

Сәлем!
Бұл кітап сізге технологиялар әлеміндегі түрлі
құбылыстар туралы айтып береді, сондай-ақ
ғаламторда өзіңізді және деректеріңізді қалай
қорғауға болатынын пайдалы кеңестер
ұсынады.
Сапарың сәтті өтсін!

Киберәліппе



Бұл кітап иесі _____



Цифрлық әлемді зерттеушілерге арналған

Сен «Киберқауіпсіздік әліппесін» қолыңа ұстап тұрсың. Бұл не? Киберқауіпсіздік бізге заманауи технологияларды – планшеттен бастап, дауыстық көмекшіге дейін – қауіпсіз пайдаланып, онлайн-әлемді еш алаңсыз зерттеуге көмектеседі.

Онлайн-әлем шексіз мүмкіндіктерге толы: үйден шықпай-ақ саяхаттауға, күн сайын жаңа нәрсе білуге, достармен сөйлесуге, шет тілдерін үйренуге және, әрине, ойнап, көңіл көтеруге болады.

Бірақ, шынайы өмірдегідей, виртуалды әлемде де сақ болған жөн. Цифрлық кеңістіктегі бейқамдық пен кибергигиена негіздерін білмеу үлкен қиындықтарға әкелуі мүмкін. Мысалы, планшет немесе телефонға зиянды бағдарламаны байқамай жүктеп алып, маңызды деректерді алаяқтарға жіберіп қоюың мүмкін. Немесе сүйікті ойыныңдағы барлық жетістіктеріңді, тіпті ақшаңды жоғалтып алуың мүмкін.

Виртуалды әлемдегі саяхатың қызықты әрі пайдалы болуы үшін, ал қиындықтар жолыңды кеспеуі үшін, біздің киберқауіпсіздік әліппемізді А-дан Я-ға дейін зертте. Сен жаңа технологиялармен танысып, цифрлық қауіптерден сақтануды және онлайн-алаяқтардың айласынан қалай құтылуға болатынын үйренесің.



Балалардың онлайн кеңістікті қауіпсіз зерттеуі үшін біз Kaspersky Safe Kids атты цифрлық көмекші бағдарламасын жасадық.



Аккаунт

Аккаунт — бұл веб-сайттағы немесе қызметтегі (мысалы, ойын немесе әлеуметтік желі қызметтегі) адамның жеке кабинеті. Сондай-ақ беттің белгілі бір пайдаланушыға тиесілі екенін растау үшін қажет деректер жиынтығы.

Сайттарды және интернеттегі ақпаратты аккаунтсыз (тіркелгісіз) да қарауға болады. Бірақ пайдаланушы белгілі бір сервиске өз аккаунты арқылы кірген кезде, оған жаңа мүмкіндіктер ашылады. Мысалы, достарымен хат алмасу, сатып алу жасау, музыка тыңдау, пікір қалдыру, ұсыныстар алу және тағы басқалар.



Әлеуметтік желі

Әлеуметтік желі — адамдардың интернетте бір-бірімен байланысатын, ақпарат алмасатын алаңы.

Мысалы, егер біз компьютерге: «10-ға жеткенше қайтала» десек, ол 10-ға дейін санайды. Бұл команда компьютерлерге қайталанатын тапсырмаларды жылдам орындауға көмектеседі. Мысалы, көптеген бірдей жұлдызшаларды салуға немесе бір секундта миллионға дейін санауға!

Браузер

Браузер — интернеттегі веб сайттарын қарап шығу, өңдеу және араларымен өту әрекеттерін орындауға арналған бағдарлама.

Интернетке кірмес бұрын, алдымен оның «кіру есігін» ашу керек — көп жағдайда бұл есік браузер болып табылады. Браузер сайттарды қарауға, файлдарды жүктеуге, сондай-ақ, қаралған беттер тарихын, құпиясөздерді және басқа да деректерді сақтауға мүмкіндік береді. Браузердің мүмкіндіктерін кеңейту үшін оған арнайы бағдарламалар — плагиндерді орнатуға болады. Айтпақшы, алғашқы веб-браузер 1990 жылы жасалған!



Компьютерлік Вирус

Компьютер қауіпсіздігі — компьютердегі деректерді әртүрлі кездейсоқ немесе қасақана жоюлардан қорғау.

Адам осыған ұқсас қатерлермен кездесуі мүмкін, егер ол күмәнді хабарламалардағы сілтемелерге өтсе, ойындар, фильмдер немесе басқа файлдарды тексерілмеген сайттардан жүктесе. Сондықтан интернетте әрқашан сақ болу және қай сайттарға кіріп, қай жерден файлдар жүктейтінін мұқият талдау өте маңызды. Ал ең жақсысы — қорғаныс бағдарламасын орнату: ол құрылғыны вируспен жұқтыруға жол бермейді.



Геолокация

Геолокация — әртүрлі технологияларды қолдану арқылы пайдаланушының орналасқан жерін анықтау функциясы.

Геолокацияның арқасында адам, мысалы, адасып қалған жағдайда қай жерде екенін түсінуі мүмкін. Сондай-ақ, ол дүкенге, мектепке немесе басқа қаладағы музейге жол таба алады. Алайда, сенің нақты орналасқан жерің — бұл жеке ақпарат, оны бөтен адамдарға, оның ішінде әлеуметтік желілерде, тіпті жиі баратын орындар туралы белгілер болса да, ашық жарияламаған жөн. Егер қосымша сенің геолокацияңа қолжетімділік сұраса, оның оған шын мәнінде қажет екенін ойлан. Егер қажет болмаса (мысалы, жарық шамы қосымшасы), онда мұндай қолжетімділікті бермеген дұрыс.



Ғаламтор

Ғаламтор — дүние жүзіндегі құрылғыларды байланыстыратын жаһандық желі.

Ғаламтордың арқасында кез келген уақытта қажетті ақпаратты табуға, онымен бөлісуге, достармен байланысуға, музыка тыңдауға, фильмдер көруге және басқа да қызықты нәрселер жасауға болады. Тек елестетіп көріңіз, Ғаламторға қосылған әртүрлі құрылғылар саны жер бетінде өмір сүріп жатқан адамдар санынан әлдеқайда көп! Қызықты факт: Ғаламтордағы бірінші сайт бүгінгі күні білетін күйде 1991 жылдың 6 тамызында құрылды. Айтпақшы, ол әлі де қолжетімді.



Домен

Домен — ғаламтордың иерархиялық жүйесінде бірегей атаулар кеңістігінің белгілі бір аумағы.

Ғаламторда көптеген сайттар бар! Әрқайсысының өзіндік, қайталанбас атауы — домен бар. Ол әріптер мен цифрлардан тұруы мүмкін. Сонымен қатар, әр доменнің өзінің домендік аймағы бар — бұл сайттың қай жерде жасалғанын көрсетеді. Мысалы, *kaspersky.kz* сайтының атауындағы *kz* дегеніміз — сайт Қазақстан үшін арнайы жасалғанын білдіреді.

Неліктен әр доменнің бірегей екенін білу маңызды? Себебі, қаскүнемдер жиі әртүрлі компаниялардың, мысалы, онлайн дүкендер немесе әлеуметтік желілердің сайттарына өте ұқсас парақшалар жасайды. Онда олар ақша мен құпия ақпаратты ұрлауы мүмкін, егер адамдар уақытында алаяқтықты байқамаса. Бірақ нағыз доменді жалған парақшалар үшін пайдалана алмайды. Сондықтан әрдайым домен атауын тексеріп, сайтта жеке ақпарат (оның ішінде логин мен пароль) қалдырмас бұрын, оның шынайы екенін тексеру қажет. Егер домен атауы нағыз доменнен бір әріпке де болмаса айырмашылық болса, онда осындай сайтқа ештеңе енгізбеу керек.



ДерЕкқор

Дерекқор — электронды түрде сақталатын мәліметтердің жүйелі жиынтығы.

Дереклар компьютерлерге қажетті ақпаратты есте сақтауға және жылдам табуға көмектеседі. Мысалы, кітапханада компьютерлер деректер қорын пайдаланып, сенің сүйікті кітабың қай жерде тұрғанын табады.

Операциялық Жүйе

Операциялық жүйе — компьютердің жұмысын басқаратын басты программа.

Операциялық жүйе саған ойындар ойнауға, бейнемазмұн көруге және тіпті сурет салуға көмектеседі: ол барлық нәрсенің дұрыс жұмыс істеуін бақылап тұратын көрінбейтін сиқыршы сияқты. Ол құрылғыдағы барлық бағдарламалар мен процестердің жұмыс істеу ережелері мен талаптарын анықтайды. Өртүрлі операциялық жүйелер бар, мысалы, Windows, macOS, Linux және басқалар, және әрқайсысы компьютердің жұмысын өзіне тән түрде ұйымдастырады.



