**Интернетте қауіпсіз жұмыс істеуге арналған ұсыныстар**

Біздің күнделікті өміріміздің көп бөлігі қалай да интернетпен байланысты: интернет арқылы жұмыс істейміз, оқимыз, әлеуметтік желілерде бөтен адамдармен танысамыз, достарымызбен әңгімелесеміз және көңіл көтереміз. Сондықтан да интернетте жұмыс істеу бойынша қауіпсіздік ережелерін білу және қолдану өте маңызды. Ол ережелер жағымсыз жағдайларды болдырмауға, өз деректеріңіз бен құрылғыңызды қорғап қалуға көмектеседі.

**Интернеттің негізгі қауіптері**

Интернетте кездестіруге болатын бірнеше интернет-қауіптері мыналар:

* Дербес деректерді ұрлау.
* Деректердің жоғалуы.
* Зиянды бағдарламалар мен вирустар.
* Фишингілік және алаяқтық электрондық хаттар.
* Жасанды сайттар.
* Интернет-алаяқтық.
* Танысуға арналған сайттар мен қосымшалардағы алаяқтық.
* Қабылдауға келмейтін контент.
* Кибербуллинг (сандық технологияларды пайдаланып қорқыту және құдалау).

**Интернетте қауіпсіз іс-қимылдар жасаудың негізгі ережелері**

Жоғарыда көрсетілген қауіптерді болдырмау немесе азайту үшін:

**1. Сенімді интернет-байланысты пайдаланыңыз.**

Жария (жалпыға қол жетімді Wi-Fi желілерін пайдалануды минимумға дейін қысқартыңыз. Егер басқа амалыңыз болмаған жағдайда, дербес деректерді пайдалану арқылы жасалатын операцияларды орындамауға тырысу қажет, мысалы интернет-банк қызметтерін пайдалану және онлайн-сатып алуларға қатысу. Мұндай жағдайларда мобильді интернетті пайдаланған дұрысырақ.

Виртуалды жеке желі (VPN) технологиясын пайдаланған дұрыс. Мұндай технология – нақты уақытта сенімді желі арқылы сіз жіберіп жатқан барлық деректерді қорғауды қамтамасыз ете отырып, оларды шифрлауға мүмкіндік береді. Алайда мұнда да VPN жеткізушіні таңдауда аса мұқият болу қажет.

**2. Сенімді құпиясөздерді пайдаланыңыз.**

Құпиясөздер пайдаланатын аккаунттарды бұзып кіруден және дербес ақпараттарды ұрлаудан қорғауға пайдаланылады. Шын мәнінде киберқауіпсіздік жүйесінде құпия сөздер ең осал орын болып саналады. Себебі, адамдар көбінше жаттауға оңай комбинацияларды пайдаланады, ал шынтуайтында бұзу қиын комбинацияларды қолдану қажет. QWERTY, 12345, туған күн секілді нұсқаларды тіпті пайдалануға болмайды, бас және кіші әріптер, сандар мен арнаулы символдарды қолдана отырып, кемінде 12 таңбадан құралған құпиясөз пайдаланыңыз. Бірнеше есептік жазбаға бірдей құпиясөзді пайдалану арқылы өз деректеріңізді одан да үлкен қауіпке дұшар қыласыз. Себебі, бір сайттан есептік деректерді алған зиянкестер сол құпиясөзбен сіздің басқа аккаунттарыңызға да кіре алатын болады.

Бернеше кеңестер:

* құпиясөзді қағазға немесе телефондағы жазбаларға жазуға болмайды;
* құпиясөзді браузердегі автотолтыру өрісінде сақтауға болмайды;
* екі факторлы аутентификацияны қосыңыз;
* интернет-банкингіде, электрондық поштада, телефон операторының және интернет-провайдердің жеке кабинеттерінде пайдаланатын құпиясөзді жүйелі түрде жаңартып жүріңіз.

Құпиясөздер менеджерін (генераторын) пайдалану туралы да ойланып көруге болады. Құпиясөздер менеджерлері сенімді құпиясөздер құруға, оларды бірегей мастар-құпиясөзбен қорғалған сандық қоймада сақтауға және есептік жазбаға кіруге кезінде дағдылы түрде алмастыруға көмектеседі.

