ կատարելագործվում են, և ժամանակի ընթացքում ավելի ու ավելի են մեծանում դրանց կարևորությունն ու պահանջարկը: Այժմյան ցանցային դիտարկիչը վեբ-կայքի մշակման և արտածման համար նախատեսված ծրագրային համակարգ է, որը վեբ-կայքի և իր հաճախորդի միջև միջանկյալ օղակ է, միջավայր: Գրեթե բոլոր հայտնի ցանցային դիտարկիչներն այլ լրացնող ծրագրերի հետ անվճար տարածվում են:

15. Տեսագանգ - Տեսագանգը սոցիալական մեդիայի մեսենջերներում առկա ֆունկցիոնալ հնարավորություն է: Այն կարող է լինել նաև առանձին ծրագրային ապահովումների և հավելվածների տեսքով: Այս գործիքի նպատակն է կատարել անհատական և խմբային զանգեր, զանգերին զուգահեռ տեսնել ուղեկցվող պատկերը: Տեսագանգի ծառայությունները մեծ զարգացում և տարածում գտան Քովիդ-19 համավարակի պայմաններում, երբ մարդիկ անցան հեռավար աշխատանքի և կրթության ձևաչափերի:

1. Հակավիրուս - Հակավիրուսային ծրագրերի նպատակն է կանխել, հայտնաբերել, ոչնչացնել վնասակար ծրագրերը: Հակավիրուսային ծրագրերը, կախված իրենց տեսակից, վնասակար ծրագիր հայտնաբերելու դեպքում կատարում են տարբեր գործողություններ: Տրոյանները և Որդերը (վնասակար ծրագրեր) ամբողջությամբ բաղկացած են վնասակար կոդից և որևէ օգտակար տեղեկություն չեն պարունակում, այդ իսկ պատճառով էլ հակավիրուսը դրանք ջնջում է: Դասական վիրուսներն իրենց կոդերով այլ ֆայլերի մեջ են, հետևաբար դրանց նկատմամբ կիրառվում է «բուժում», այսինքն՝ ֆայլի կոդը մաքրվում է վիրուսային հատվածից:

2. Սպամ - Աղբային էլեկտրոնային փոստի նամակները, որոնք մեզ բերում են անցանկալի գովազդներ, հայտարարություններ, կոչվում են սպամ: Երբեմն սպամները հայտնվում են հենց դրանց համար նախատեսված պանակում, երբեմն էլ՝ մեր ընդհանուր նամակների մեջ: Ընդհանուր նամակների մեջ հայտնվելու պարագայում հարկավոր է այն տեղափոխել համապատասխան սպամ պանակ, որպեսզի նույն հասցեից հետագայում ստացված նամակները նույնպես հայտնվեն սպամում կամ ավտոմատ բլոկավորվեն:

3. Գաղտնաբառ - Գաղտնաբառը սիմվոլների հերթականություն է, որն օգտագործվում է ինքնությունը կամ իրավասությունը հաստատելու համար: Գաղտնաբառը գաղտնի է պահվում բոլոր այն անձանցից, որոնք չունեն մուտք գործելու իրավասություն: Վստահելի և ապահով գաղտնաբառերը պարունակում են առնվազն 10-12 նիշ, որոնց մեջ կան և՛ լատինական այբուբենի մեծատառեր ու փոքրատառեր, և՛ թվեր, և՛ հատուկ նիշեր, օրինակ՝ #, *, \$, !, @ և այլն:

4. Ինկոգնիտո - Ինկոգնիտոն Գուգլ որոնողական համակարգում որոնումներ իրականացնելու առանձնահատուկ ռեժիմ է, որի դեպքում դիտարկիչը չի գրանցում որոնումների պատմությունը, չի պահպանում սոցիալական հաշիվների մուտքի տվյալները՝ մուտքանունը, գաղտնաբառը և այլ տվյալներ, որոնք կարող են պահպանվել դիտարկիչի կարգավորումներում: Սակայն պետք է իմանալ, որ այս տվյալները, այդուհանդերձ, տեսանելի են ինտերնետ մատակարարին:

5. Մատնահետք - Մատնահետքը հաճախ հանդիպող այն անձնական տվյալն է, որ միջոցով հնարավոր է բլոկավորել և ապաբլոկավորել սմարթֆոնի էկրանը: Պետք է իմանալ, որ այս պարագայում սմարթֆոնը պարունակում է տեղեկություններ սեփականատիրոջ մատնահետքի վերաբերյալ: Ընդ որում՝ սմարթֆոնը թույլ է տալիս մատնահետքը կիրառել նաև բջջային հավելվածներ մուտք գործելու համար, օրինակ՝ բանկային հավելվածներ և այլն:

6. Դյուրակիր - Դյուրակիր են կոչվում այն համակարգիչները, որոնք շարժական են, թեթև և մատչելի տեղաշարժելու համար: Դյուրակիր են համարվում նոթբուքերը, նեթբուքերը, ուլտրաբուքերը, քրոմբուքերը, սենսորային վահանակները (պլանշետ) և այլն: Շատ կարևոր է, որ դյուրակիր համակարգիչն ամրացված լինի աշխատանքային սեղանին, եթե կա որոշակի ռիսկ, որ այն կարող են գողանալ: Դյուրակիր համակարգիչների պաշտպանության առումով ֆիզիկական ռիսկերը շատ ավելին են, քանի որ դրանք կարող են գողանալ դրսում, ինչպես նաև վնասվել տեղափոխելիս կամ մոռացվել որևէ վայրում, ինչի պատճառով կարող է տեղի ունենալ անձնական տվյալների արտահոսք:

7. Կիբեռ - Կիբեռհարձակումներն այսօր շատ տարբեր են ընդամենը մի քանի տարի առաջվա համեմատ: Այժմ էլեկտրոնային սարքերի մեծ մասը՝ հեռախոսներ, հեռուստացույցներ, համակարգիչներ, պլանշետներ, խելացի տան սարքավորումներ (սենսորներ, տեսախցիկներ) և այլն, կարող է միացված լինել համացանցին: Այս բոլոր համակարգերն ունեն ԱյՖի (IP) Նույնականացման հասցեներ, ուստի դրանք հետևելի և հասանելի են համացանցի միջոցով: Կիբեռհարձակումների միջոցով կոտրվում են արգելապատնեշները, որոնց միջոցով ցանցահեղինները հասանելիություն են ունենում համացանցին կապակցված սարքերին, կարողանում են դրանք կառավարել հեռավար եղանակով, ձեռք բերել դրանցում առկա տեղեկությունները:

8. Մուտքանուն - Մուտքանունը սոցիալական ցանցեր, էլեկտրոնային մի շարք հաշիվներ մուտք գործելու համար պահանջվող տեղեկության լրացման դաշտի համար նախատեսված տվյալներն են: Շատ հաճախ որպես մուտքանուն կարող է հանդես գալ էլեկտրոնային փոստի հասցեն, հեռախոսահամարը կամ օգտատիրոջ ստեղծած որևէ արտահայտություն: Մուտքի համար էլեկտրոնային համակարգերը սովորաբար պահանջում են մուտքանուն և գաղտնաբառ:

9. Ֆիշինգ - Ֆիշինգը կիբեռհանցագործության տեսակ է, որի նպատակն է ստանալ որևէ սոցիալական կայքի օգտատիրոջ գաղտնի տվյալները, ծածկագիրը, ծածկանունը, անձնագրային և բանկային տվյալները: Սա կատարվում է զանգվածային էլեկտրոնային սպամ նամակների միջոցով, որոնք հասցեատիրոջը հասնում են հայտնի բրենդների անունից, ինչպես նաև տարբեր ծառայությունների վերաբերյալ անձնական նամակներ, օրինակ, բանկի կամ սոցիալական ցանցերի կողմից: Նամակը հաճախ պարունակում է ուղղակի կայքի հղումը, որը արտաքինապես չի տարբերվում իրական կայքից, որտեղ մուտք գործելիս և անձնական տվյալներ մուտքագրելիս դրանք փոխանցվում են խաբեբաներին: Հաճախ ֆիշինգային նամակները ստացվում են հեռավոր ազգականի կտակը ստանալու վերաբերյալ ծանուցմամբ, որից հետո օգտատիրոջից պահանջում են ներկայացնել անձը հաստատող տեղեկություններ և կատարել նախնական վճարումներ:

10. Գաղտնագրում - Գաղտնագրումը (նաև՝ ծածկագրում) մեր և մեր տեղեկության պաշտպանության կարևորագույն տարրն է առօրյա կյանքում և առցանց շփվելիս: Այն ապահովում է մեր շրջանառած և պահպանած տեղեկության գաղտնիությունը: Սոցիալական մեդիայում և մեսենջերներում հաղորդակցվելիս մեր ուղարկած նամակները գաղտնագրվում են, դրանք ապագաղտնագրվում են միայն այն օգտատիրոջ սարքավորման մեջ, որին ուղարկվել է այն: Նույնը համակարգչում պահպանվող տեղեկության գաղտնագրումն է, որը հնարավոր է ակտիվացնել Բիթլոքերի (Bitlocker) միջոցով: Այս դեպքում որևէ մեկը չի կարող հասանելիություն ունենալ համակարգչում առկա տեղեկությանը, եթե չունի գաղտնագրման համար նախատեսված գաղտնաբառը:

11. Կրիչ - Կրիչները հիշողության արտաքին սարքավորումներ են, որոնք կարող են պահպանել մեծաքանակ տեղեկություններ և ֆայլեր: Կրիչները կարող են լինել USB ֆլեշեր, հիշողության միկրոքարտեր, ճկուն սկավառակներ, կոշտ սկավառակներ, սկավառակներ և այլն: Կրիչները նույնպես խոցելի են, եթե դրանք հայտնվեն ոչ ցանկալի ձեռքերում, և տեղի ունենա տեղեկության արտահոսք: Կրիչների պաշտպանության լավագույն միջոցը դրանց հասանելիության գաղտնաբառի նշանակումն է և դրանցում առկա տեղեկության գաղտնագրումը:

12. Սիգնալ - Մինչ այս պահը (2022 թ.) Սիգնալը համարվում է ամենաապահով, անվտանգ և գաղտնի մեսենջերը: Անդրոիդի համար հավելվածը կարող է օգտագործվել նաև ոչ ծածկագրված SMS-ների ուղարկման և ստացման համար: Մինչև 2015 թվականի նոյեմբերը հավելվածը կոչվում էր «TextSecure» և թույլ էր տալիս միայն անկախ թափաթեկի հաղորդագրությունների փոխանակում: Նոր անվան հետ միացվել է նաև «RedPhone» հավելվածի զանգերի գործառնությունը:

13. Շտեմարան - Շտեմարանը տվյալների բազա է, որտեղ հավաքվում են մեծաքանակ և մեծածավալ տեղեկություններ: Շտեմարաններում տեղեկությունները հնարավոր է թարմացնել, ֆիլտրել՝ ըստ դասակարգիչների և տեսակների, ինչն օգնում է վերլուծելու տվյալները: Կան բազմաթիվ շտեմարաններ, որոնք հավաքում են մարդկանց մասին անձնական տվյալներ՝ անուն, ազգանուն, սեռ, տարիք, բնակության վայր, հեռախոսահամար, էլեկտրոնային փոստի հասցե և այլն: Այս տեղեկությունները կարող են վաճառվել սև շուկայում գովազդի իրացման նպատակով:

14. Թրաֆիկ - Օգտվողի բոլոր այցելությունները կարող են վերահսկվել, եթե չեն կիրառվում հատուկ պաշտպանական միջոցներ: Մարդու այցելած կայքերի, ընթերցած հոդվածների ցանկը կարող է վերահսկել երրորդ կողմը: Հատկապես եթե օգտվողն այցելում է կայքեր, որոնք պաշտպանված չեն <https> գաղտնագրմամբ: Պետք է հիշել, որ եթե կայքը չի միանում <https> տարբերակով, ապա դրանում չի կարելի մուտքագրել ոչ մի զգայուն տեղեկություն՝ գաղտնաբառեր, անձնական տվյալներ և այլն: Եթե <https>-ն ակտիվացված չէ կայքում, ապա ամբողջ բովանդակությունը կարող է ազատ ընթերցել երրորդ անձը: Հանրային WiFi կապից օգտվելիս (սրճարաններում, օդանավակայաններում) նույնպես կարելի է կորցնել կարևոր տեղեկություններ, օրինակ՝ գաղտնաբառեր, բանկային տվյալներ և այլն: Հաքերները նման հանրային կետերն օգտագործում են օգտվողների վրա հարձակումների համար:

15. Քարտ - Բանկային քարտը այն հիմնական միջոցն է, որի շնորհիվ հնարավոր է կատարել առցանց գնումներ, ինչպես նաև անհպում վճարումներ: Այս ամենը հեշտացնում է մարդու կյանքը, սակայն զուգահեռ առաջ է բերում բազմաթիվ ռիսկեր: Շատ կարևոր է, որ քարտապանը գաղտնի պահի իր քարտի վրա արտացոլված թվերը, գործողության ժամկետը և քարտի հետևամասում արտացոլված եռանիշ CVV կոդը: Եթե այդ տվյալները հայտնվեն երրորդ կողմի մոտ, ապա չարագործը կարող է կատարել առցանց գործարքներ ու գնումներ քարտապանի հաշվին: Չի խրախուսվում նկարել քարտը և ուղարկել մեկ ուրիշին էլեկտրոնային փոստի կամ մեսենջերների միջոցով և/կամ քարտի տվյալները մուտքագրել ոչ վստահելի կայքերում:



Դի-Վի-Վի Ինթերնեյշնալի հայաստանյան գրասենյակ



info@dvv-international.am



www.dvv-international.ge/am



Հանրային լրագրության ակումբ



info@pjc.am



www.pjc.am