Ақпараттық қауіпсіздік

Ақпараттық қауіпсіздік — ақпараттық ресурстардың, сондай-ақ ақпарат саласында жеке адамның құқықтары мен қоғам мүдделері қорғалуының жай-күйі.

Ақпараттық қауіпсіздік — бұл сенің үйіңнің есігінде тұрған құлып сияқты, бірақ телефонға, компьютерге немесе ойындарға арналған. Тіпті сен де ақпаратты қорғауға көмектесе аласың: күрделі құпиясөздер ойлап табып, оларды бөтен адамдармен бөліспе.



Жасанды И нтеллект

Жасанды интеллект — ақпарат жинақталған сайын оның функционалдығын үйрену және жақсарту сияқты адам дағдыларына еліктей алатын бағдарламалар жиынтығы.

Жасанды интеллект – бұл компьютерге үйренуге және адам сияқты ойлауға көмектесетін ақылды бағдарлама.



Йоттабайт

Йоттабайт — ақпарат көлемінің өлшем бірлігі. Бір йоттабайтта 1 000 000 000 000 000 000 000 000 (септилион) байт бар.

Компьютерлер мен басқа құрылғылар біздің деректерімізді сақтайды: фотосуреттер, бейнемазмұн, музыка, қосымшалар. Құрылғылардың жады көлемі мен файлдардың өлшемі әдетте байттарда, мегабайттарда, гигабайттарда, терабайттарда және т.б. өлшенеді. Ал йоттабайттар да болады. Бір йоттабайтта 1 000 000 000 000 000 000 000 000 (септиллион) байт бар. Елестетіп көр, осындай сақтау орнында қаншама ақпарат жүктеуге болар еді!



Куки-файлдар (cookie-файлдар)

Куки-файлдар (cookie-файлдар) — деректердің шағын бөліктері. Олардың көмегімен сайт пайдаланушының келуі туралы ақпаратты есте сақтайды.

Мысалы, адам сайтта қанша уақыт болғаны, қай интернет-ресурстан өткендігі туралы ақпарат. Олардың көмегімен сайт пайдаланушының келуіне қатысты ақпаратты есте сақтайды.



Компьютер Қауіпсіздігі

Компьютер қауіпсіздігі — компьютердегі деректерді әртүрлі кездейсоқ немесе қасақана жоюлардан қорғау.

Сенің компьютеріңді қорғау үшін күмәнді файлдарды ашпа және қорғау бағдарламаларын қолдан.



Зиянды бағдарламалардан құрылғыларды қорғауға Kaspersky Premium сияқты кешенді және сенімді қорғаныс шешімі көмектеседі.



ЛОГИН

Логин — интернетте өз аккаунтыңа кіру үшін қолданылатын пайдаланушы аты.

Логин сайтқа немесе қосымшаға адамның кім екенін «білуге» көмектеседі, осылайша ол аккаунтына кіріп (авторизациялана) алады. Логин ретінде аты, электронды пошта мекенжайы, мобильді телефон нөмірі немесе лақап аты қолданылуы мүмкін. Есіңде болсын, логин (құпиясөзіңмен бірге) құпияда сақталуы керек. Оны бөтен адамдарға айтпа, әйтпесе қаскүнемдер сенің профиліңді ұрлап кетуі мүмкін.

Машиналық оқыту

Машиналық оқыту — бұл компьютерді пайдалана отырып, тапсырмаларды шешу немесе бағдарламалар жасау тәсілі. Бұл жағдайда шешім немесе бағдарлама адамның тікелей қатысуынсыз жиналған деректер негізінде компьютер арқылы жасалады.

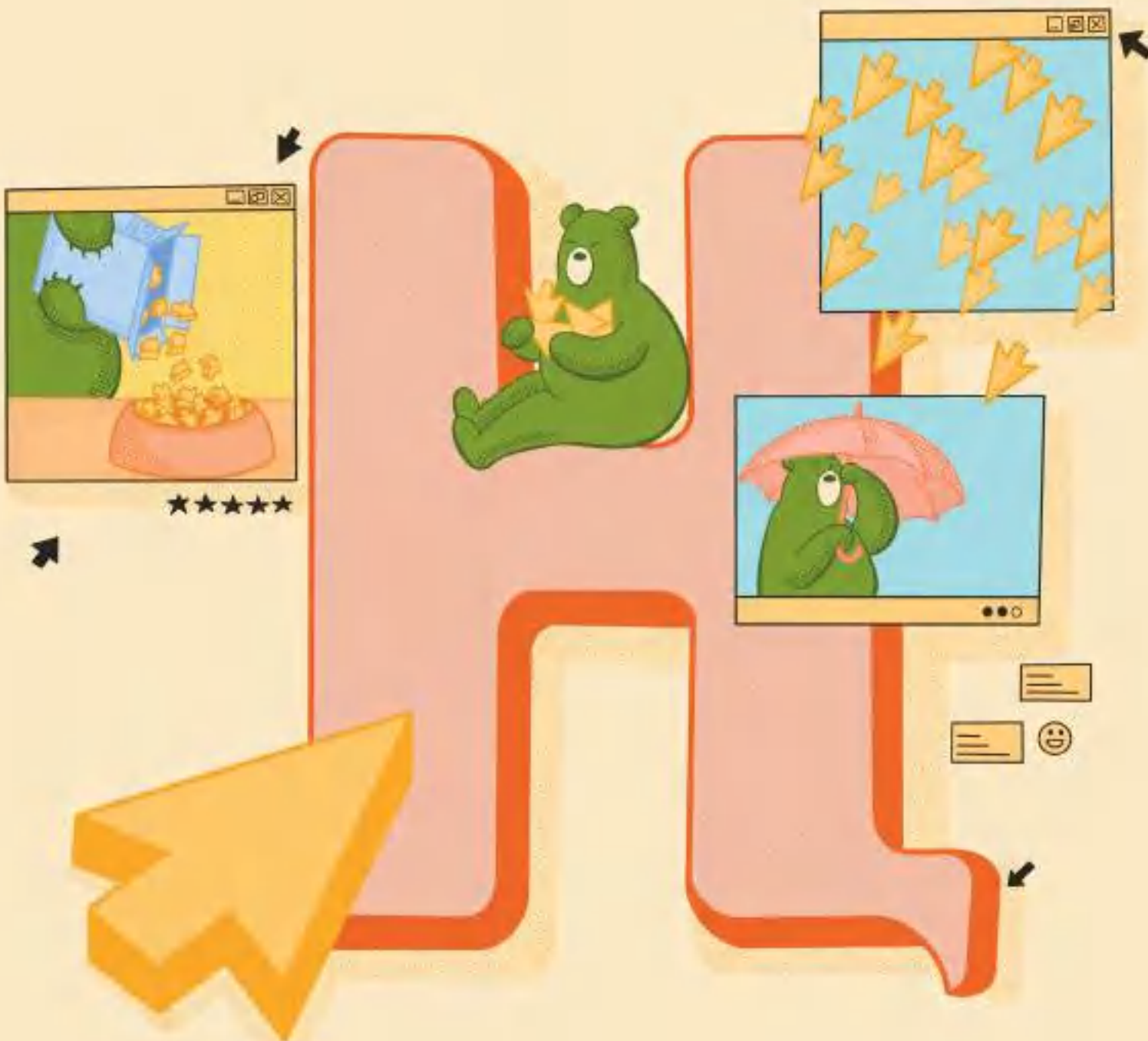
Көбінесе бағдарламалар жинақталған деректер негізінде, адамның немесе басқа бағдарламаның белгілі бір тапсырмаларды шешу мысалдары бойынша үйренеді. Мұндай оқытудан кейін бағдарламалар заңдылықтарды анықтап, адамның қойған тапсырмаларын шеше бастайды. Мысалы, «Касперский зертханасында» күн сайын шамамен 467 мың жаңа зиянды файл анықталады. Олардың 99%-ы түрлі автоматтандырылған жүйелер арқылы өңделеді, соның ішінде машиналық оқытуды қолдана отырып, яғни адамның қатысуынсыз.



Никнейм

Никнейм — пайдаланушының желідегі аты, әдетте форумдарда, ойындарда немесе чаттарда.