**3. Мүмкіндігінше көп факторлы аутентификацияны қосыңыз.**

Екі немесе көп факторлы аутентификация – түпнұсқалылықты тексеру тәсілі. Мұнда есептік жазбаға кіру үшін екі немесе одан көп тексеру әдістері қолданылады. Мысалы, көп факторлы аутентификация кезінде жай ғана пайдаланушының атын немесе құпиясөзді сұраудың орнына, қосымша ақпараттар да сұралады:

* Қосымша бір реттік құпиясөз. Оны веб-сайттың аутентификациялау серверлері телефонға немесе электрондық поштаға жібереді.
* Жеке қауіпсіздік сұрақтарына жауап беру.
* саусақтың ізі немесе басқа биометриялық ақпарат, мысалы, дауыстық деректер немесе жүзін айырып тану.

Онлайн-аккаунтты қорғау үшін мүмкіндігінше көп факторлы аутентификацияны пайдалануға кеңес беріледі. Бұл ретте, көп факторлы аутентификация кибершабуылдың сәтті болу ықтималдығын азайтады. Интернетте қауіпсіздікті қамтамасыз ету үшін Google Authenticator немесе Authy секілді түпнұсқалықты тексеру қосымшаларын қолдануға болады.

Өзіңіздің аккаунттарыңызды бөтен құрылғыларда қалдырмаңыз: кей кездерде өзіңіздің ноутбугыңыз немесе компьютеріңіз болмай қалады, міне сондай жағдайда басқа адамның құрылғысын пайдаланасыз және өз аккаунтыңыз қолданылған парақшаны ашық қалдырып кетуіңіз мүмкін. Браузерді жапқан жағдайда да аккаунтқа кіру жүзеге асырылады, демек, оны бөтен адамдар пайдаланып кетуі мүмкін.

Бөтен адамдардың құрылғыларында логинді өшіріп кетуді және өз аккаунтыңызға қолданатын құпиясөзді енгізуден алдын «бөтен компьютер» белгісін қоюды әдетке айналдырыңыз.

**4. Операциялық жасақтама мен операциялық жүйені жаңартып жүріңіз.**

Операциялық жасақтамаларды әзірлеушілер тұрақты түрде өнімдердің қауіпсіздігін сақтау бойынша жұмыстар атқарып отырады. Олар соңғы қауіптерді қадағалап, қосымшаларда осал жерлерді анықтаған жағдайда, қауіпсіздікке түзетулер енгізеді. Пайдаланушының төлем деректері, денсаулық жағдайы туралы мәліметтер және басқа құпия ақпараттар қамтылған операциялық жүйелер мен қосымшалардың соңғы нұсқаларын пайдаланыңыз.

**5. Сайттың сенімділігіне көз жеткізіңіз.**

Сенімділік – барлық веб-сайттардың маңызды атрибуты, әсіресе, онлайн-сатып алулар мен интернет-банкинг жүзеге асырылатын веб-сайттар. HTTPS-пен басталатын сайттар SSL-сертификатпен қорғалған. HTTP-мен басталатын сайттарға сенуге болмайды, мұндай ресурстар қорғалмаған. Мекенжай жолындағы жабық құлып түріндегі белгі – қауіпсіз парақшаның айрықша ерекшелігі болып табылады. Егер сол белгіге бассаңыз, қосымша бетте сайт тұралы ақпарат пайда болады.

Сайттың басқа да сенімділік белгілері келесілерді қамтиды:

* Тыныс белгілері дұрыс қойылған, орфография және грамматикалық тұрғыдан дұрыс жазылған мәтін. Беделді брендтер өз веб-сайттарының лайықты сапада рәсімделуіне аса мән береді;
* Экранның еніне сәйкес келетін сапалы көрініс.
* Сайттың құрылымына үйлесімді және оны аса көп қамтымаған хабарландырулар.
* Біркелкі түстермен рәсімдеу және тыңғылықты тақырып.

**6. Қандай сілтемелермен кіріп жатқаныңызды қадағалаңыз.**

Сілтеме бойынша бір абайсыз ауысым арқылы сіздің дербес деректеріңіз зиянкестердің қолына түседі немесе құрылғыға зиянды бағдарлама арқылы зақым келеді. Сондықтан да қандай сілтемелер бойынша кіріп жатқаныңызды қадағалауыңыз қажет және белгілі бір түрдегі контенттерден: сенімсіз дереккөздерден келген сілтемелерден, спам-хабарламалардан, онлайн-викториналардан, «тегін» ұсыныстардан және қажетсіз жарнамалардан алшақ болған дұрыс.

Түпнұсқалығына күмәніңіз болған электрондық хаттар келген кезде, сонда қамтылған сілтемелер бойынша кірмеңіз және қосымшаларды ашпаңыз. Ондай хабарламаларды мүлдем ашпауға кеңес береміз. Егер электрондық хаттың түпнұсқалығына сенімді болмасаңыз, тікелей жіберушіге хабарласыңыз. Мысалы, сіздің банктен іспетті күмәнді хат алған кезде банкке қоңырау шалыңыз да, расында солар хат жіберді ме, сұраңыз.

