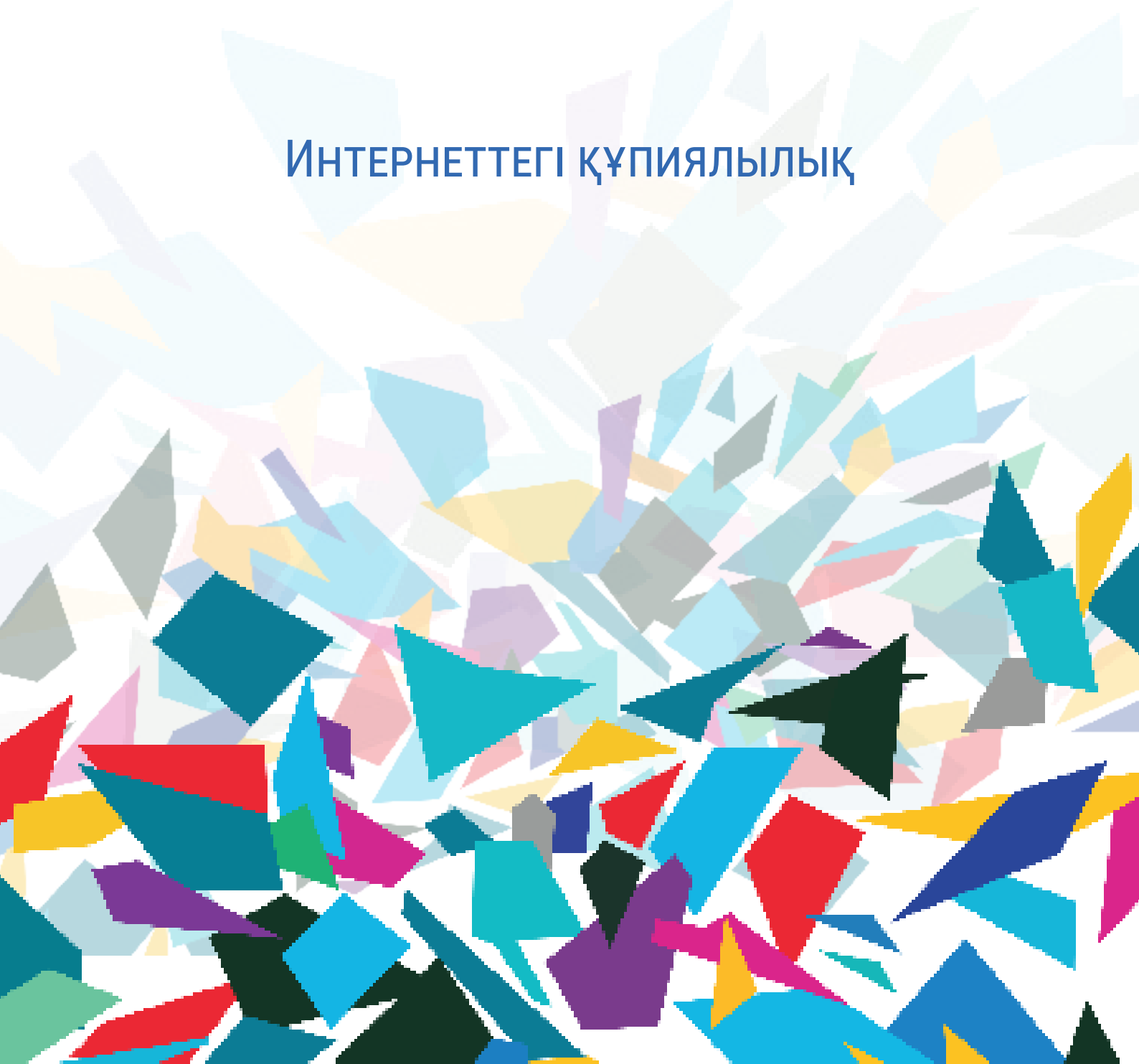
17-дәріс

ҚАЗАҚСТАННЫҢ АШЫҚ УНИВЕРСИТЕТІ

ИНТЕРНЕТ ПСИХОЛОГИЯСЫ

Интернеттегі құпиялылық



Интернетте жеке өмір құпиялығын қамтамасыз ету мәселелері шынайы өмірдегіден де өзекті. Қазіргі таңда жалпыға ортақ байланыс желілері арқылы құралдарды қосуға арналған хаттама болатын Интернет адамзат бір кездері бетпе-бет келген жеке өмірдің интернет-құпиялығының жаһандық қатері болып табылады. Интернет ақпарат алмасуды айтарлықтай жеңілдетеді, бірақ жіберілетін ақпаратқа, ол жіберілетін байланыс жүйелеріне әр секунд сайын бұзу, мәліметтерді ұрлау немесе басқа да шығын қатерлері төнеді. Интернет жалпыға ортақ желі болғандықтан, кез келген қолданушы оны кез келген мақсатта қолдана алады және өкінішке орай, көп жағдайда қаскүнемдер мен айлакерлер оны белсенді түрде пайдаланады.

Адамдар Интернетте тек өздері ғана емес, сонымен қатар басқа да адамдар жайлы да құпия ақпарат қуана-қуана береді. Физикалық арақашықтық, сондай-ақ көптеген интернет-сайттардағы анонимділікті жоғары қабылдау Интернеттегі құпиялық бізді ендігәрі толғандырмайды деп ойлауға мәжбүрлейтін тәртіптің дамуына алып келеді.

2007 жылы, мысалы, Facebook қолданушылар «қорқынышты» деп аталған қызметті іске қосты, ол қолданушылардың басқа сайттардағы әрекеттерін аңдып, содан кейін оны өз достарына жіберіп отырған. Facebook бұл тәжірибеден бас тартты, бірақ кейін 2010 жылы компания қолданушылардың құпиялық параметріне үнсіздік бойынша «барлығы» мәнін орнату жайлы шешім қабылдады. Бұл тек «достарының» ғана емес, кез келген адамның сайтын көруге болатындығын білдіреді. Facebook жеке ақпарат құпиялығына қатысты наразылықтар мен сот процестерін тудыруды жалғастыруда.