Онлайн-сервистерде, соның ішінде онлайн-ойындарда тіркелу кезінде никнейм ойлап табу қажет. Ойлап табылған аты бірегей болып, басқа пайдаланушылардың есімдерінен ерекшеленуі тиіс. Бұл сөз ағылшын тілінен "лақап аты" деп аударылады. Кейбір адамдар өздерінің нақты аты-жөндерін желідегі лақап аты ретінде көрсетеді. Ал басқалары ойдан шығарылған аттарды қолданады, мысалы, сүйікті мультфильмдер, фильмдер, компьютерлік ойындар немесе кітаптар кейіпкерлерінен шабыт алады — бұл дұрыс амал. Ғаламторда мүмкіндігінше аз жеке деректер қалдырған дұрыс.



Меңзер

Меңзер — бұл компьютер, планшет немесе ноутбук экранындағы көрсеткіш (әдетте жебе түрінде болады). Оның көмегімен түймелерді басуға, файлдарды ашуға, ойындарды іске қосуға және сурет салуға болады.

Назар аударыңыз: курсормен кездейсоқ нәрселерді баспау керек. Кейбір сілтемелер зиянды сайттарға апара алады немесе қауіпті файлдарды іске қоса алады.



Овершеринг – бұл желіде өзіміз туралы тым көп ақпаратты бөлісетін құбылыс.

Киберәліппе



Өріс

Өріс — деректерді сақтайтын немесе өңдейтін арнайы аймақ.

Өріс ақпаратты реттеуге көмектеседі, дәл өз достарыңды жазып отырғандай: бір бағанда — олардың есімдері, ал екіншісінде — телефон нөмірлері. Өрістерді тек белгілі бір деректерді сақтау үшін баптауға болады, мысалы, тек сандар немесе тек мәтін. Егер көптеген өрістерді бір кестеге біріктірсең, іздеуге ыңғайлы дерекқор пайда болады!



Пиксель

Пиксель — әдетте нүктеге ұқсайтын сандық кескін элементі.

Сен экраннан көретін барлық нәрсе пиксельдерден тұрады. Кез келген сурет, видео, мәтін – бәрі кішкентай нүктелердің үйлесуі арқылы жалпы бейнені қалыптастырады. Пиксельдердің саны мен өлшемі экранның ажыратымдылығын анықтайды: олардың саны неғұрлым көп болса, сурет соғұрлым анық әрі егжей-тегжейлі болады. Әдетте, пиксельді квадрат түрінде елестетеді, бірақ оның пішіні экран сипаттамалары мен оның жақтар арақатынасына байланысты аздап өзгеруі мүмкін.



Сақтық көшіРме

Сақтық көшірме — бұл пайдаланушылар жоғалтқысы келмейтін деректердің (мысалы, файлдар) көшірмесі.

Елестетіп көрші, егер жоғалған заттарды арнайы қоймадан қайтарып алу мүмкіндігің болса, қандай керемет болар еді! Құрылғыларда осындай мүмкіндік бар, оны сақтық көшіру деп атайды. Бұл – түрлі деректердің, мысалы, фото, видео және басқа файлдардың көшірмесін жасау процесі. Бұл деректерге бірдеңе болған жағдайда, мысалы, құрылғыға шифрлаушы бағдарлама жұққанда қажет болады. Мұндай бағдарламаларды қолдана отырып, киберқылмыскерлер пайдаланушылардың деректерін шифрлайды және оларды ашу үшін ақша талап етеді. Киберқауіпсіздік мамандары маңызды файлдардың сақтық көшірмесін үнемі жасап отыруды ұсынады, осылайша деректерді жоғалтудан қорғауға болады.



Спам

Спам — бұл электрондық пошта немесе жедел хабар алмасу арқылы таратылатын қажет емес хабарламалар. Спам қоңыраулар да бар.

Кейде поштаға өзің алғың келмеген жарнамалық хаттар келуі мүмкін, бірақ олар бәрібір жіберіледі. Бұл – спам. Мұндай хабарламалар мессенджерлерде де, телефон қоңыраулары түрінде де пайда болуы мүмкін.

Спам кейде қауіпті болуы мүмкін: кейбір хабарламалар алаяқтық мақсатта жіберіледі немесе ішінде фишингтік сілтеме болады. Сондықтан сақ болу маңызды – күмәнді хабарламалардағы сілтемелерге ешқашан өтпеу керек.

Егер өміріңде спамның аз болуын қаласаң, электрондық пошта мекенжайың мен телефон нөміріңді қайда қалдыратынына мән бер. Спаммен күресуге қорғаныс шешімдері, соның ішінде машиналық оқыту технологиялары көмектеседі.

Айтпақшы, «спам» терминінің ерекше шығу тарихы бар және ол бастапқыда ақпараттық технологиялармен байланысты болмаған. Бұл туралы (және басқа да қызықты нәрселер туралы) интернеттен білуге болады.



Троян вирусы

Троян вирусы — бұл нақты немесе пайдалы қолданбалар ретінде көрінетін, бірақ құрылғылар мен деректерге көп зиян келтіруі мүмкін зиянды бағдарламалар.

Трояндар, әдетте, танымал қолданбаларға ұқсап жасырынатын зиянды бағдарламалар (дәл Троя жылқысы туралы аңыздағыдай – бұл туралы ата-анаңнан сұрап көр). Алаяқтар оларды ойындар, әлеуметтік желі қосымшалары, мессенджерлер және басқа да бағдарламалар түрінде таратуы мүмкін.

Мұндай бағдарламаларды киберқылмыскерлер деректерді ұрлау немесе пайдаланушыларды аңду үшін қолданады. Троянға күмәнді сайттардан кездейсоқ тап болуың мүмкін. Егер саған әлі шықпаған ойынды тегін жүктеуді ұсынса, немесе қандай да бір бағдарламаны орнатуды талап етіп, ақшаңнан немесе деректеріңнен айырылатыныңмен қорқытса – бұл, ең ықтимал, алаяқтық.

Сондықтан тым жомарт ұсыныстарға сенбей, тек сенімді сайттарды қолданған дұрыс. Трояндардан қорғану үшін сенімді қауіпсіздік шешімдерін пайдалану, соның ішінде мобильді құрылғыларда да қорғау орнату маңызды.



БҰлтты технология

Бұлтты технология — ыңғайлы интерфейсті пайдалана отырып тұтынушыға компьютерлік желі арқылы белгілі бір ресурстарға қашықтан қатынау мүмкіндігін беретін қызмет.

Бұлттар – бұл үлкен көлемдегі ақпаратты сақтайтын арнайы серверлер, яғни қуатты компьютерлер. Олар құрылғыңдағы орынды үнемдеуге көмектеседі: барлық файлдар, ойындар мен қосымшалар бұлтта сақталады, сондықтан жад толып қалмайды. Барлық қажетті деректер осы серверлерде орналасқан, ал сен оларға қашықтан қосыласың.

Тіпті бір фотосурет телефоныңда сақталса да, «бұлт» арқылы оны компьютерден ашуға болады!



КибербУллинг

Кибербуллинг — интернетте немесе әлеуметтік желілерде басқа адамдарды қорлау, мазақтау немесе жәбірлеу.

Бұл әртүрлі жолдармен болуы мүмкін, мысалы, ренжітетін хабарламалар жіберу немесе біреу туралы жалған өсектер тарату. Кибербуллинг адамдарды көңілсіз, ұялшақ немесе қорқақ сезінуге мәжбүрлейді.

Интернетте де, шынайы өмірде де басқаларға мейірімді болу маңызды. Егер сені онлайн ренжітіп немесе қорлап жатқандай сезінсең, бұл туралы ересектермен бөліс.

Өкпелі адамның айтқаны сенің шын мәнінде қандай екенінді көрсетпейді, сондықтан олардың сөздерін жүрегіңе жақын қабылдама. Оларға дәл солай жауап қайтармауға тырыс, өйткені бұл жағдайды одан әрі ушықтыруы мүмкін. Оның орнына, сөйлесудің скриншоттарын жасап, ренжітушіні бұғаттап таста.



Түйін

Түйін — компьютерлік желінің бөлігі ретінде басқа құрылғымен қосылған құрылғы.

Түйіндер желідегі құрылғыларға бір-бірімен байланысуға көмектеседі, дәл бір үлкен команда мүшелері сияқты. Желідегі түйіндер саны көп болған сайын, ақпарат алмасу мүмкіндігі де артады. Бірақ желінің шамадан тыс жүктелмеуі маңызды!



Фишинг

Фишинг — шабуылдаушылар адамдарды алдап, адамның құпия ақпаратын немесе төлем мәліметтерін ұрлауға тырысатын онлайн-алаяқтықтың бір түрі.