Соған қарамастан, адамдар хабарлама жіберуді тоқтатқан жоқ. Олар өздері онша танымайтын «дос» адамдарды қолдайды. Миссури штаты Университетінің студенті адамдардың «достарды» қосуға қаншалықты дайын екендігін көрсететін сынақ жүргізді. Ол досы ретінде қосуды сұрайтын сұраныс құрастыратын компьютерлік бағдарлама құрып, оны 250 000 адамға жіберді. Шамамен олардың үштен бірі оның кім екенін білмесе де, сұранысты қабылдаған. Facebook-тің көптеген қолданушылары мұның тәжірибе екенін байқап, оған жеккөрінішті және әдепсіз хабарламалар жазған. Алайда оның нәтижелері адамдардың көпшілігінің өз «достарының» тізімін қалай толтыратындығын көрсетті.

Құпиялық парадоксі адамдар аталған мәселенің өздерін алаңдататындығы жайлы айтуында болып табылады; сонымен қатар, олар өз құпиялық параметрлерін қалай баптау жайлы білмейді.

Адамдар толық, жеке ақпаратты көпшілікке ашып салады. Шынында да, «бірігіп пайдалану» Web 2.0-нің негізгі құрауышы болып табылады, ал оны жеңілдету үшін бағдарламалық құралдар құру — үлкен бизнес. Мысалы, зерттеулердің бірінде сауалнама жүргізілген колледж студенттерінің ішінде олардың тек жартысы ғана өз профильдерін әдетте жеке және құпия ақпаратты қамтитын деректерді «тек достар» ғана көре алатындай етіп шектегенін айтқан. Бір қарағанда бұл дұрыс қадам болып көрінуі мүмкін. Бірақ Миссури университетіндегі тәжірибе көрсеткендей, қанша Facebook қолданушысының өздері танымайтын адамдарды желісіне «дос» етіп қосқаны жайлы ойланып көріңізші.