Алаяқтар интернетте қауіпті сілтемелер таратады. Олар фишингтік беттерге апаруы мүмкін, онда адамның деректері ұрлануы ықтимал. Мұндай беттер әлеуметтік желілердің, онлайн-дүкендердің және басқа да таныс сайттардың көшірмесіне өте ұқсас болуы мүмкін, сондықтан оларды шынайысынан ажырату қиын.

Бірақ алаяқтар сайттың нақты атауын мекенжай жолында (URL) қолдана алмайды. Сондықтан деректерді енгізбес бұрын, сайттың домендік атауына назар аудар. Егер ол саған таныс атаудан өзгеше болса, абай болған жөн.

Қауіпсіздік шешімдеріндегі арнайы антифишингтік технологиялар пайдаланушыларды бұл қауіптен қорғайды. Егер адам жалған бетке өтпек болса, олар сайттың қауіпті екенін ескертіп, зиянды ресурстан қорғайды.



Xaker

Хакер — белгілі бір мақсаттарда компьютерлік қауіпсіздік жүйелерін айналып өту үшін өз білімі мен дағдыларын пайдаланатын адам.

Қалай ойлайсың, хакерлер мен бас киімдердің арасында қандай байланыс бар? Шын мәнінде, хакерлердің кем дегенде екі түрі бар: white hat (ақ қалпақтар) және black hat (қара қалпақтар).

Ақ қалпақтар (white hat) – бұл этикалық хакерлер, яғни компьютерлік жүйелердің қауіпсіздігін тексерумен айналысатын мамандар немесе киберқауіпсіздік саласының сарапшылары.

Қара қалпақтар (black hat) – бұл өз мақсаттары үшін қауіпсіздік жүйелерін бұзатын алаяқтар.

Көпшілік мәдениетте «хакер» сөзі көбінесе қара шляпалы хакерлерге қатысты қолданылады, бірақ шын мәнінде, хакерлердің арасында жүйелерді қорғаумен айналысатын мамандар да бар.



Жаһандық

Жаһандық — бүкіл жер шарының аумағын немесе халқын қамтитын құбылыс.

Жаһандық кибершабуылдар, мысалы, шифрлаушы бағдарламалар, өте жылдам таралып, миллиондаған пайдаланушыларға зиян тигізуі мүмкін. Халықаралық ұйымдар мен компаниялар, мысалы, «Касперский Лабораториясы», пайдаланушыларды жаһандық қауіптерден қорғау үшін бірлесіп жұмыс істейді.

Цифрлы құпиялылық

Цифрлы құпиялылық — бұл сіздің жеке және құпия ақпаратыңыздың желіде басқаларға қолжетімді болмауына құқығы.

Көп жағдайда адам өз цифрлық құпиялылығын өзі бұзады. Мысалы, жеке фотоларын, ата-анасы туралы ақпаратты, телефон нөмірін және басқа да жеке деректерін ашық қолжетімді түрде жариялаған кезде, әсіресе әлеуметтік желілерде.

Есінде ме, біз «овершеринг» (шамадан тыс ақпарат бөлісу) туралы сөйлескен едік? Егер адамның цифрлық құпиялылығы бұзылса және оның деректері бөгде адамдарға қолжетімді болып қалса, бұл ақпаратты алаяқтар өз мақсаттарына пайдалануы мүмкін.

Қазір өзіңнің әлеуметтік желідегі парақшаңа мұқият қарашы (егер бар болса): онда қандай ақпарат жарияланған? Бұл деректерді бейтаныс адамдардың білуін қалайсың ба?



Чат-бот

Чатбот — бұл пайдаланушымен «байланысатын» және оның сұрақтарына жауап беретін бағдарлама.

Сайттарда көмек ұсынатын қалқымалы терезені байқап көрдің бе? Бәлкім, бұл чат-бот болған шығар!

Әрине, бұл кәдімгі адаммен сөйлесу емес. Мұндай бағдарлама тек алдын ала орнатылған сценарийлерге жауап береді. Мысалы, егер адам интернет-дүкен сайтында тапсырыс нөмірін енгізсе, чат-бот жеткізу мәртебесін анықтауға көмектеседі.

Чат-боттар сұрақтарға жылдам жауап беру немесе мәселені шешу үшін пайдалы. Бірақ одан да күрделі міндеттерді орындай алатын басқа да цифрлық көмекшілер бар.

Соңғы кезде «нейрожелілер негізінде жұмыс істейтін ақылды чат-боттар» көп қызығушылық тудыруда. Олар интернеттен үлкен көлемдегі ақпаратты өңдей алады және адаммен хат алмасу сияқты сөйлесуді имитациялайды. Бірақ мұндай чат-боттармен абай болу қажет: олар кейде фактілерді шатастырып, даталарды қате беруі немесе дұрыс емес кеңес ұсынуы мүмкін.



Шифрлеу

Шифрлеу – деректерді (мысалы, біз түсінуге болатын мәтінді) бір қарағанда кездейсоқ және мағынасыз таңбалар жиынына (шифр) түрлендіру процесі.

Адамдар деректерді шифрлағанда, оларды тек белгілі бір пайдаланушылар ғана оқи алатындай етіп түрлендіргісі келеді – яғни, шифрды ашуға арналған кілт немесе дешифратор бар адамдар.

Арнайы кілтсіз шифрланған ақпаратты бастапқы түсінікті мәтінге айналдыру дерлік мүмкін емес.

Көптеген сайттар мен қосымшалар біздің деректерімізді қорғау үшін шифрлау құралдарын пайдаланады.

Көптеген мессенджерлерде қатардан-қатарға шифрлау немесе ұштан-ұшқа шифрлау (ағылш. end-to-end encryption) қолданылады. Бұл дегеніміз, хат алмасу тек қолданушылардың құрылғыларында шифрдан ашылады, ал оны үшінші тараптар оқи алмайды.



КиберсыЩик (Кибертыңшы)

Кибертыңшы — желіде жасалған киберқылмыстарды тергеумен айналысатын маман.

Ол ұрланған мәліметтерді табуға, зиянды бағдарламаларды анықтауға және кімнің кибершабуыл жасағанын білуге көмектеседі. Кибертыңшылар — цифрлық әлемнің қорғаушылары!



Дизъюнкция

Дизъюнкция — бастапқы екі пікір жалған болғанда ғана жалған болатын логикалық операция. Дизъюнкцияны кейде «Логикалық қосу», «Логикалық НЕМЕСЕ» деп те атайды.

Компьютерлер осындай логикалық операцияларды қолданып, әртүрлі нұсқаларды тексеріп, шешім қабылдайды. Олар үшін басты ереже: егер кем дегенде бір шарт орындалса, белгілі бір әрекетті орындауға болады.

Мысалы, сен ойын ойнап жатырсың. Есіктен өту үшін:

- Кілт табу немесе жұмбақты шешу керек.

Компьютер келесі тексерісті жүргізеді:

- Егер сенде кілт бар болса – есік ашылады.
- Егер сен жұмбақты шешсең – есік те ашылады.
- Егер сенде кілт жоқ және жұмбақты шешпесең – есік жабық күйінде қалады.

Осылайша, дизъюнкция (логикалық «немесе») компьютерге бірнеше нұсқаның ішінен дұрыс әрекетті таңдауға мүмкіндік береді.



Электронды қолтаңба

Электронды қолтаңба — бұл кәдімгі қағаздағы қолтаңба сияқты, бірақ цифрлық форматта. Ол құжаттың шын мәнінде саған тиесілі екенін және ешкім оны өзгертпегенін дәлелдейді.

Электронды қолтаңба онлайн-құжаттарды қағазға басып шығармай-ақ қол қою үшін жиі қолданылады. Ең бастысы – компьютерлік технологиялардың арқасында мұндай қолтаңбаны бұрынғыдай оңай қолдан жасау мүмкін емес!



Гиперсілтеме

Гиперсілтеме — басқан кезде белгілі бір веб-ресурсты ашатын элемент (мәтін, белгіше).