Бұл парадокс нені білдіреді? Мүмкіндіктердің бірі адамдардың көбісі белгілі бір білімге ие болса да, Интернеттегі өз құпиялығын қалай басқаруды шын мәнінде білмейтіндігі болып табылады. Құпиялық баптаулары күрделене түсуде, ал компаниялар әрдайым саясатты өзгертіп отырады. Саясаттың өзі оқуға қызықсыз, оны түсіндіру қиын және әдетте кез келген жағдайда қолданылмайды.

Шын мәнінде, бір зерттеу жұмысы адамдардың көбісі өздеріне қарағанда басқа адамдар құпиялық қатерлері үшін осал келеді деп есептейтіндігін растады. Кореядағы ұлттық таңдама сауалнамасында негізгі екі сұрақ қойылған. Олардың бірі: «Сіздің жеке онлайн-ақпаратты дұрыс пайдаланбау құрбаны болуыңыз қаншалықты ықтимал?». Жалпы алғанда адамдар олардың ойынша басқалар, әсіресе олар жасөспірімдер болса, қабылдаған қатерлерге қарағанда өз қатерлеріне оптимистік түрде қараған.

Парадоксты түсіндірудің үшінші мүмкіндігі әлеуметтік желінің құпиялықты психологиялық тұрғыда да, технологиялық тұрғыда да қамтамасыз етудің аса қауіпті онлайн-ортасы екендігі болып табылады. Адамдар олар өздері шақырған аудиториямен — негізінен «достарымен» шектелеміз деп ойлайды. Олар өздері жайлы жалпы деректерді ашуы мүмкін, бірақ олар өздерінің әлеуметтік желідегі парақшасын жеке орта деп есептейді және құпия ақпаратпен бөлісуде өздерін еркін сезінеді. Бұл қарым-қатынас орнату мен оны дамытудың негізі болады.

Адам желісі өскен сайын құпиялық қатері де артады.

Құпиялық Интернеттің ашық ақпараттық кеңістігінің маңызды элементі болып табылады. Адамның құпиялық құқығын, атап айтсақ, жеке ақпарат құрамы мен оның таралу деңгейін бақылау құқығын ескермеу қолданушы сенімінің жоғалуына, бақылаудың күшеюіне және нәтижесінде ақпарат алмасудың инновативтігінің, қарқындылығының және көлемінің азаюына алып келеді.

Сондықтан құпиялық және ашықтық, қолдану ыңғайлылығы және жеке ақпараттың таралуы арасындағы күрделі тепе-теңдікті ұстап тұру аса маңызды болады. Қолданушылар мұны өздері де браузер немесе әлеуметтік желіні орнату арқылы белгілі бір дәрежеде орындай алады. Мысалы, сұраныстағы Referer тақырыпшасын бұғаттау немесе үшінші тарап сайттарынан cookie қабылдауға тыйым салу. Алайда аталған шаралардың тиімділігі төмен. Мысалы, қазіргі таңда кіріп отырған сайттың cookie-нен бас тарту функционалдықты айтарлықтай жоғалтусыз мүмкін емес деуге болады.

Бұл мәселені шешуге сайттар мен әлеуметтік желілердің құрастырушылары үлкен үлес қоса алады. Мысалы, үшінші тарапқа жіберілетін ақпарат көлемін барынша азайту немесе қолданушыларды олардың әлеуметтік желідегі ақпараттарының ашықтығы жайлы хабарландыру арқылы. Мұны Facebook-тің 2007 жылғы қарашада желінің барлық қолдану-шылары автоматты түрде жазылған Beacon атты қызметімен болғандай сот үдерісіне дейін жеткізбей орындау керек. Beacon арқасында қолданушылардың достары басқа кей сайттардағы соңғы іс-әрекеттері, мысалы, Fandango (http://www.fandango.com/) сайтында киноға билет алу, жайлы хабарлама алған. Іс екі жылдан кейін қызметтің толықтай тоқтауымен және Facebook-тің онлайн құпиялық саласындағы жұмыстарға арналған 9,5 миллион долларлық қор құруымен аяқталды.

Бұл мәселелерді білу және талқылау — оларды шешуге жасалған қадам. Мәселелер шынымен де шешіледі: қолданушылар әлеуметтік желіде үлкен қолдауға ие болады, браузерлер біздің қауіпсіздігіміз бен құпиялығымызға қамқор болады. Себебі адамдар ештеңеге қарамастан өз достарымен, таныстарымен, кейде бүкіл әлеммен ақпарат алмасқысы келеді.

Он жыл бұрын онлайн төлем жүргізу қатерлі іс болып саналып, аса мұқият орындалатын. Желіде әлеуметтік қарым-қатынас кезінде шын атты пайдаланудың мәні жоқ, ал Интернет қызметінің анонимділігі абсолютті болып есептелетін.

Әлеуметтік желілер бұл жағдайды түбегейлі өзгертті. Біз әлеуметтік желілерде бейтаныс немесе виртуалды кейіпкерлермен емес, өзіміз танитын немесе танысқымыз келетін адамдармен араласқымыз келеді. Бұл біздің желідегі бейнеміздің шынайы екендігін білдіреді.

Біз өз достарымызбен, таныстарымызбен, кейде бүкіл әлеммен өз жасымыз, қызығушылықтарымыз, мекенжайымыз, ағымдағы жұмыстарымыз, барлығы жайлы шынайы ақпаратпен бөлісеміз. Мысалы, мен жақында газеттен жасалған сауда жайлы ақпарат алмасуға мүмкіндік беретін Blippy сайты жайлы оқыдым. Қандай да бір Марк бүкіл әлемге iPad-қа арналған кейсті $41 сатып алғаны, Х мейрамханасында $24 жұмсағаны және мұрнына ота жасату үшін Флоридадағы пластикалық хирургия клиникасында $6450 жұмсағаны жайлы жария етеді. Сирек жағдай ма? Олай емес сияқты. Күн сайынғы әртүрлі ақпараттармен алмасуға арналған сайттар мен олардың артында тұрған әлеуметтік желілер жаңбырдан кейінгі саңырауқұлақтай қаптау үстінде және олар аса танымалдылыққа ие.

Бір қарағанда, мысалы Сіздің сүйікті істеріңіз, жеке суретіңіз немесе Сіз бітірген мектеп нөмірі жайлы жеке болса да, зиянсыз ақпаратты Интернетте жариялау қауіпсіз болып көрінуі мүмкін. Бірақ PleaseRobMe.com сайты әлеуметтік желілердегі ақпаратты зиянды мақсаттарда қалай пайдалануға болатындығын көрсетті. Бұл сайт желідегі қолжетімді ақпаратты қожайындары басқа жақта болған бос пәтерлерді табу үшін пайдаланған.

Басқа тұсы Сіздің жеке ақпаратыңыздың таралу аймағы Сіз ойлағаннан да ауқымды болуы мүмкін екендігі болып табылады. Ол әдетте достар мен таныстар ортасымен шектелмей, арқашан Сіздің әлеуметтік желіңіздің шегінен шығып кетіп жатады. Бұл, өз кезегінде, Сіздің өзіңіз қалаған жағдайларда анонимді түрде қалу мүмкіндіктеріңізді айтарлықтай шектеуі мүмкін.