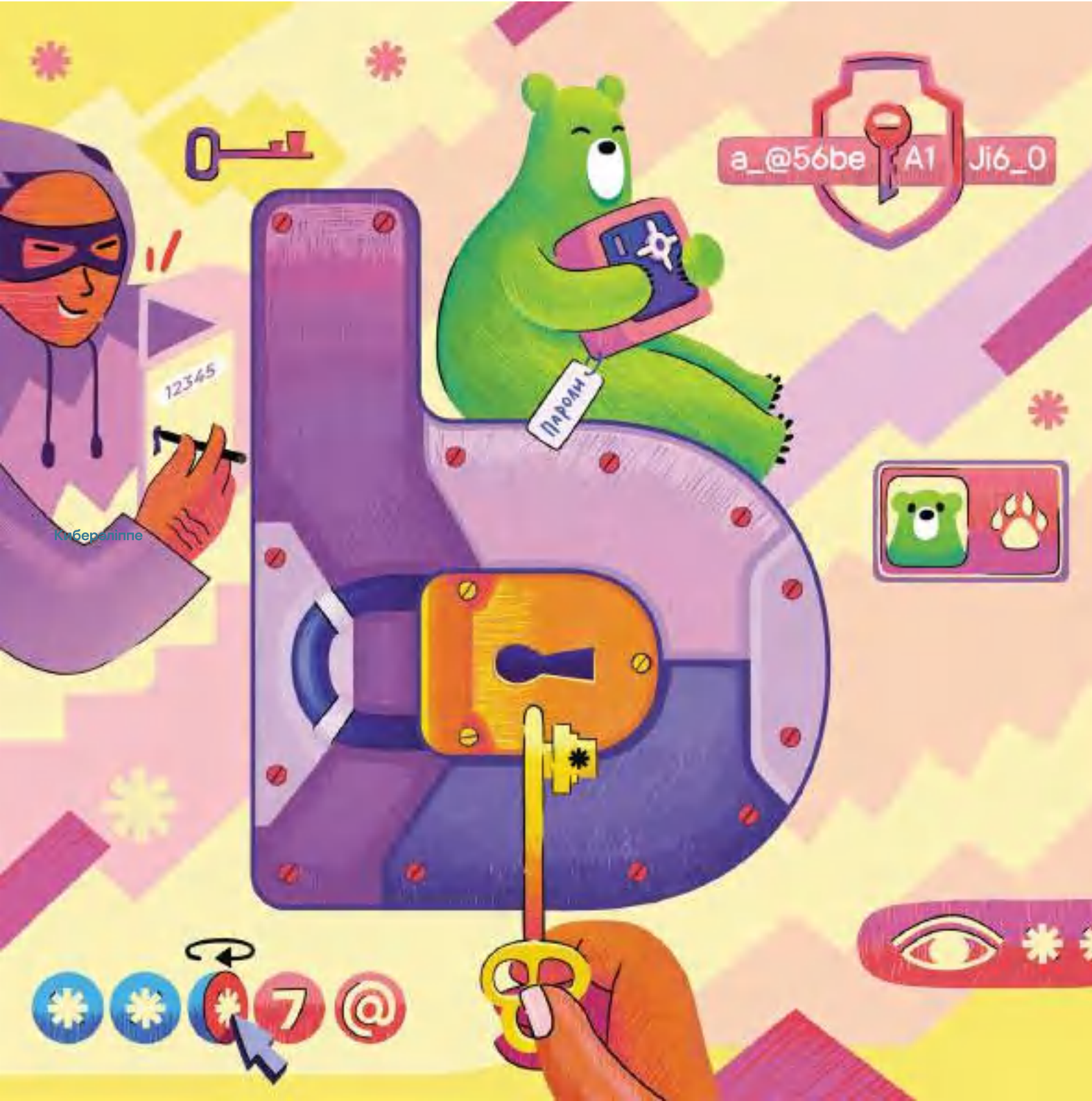
Гиперсілтемелер сені интернеттегі қажетті бетке немесе құжат ішіндегі басқа бөлімге тез алып барады, сондай-ақ файлдарды жүктеуге мүмкіндік береді.

Олар портал сияқты жұмыс істейді:

- Көк түспен астын сызған мәтін,
- Батырма,
- Сурет түрінде көрінуі мүмкін.

Абай бол! Егер саған мессенджерде немесе электрондық поштамен белгісіз біреу сілтеме жіберсе, бірден баспай тұра тұру керек – ол қауіпті болуы мүмкін.

- Кейбір гиперсілтемелер «бұзылған» (өлі сілтемелер) болып шығады. Бұл сілтемелер жойылған файлға немесе интернетте жоқ бетке апаруы мүмкін.



Паролъ

Пароль — аккаунтқа кіру үшін пайдаланылатын таңбалар (әріптер, сандар және арнайы таңбалар) жиынтығы.



Электрондық пошта

Электрондық пошта — бұл хаттарды, фотосуреттерді және басқа файлдарды жіберуге және алуға мүмкіндік беретін технология мен қызметтер.

Қазіргі уақытта электрондық пошта қарым-қатынастың ажырамас бөлігіне айналды. Оның көмегімен адамдар әлемнің кез келген нүктесінен хат алмасады.

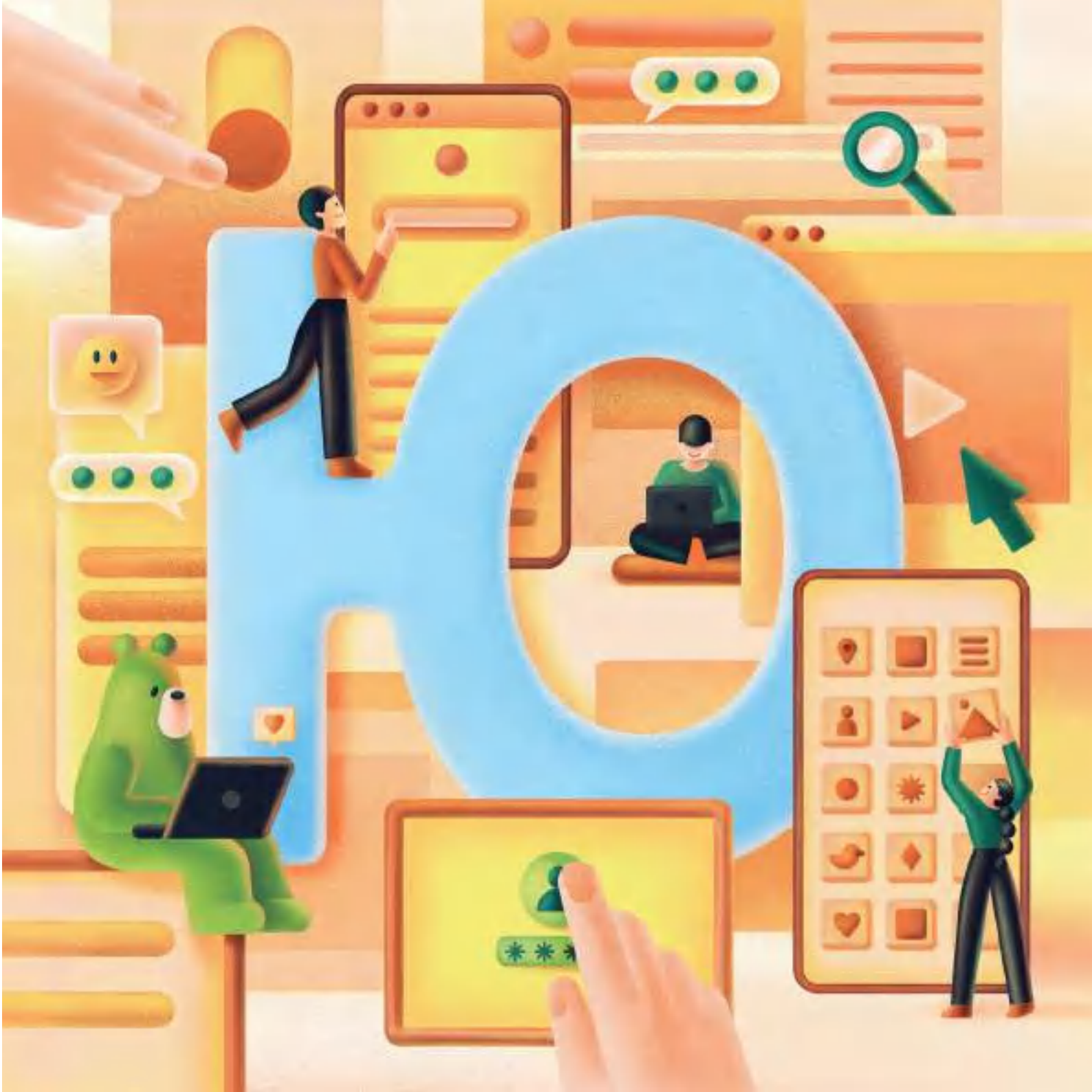
Электрондық поштаның мүмкіндіктері.