1993 жылы бір журналда бірі екіншісіне: «Интернетте сенің ит екеніңді ешкім білмейді» деп айтатын компьютер дисплейінің алдында отырған екі ит бейнеленген келемеж сурет жарияланды. Бүгінгі шынайылық аталған суреттен қатты ерекшеленеді.

Бұл мәселені толығырақ қарастырып көрейік.

«Жалпы Интернетті пайдалану қаншалықты құпиялы?» деген сұрақтан бастайық. Бір қарағанда Интернетті пайдалану толық анонимді болып көрінеді. Әрине, сіз кірген веб-сайт компьютеріңіздің IP-адресін біледі, ол не істей алады? Жеке сайт және жалпылама мекенжай. Алаңдайтын себеп жоқ сияқты.

Алайда, көпшілік болмаса, біраз веб-сайттар кірген адамдарды аңдудың қандай да бір технологияларын пайдаланады. Тіпті егер бұл қолданушы аты мен құпиясөзі болатын портал болмаса да, Сіз сайтқа әр кірген сайын (қазіргі таңда мұны Интернеттегі жұмыс сөзінің синонимі деуге болады) сайт қонағы, яғни Сіз жайлы жеке ақпарат «жайылады». Мысалы, 1 пиксель сурет түріндегі кірістірілген «қоңыздар», cookies немесе JavaScript қосымшалары танымал технологиялар болып табылады.

Жеке ақпараттың жайылуы Сіз кірген веб-сайтта ғана емес, сонымен қатар, үшінші тарап сайттарында да орындалады. Бұл сайттар, әдетте, анық болмаса да, қаралып отырған веб-парақшада, мысалы, жарнамалық фрагменттер түрінде болады. Қарапайым сценарий, мысалы Google's Adsense, Yahoo! сияқты жарнамалық провайдерлердің сайт иесінің келісімімен жарнамалық хабарландырулар орналастыруы болып табылады. Әдетте бұл фрагменттер JavaScript құрауыштары немесе жай ғана графикалық сурет түрінде болады. Заманауи ақпараттық веб-сайттың парақшасын бейнелеу түрлі элементтерге, соның ішінде үшінші тарап сайттарына ондаған сілтеме жасауды қамтиды. Мұның қолданушы баннерді басса да, баспаса да орындалатындығын айта кету керек.

2014 жылдың қаңтарында кибержурналист Джозеф Стейнберг Forbes журналына Интернетпен байланысты, бізді өз үйіміздің ішінде-ақ «аңдитын» құралдар тізімін жариялаған. Бұл заттар Интернеті.

Заттар Интернеті (ағылшынша Internet of Things, IoT) — бір-бірімен немесе желілердің ұйымдастырылуын адамның қатысу қажеттелігі әрекеттері мен операцияларын ескермейтін, экономикалық және қоғамдық процестерді қайта құра алатын құбылыс ретінде қарастыратын сыртқы ортамен өзара байланысуға арналған кірістірілген технологиялармен жабдықталған физикалық нәрселердің («заттардың») есептеуіш желісінің тұжырымы.

Заттар Интернеті енді басталса да, өте жылдам дамып келеді және барлық енгізілетін жаңалықтар ақпараттық қауіпсіздікке қатысты маңызды мәселелерді қосып отырады. Business Insidero жаңалықтар веб-сайты 2013 жылы сұхбаткерлер үшін заттар интернеті технологияларын енгізу кезіндегі ең үлкен мәселенің қауіпсіздікке күмәндану екендігін көрсететін зерттеу жұмысын жариялады.

Оларға теледидар, ас үй техникасы, камералар жатады. Тежегішті, қозғалтқышты, құлыптарды, капотты, желдеткішті және құралдар тақтасын басқаратын автокөліктерге арналған компьютерлік жүйе өте сенімсіз; жүйенің аталған бөліктері борттық желіге қол жеткізу кезінде қаскүнемдер үшін өте осал болып келеді. Сонымен қатар шабуылды Интернет арқылы қашықтан жасауға болады. Хакерлер жүректің электр ширатқышын қашықтан басқаруға болатындығын көрсетті. Олар кейінірек инсулиндік сорғылар мен имплантталатын кардиодефибрилляторларға қол жеткізуді үйренді.