Оқу мен жұмысқа пайдаланылады – мұғалімдер тапсырмалар мен материалдар жібереді.

Әртүрлі сервистерге тіркелу үшін қажет – әлеуметтік желілерде, білім беру және ойын платформаларында логин ретінде қолданылады.

Файлдармен алмасу – мәтіндер, суреттер, құжаттар жіберуге болады.

Бірақ пошта арқылы үлкен файлдарды жіберу мүмкін емес – көптеген пошта сервистерінде файл өлшеміне шектеу бар. Мұндай жағдайда файлды бұлтты сақтау орнына немесе флешкаға жүктеп, сілтемесін жіберген дұрыс.



Юзер

Юзер — компьютердің, смартфонның немесе басқа құрылғының пайдаланушысы.

«Юзер» сөзі ағылшын тілінен аударғанда «пайдаланушы» дегенді білдіреді.

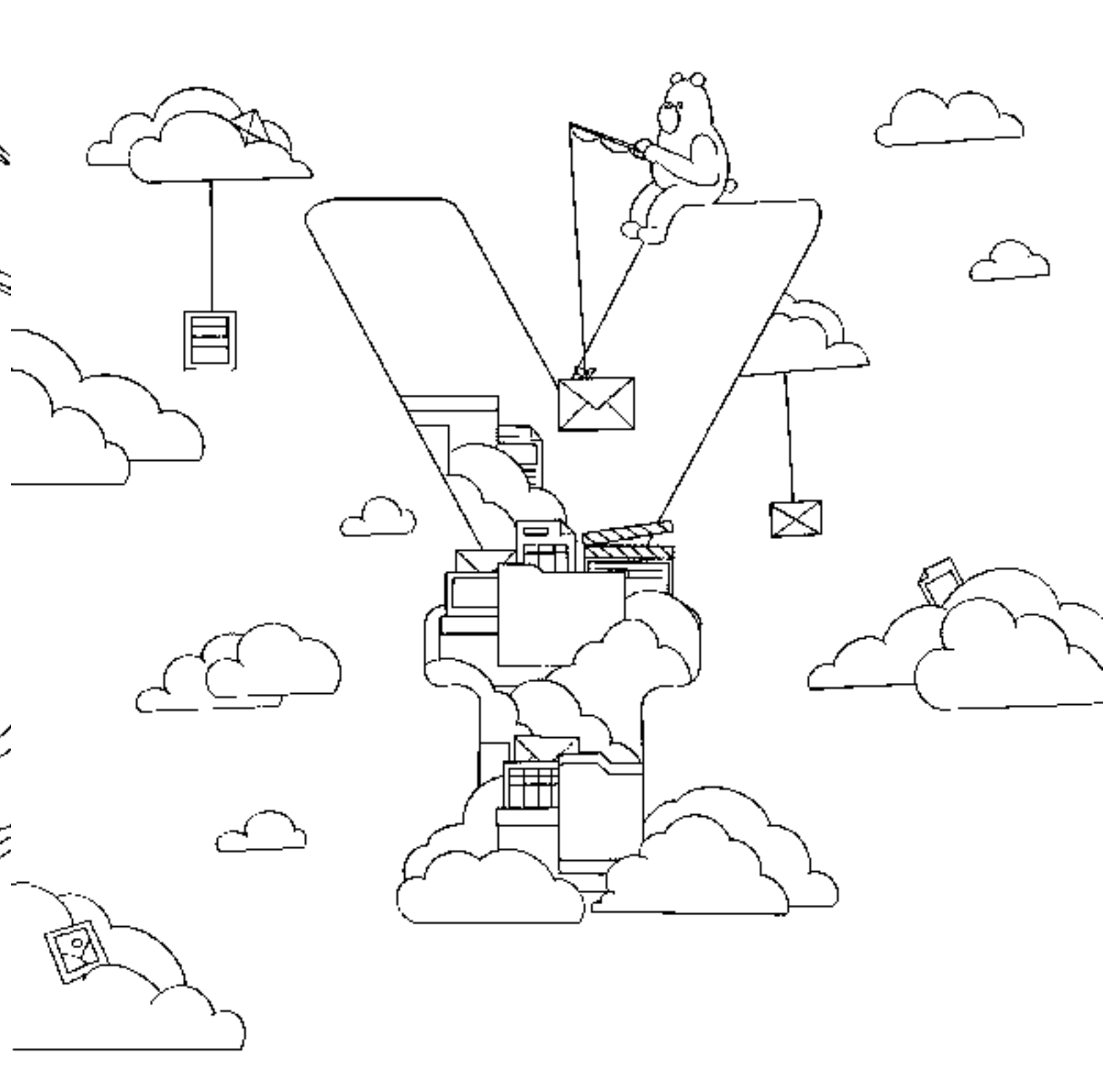
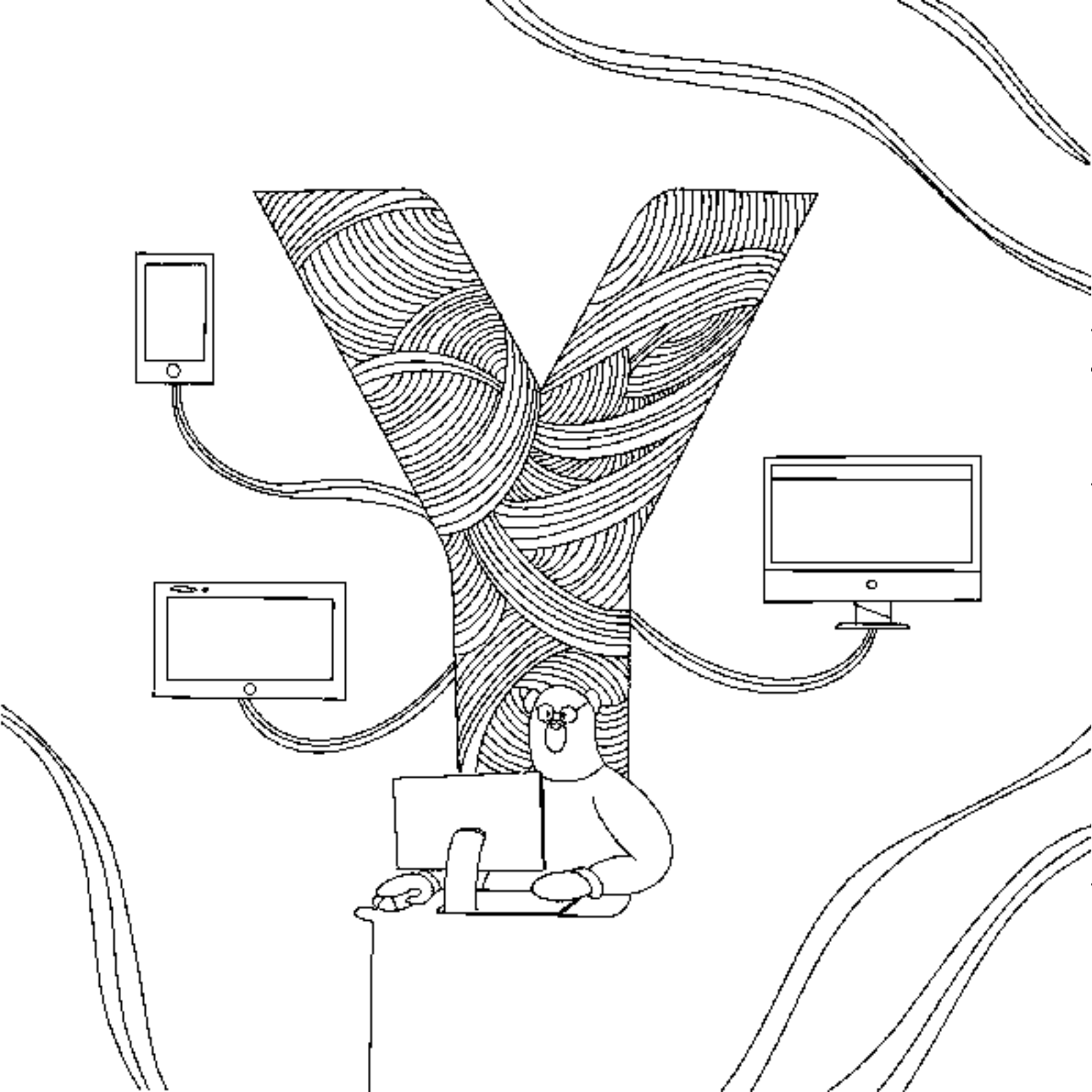
Егер сен гаджеттерді қолдана алсаң – оларды қосып-өшіруді, хабарлама жіберуді, интернеттен ақпарат іздеуді білсең, сен юзерсің!

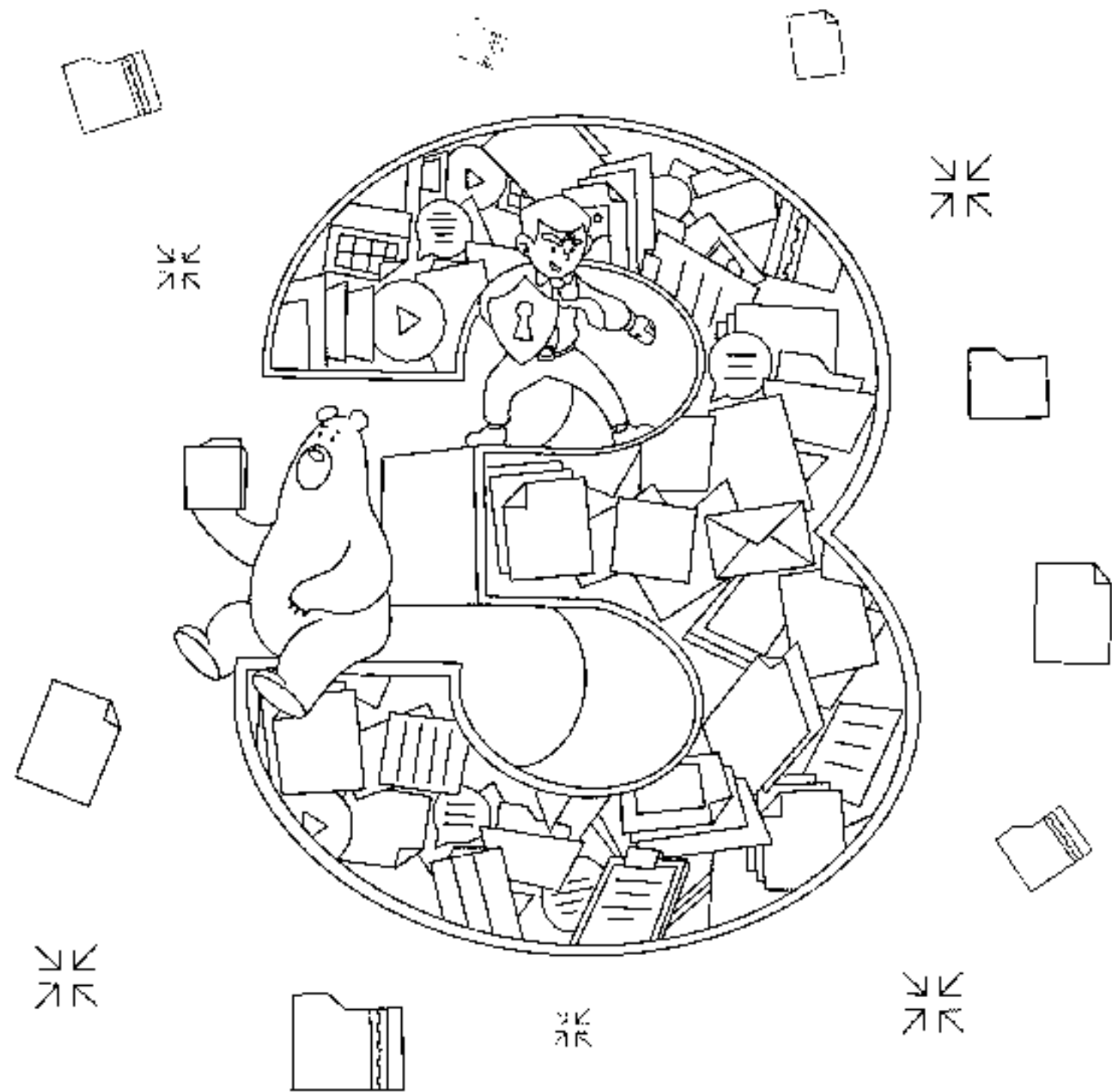
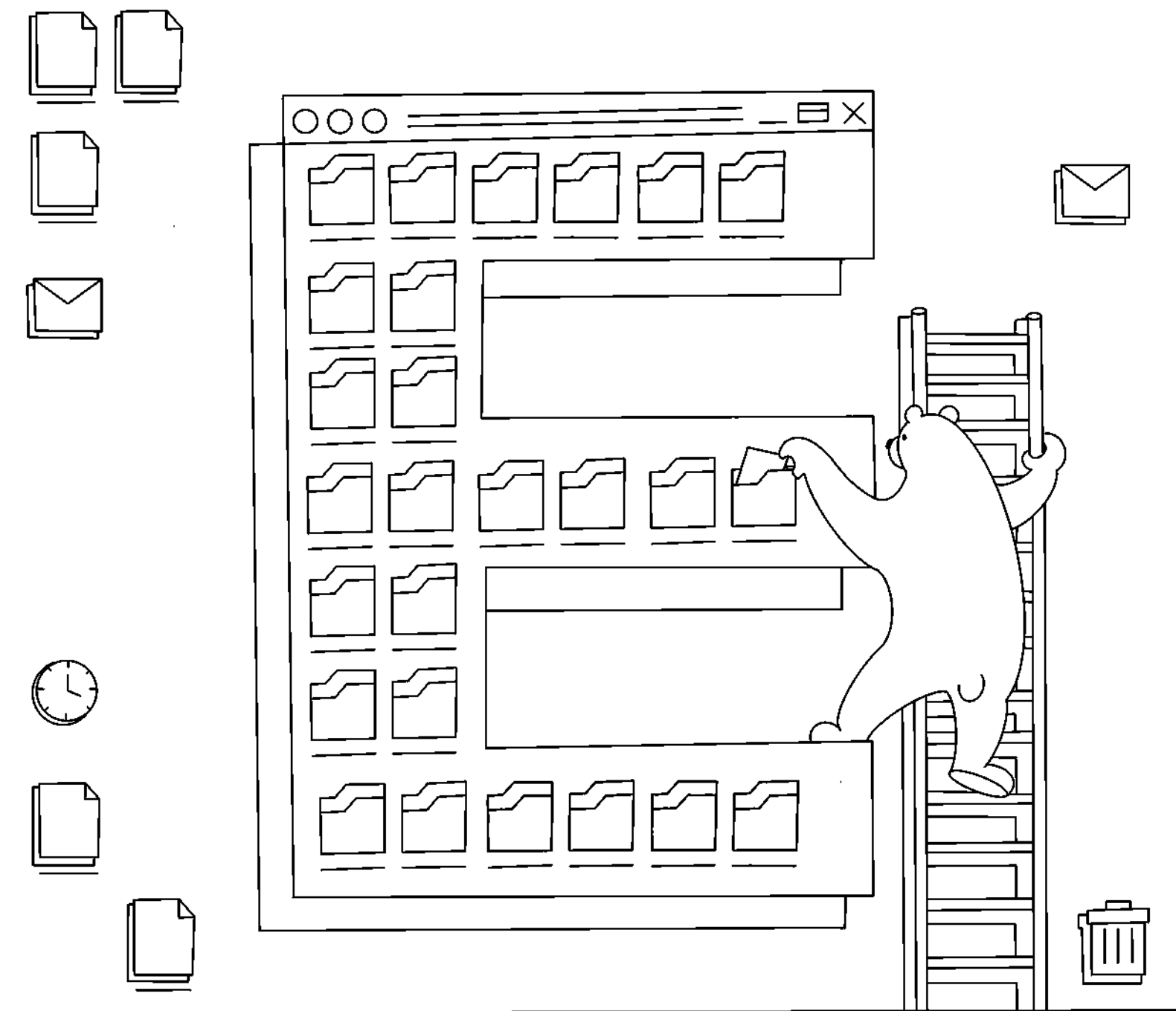