Hewlett Packard компаниясы 2015 жылы ірі көлемді зерттеу жүргізді, ол жерде IoT құралдарының 70%-ында өз құпиясөздерінің қауіпсіздігінде осалдық бар екені, мәліметтерді шифрлау мен қолжетімділікті беруде қиындықтар туындайтындығы және мобильді құралдарға арналған қосымшалардың 50%-ы мәлімет алмастырмайтындығы көрсетілді.

Касперский лабораториясы — ақпаратты қорғауға арналған бағдарламалық жабдықтама өндірісінде қызмет ететін компания IoT-қа қосылған нысандарға сынақ жүргізіп, бейнебала күтушілерді бейнежазбаны ұстап қалу үшін бұзуға болатындығын және ақпаратты шифрланбаған күйде тасымалдайтын кофемашинаның қосылған Wi-Fi желісінің құпиясөзін сақтай алатындығын көрсетті.

IoT қауіпсіздігі жаңа технологиялардың ең маңызды тұстарының біріне айналды. Мұндай жүйелер арқылы тасымалданатын және сақталатын мәліметтерге қауіп төнбейтіндей көрінуі мүмкін, бірақ, олай емес. Қажетті қорғанысы жоқ IoT құралдарының ботнетті құруға арналған зиянды кодпен әдейі зақымдалып, шабуылдарға ұшырайтыны шындық.

Интернетте жеке интернет-құпиялық пен қауіпсіздікті қалай сақтауға болады?

VPN киберқауіпсіздіктің көптеген мәселелерін шеше алады және компаниялардың да, жеке тұлғалардың да интернет-құпиялығын барынша арттыра алады. VPN-ді қолдану арқылы Сіз қорғалған VPN желіге қосыласыз, қажетті веб-сайттарға немесе әлеуметтік желілерге еркін кіре аласыз. Сіздің өз қауіпсіздігіңізді қамтамасыз ету үшін осы уақытқа дейін неге VPN мүмкіндіктерін пайдаланбағаныңыз маңызды емес, маңыздысы Сіздің мұны дәл қазір жасай алатындығыңыз болып табылады. VPN қызметтері Интернет желісінің кез келген қолдануышысына қаржылық қолжетімді болды, бұл дербес киберқауіпсіздік пен құпиялықтың жоғары деңгейіне кепілдік береді. VPN-ге жазылу қолданушы үшін айына бірнеше ғана долларға айналады, ол Интернетке шексіз қолжетімділікті, барлық интернет қосылулардың құпиялығы мен қорғанысын қамтамасыз етеді, отбасыңыздың жеке ақпаратының жоғалуының алдын алады.

Қазіргі таңда Интернетте ақпарат алмасу мүмкіндіктері шын мәнінде шексіз және олар қарқынды даму үстінде. Әлеуметтік желілер жаһандық деңгейдегі адамдар арасында осы уақытқа дейін белгісіз болған ақпараттық байланыс дәрежесін құрды. Интернет жүз мыңдаған миллион адамды біріктіретін динамикалық әлеуметтік ортаға айналды. Facebook-тің негізін қалаушы Марк Цукерберг айтқандай, компания миссиясы әлемді барынша ашық және байланысқан ету болып табылады.

Бұл мәселелерді білу және талқылау — оларды шешуге жасалған қадам. Мәселелер шынымен де шешіледі: қолданушылар әлеуметтік желіде үлкен қолдауға ие болады, браузерлер біздің қауіпсіздігіміз бен құпиялығымызға қамқор болады. Себебі адамдар ештеңеге қарамастан өз достарымен, таныстарымен, кейде бүкіл әлеммен ақпарат алмасқысы келеді.