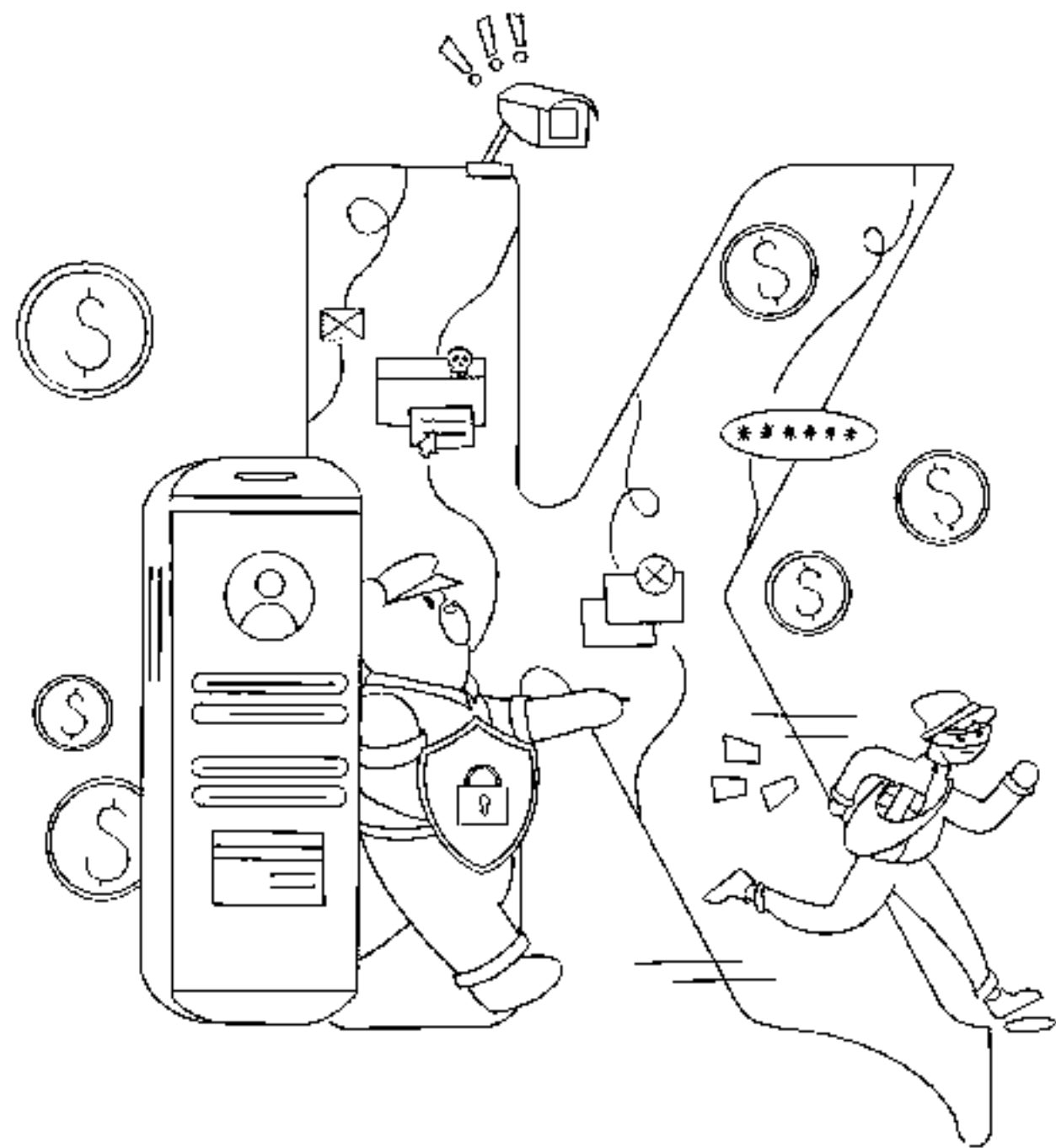
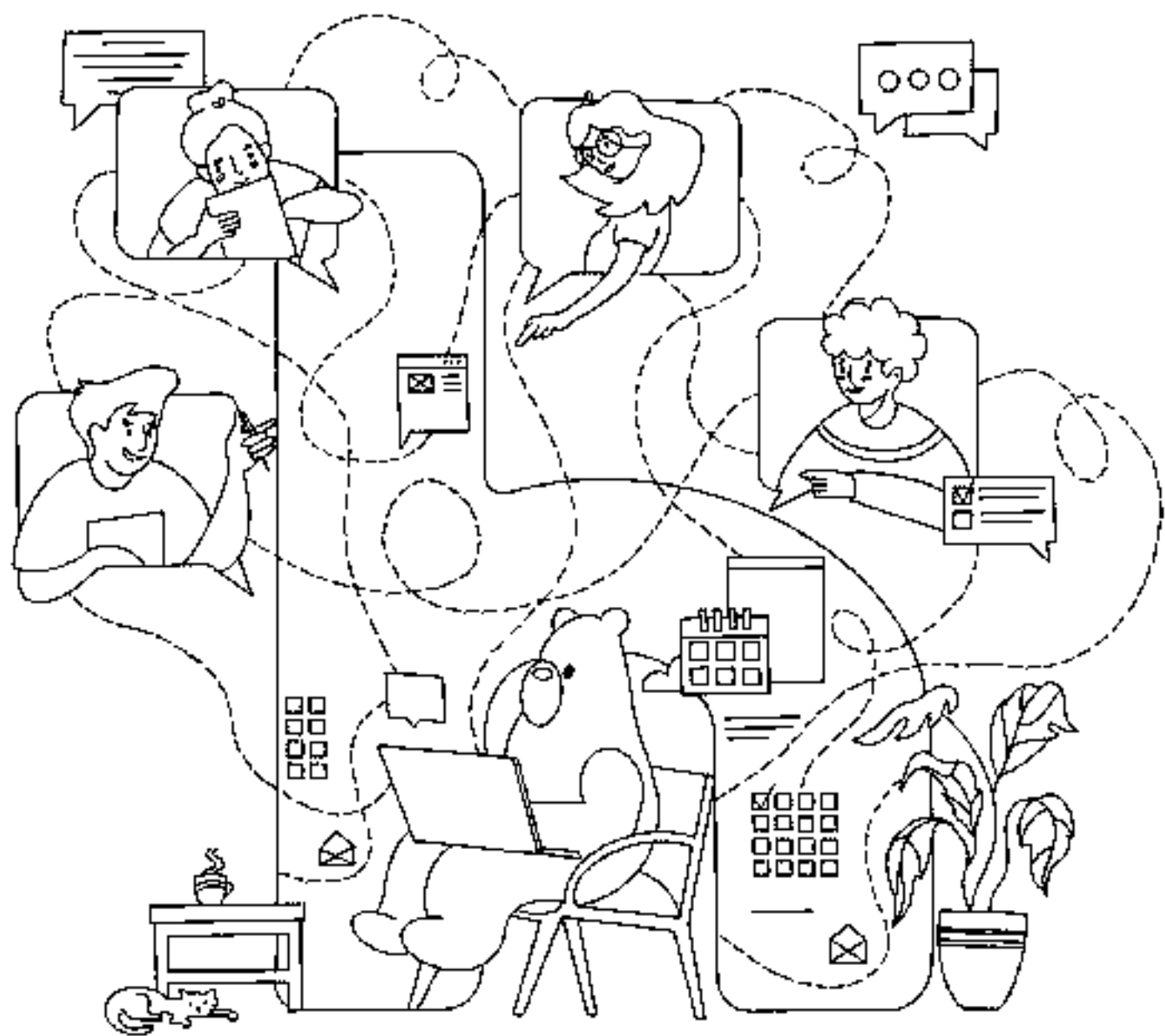
АутентификацияЯ

Аутентификация — қатынасатын субъект пен оның идентификаторының сәйкестігін тексеру әрі растау операциясы.

Бұл есіктегі құлып сияқты: тек кілті (құпия сөз немесе саусақ ізі) бар адам ғана кіре алады. Аутентификация деректерді бөгде адамдардан қорғауға және интернеттегі қауіпсіздікті қамтамасыз етуге көмектеседі.







Ескертпелер



Құрметті киберзерттеуші!

Бұл ерекше әліппені оқып, жаңа дүниелермен танысу саған қызықты болды деп үміттенеміз. Алда сені әлі талай жаңалық күтіп тұр, өйткені сенің цифрлық әлемдегі шытырман оқиғаларың енді ғана басталды!

Сұрақ қой, үлкендерден түсінбеген нәрселерді сұра, әліппені достарыңмен бірге оқы және оны ата-анаңмен қайта қарап шық. Ең бастысы, цифрлық қауіпсіздік ережелерін есте сақта:

- Өзің, отбасың және достарың туралы ақпаратты интернетте тым көп бөліспе.
- Қиын, ұзын және бірегей құпиясөздер ойлап тап, олардың ішінде сандар, әріптер және арнайы таңбалар болсын.
- Қосымшаларды тек ресми сайттардан немесе ресми қолданба дүкендерінен жүктеп ал.
- Хабарламадағы сілтемеге өтпес бұрын жақсылап ойлан – тіпті ол жерде бір нәрсе қызықты деп уәде берсе де.