Сайтты қарау кезінде сілтемелер бойынша көшу байланысты немесе күтілген беттер арқылы жүзеге асырылып жатқанына көз жеткізіңіз. Мысалы, егер сіз антивирустық бағдарламаны орнатудың сипаттамасына сілтеме бойынша кіргіңіз келсе, бірақ оның орнына шоу-бизнестің жаңалықтарына кіріп кетсеңіз, ол парақшадан шұғыл шығып кетіңіз.

**7. Құрылғыларыңызды қорғаңыз.**

Пайдаланушылардың көпшілігі керегін сатып алу немесе интернеттен ақпарат іздеу үшін компьютерге қарағанда мобильді құрылғыларды көп пайдаланады. Сондықтан да мұндай құрылғылар сенімді түрде қорғалған болуы қажет. Барлық құрылғыларда: телефондарда, компьютерлерде, планшеттерде, ақылды сағаттарда, ақылды теледидарларда және басқа құрылғыларда құпиясөздер, құпия кілтсөздер және саусақ іздерін тану немесе жүзін айырып тану технологиясы секілді басқа қауіпсіздік құралдарын пайдалануға кеңес беріледі. Қауіпсіздіктің осындай шаралары кибершабуылдың немесе дербес деректеріңізді ұрлаудың ықтималдығын азайтады.

**8. Тұрақты түрде резервке көшіріп отырыңыз.**

Маңызды жеке ақпараттарды сыртқы қатқыл дискіге көшіріп және тұрақты түрде резервтік көшірмелер жасап отыру қажет. Бопсалаушы-бағдарламалар – компьютерді бұғаттайтын және өзіңізге маңызды және қажет файлдарды көруді болдырмайтын зиянкес бағдарламалар. Деректерді резервтік көшіру бопсалаушы-бағдарламалардың шабуылынан болатын жағымсыз салдарды азайтуға көмектеседі. Зиянкес бағдарламалардың басқа да түрлері бар, олар дербес деректерге қол жеткізуді бұғаттайды, операциялық жүйеге шамадан тыс кедергі жасайды немесе файлдарды жойып жібереді.

**9. Пайдаланбайтын есептік жазбаларды жойып тастаңыз.**

Көп адамдардың ұзақ уақыттан бері пайдаланбай жүрген есептік жазбалары бар. Ондай жазбалардың болуы интернетті пайдалану кезінде осалдық көзі болуы мүмкін. Ескі есептік жазбаларда әдетте әлсіз құпиясөздер болады, ал олар пайдаланылған сайттарда деректерді қорғаудың сенімді саясаты қолданылуы мүмкін. Сондай-ақ, әлеуметтік желілердегі ескі профильдердің деректері бойынша киберқылмыскерлер сіз туралы түрлі деректерді, мысалы туған күніңіз мен тұратын жеріңізді жинап алуы және оларды өз мақсаттарына пайдалануы мүмкін. Ескі есептік жазбаларды жойып тастау және есептік жазбалар жойылған бөтен серверлерден сіздің деректеріңізді жоюға өтінім жіберу керек.

**10. Жүктеуде абай болыңыз.**

Зиянкестердің мақсаты – сізді зиянкес бағдарламаны жүктеп алуға мәжбүрлеу. Солай бола қалған жағдайда олар сіздің құрылғыңызға оңай кіре алатын болады. Зиянкес бағдарламалар белгілі ойындардан бастап, ауа-райын немесе жолдардағы кептелістерді тексеруге арналған қосымшалар секілді кез келген бағдарламалық жасақтама ретінде ұсынылуы мүмкін. Сонымен қатар, ондай бағдарламаларды зиянкестер өздері жасаған веб-сайттарға жасырып қоюы мүмкін. Сол сайттарға кірген кезде олар зиянкес бағдарламаларды сіздің құрылығыңызға орнатуға тырысады.

Зиянкес бағдарламалар келесідей залалдар келтіреді: құрылғының жұмысын бұзады, дербес деректерді ұрлайды, компьютерге заңсыз кіру рұқсатын береді. Әдетте, зиянкес бағдарламаларды жүктеу үшін пайдаланушы тарапынан бірқатар әрекеттер жасау қажет болады, алайда веб-сайт алдын ала рұқсат сұрамай, зиянкес бағдарламаларды компьютерге орнату барысында жасырын жүктеу арқылы да жүзеге асыруы мүмкін. Таныс емес сайтқа кіру және құрылғыға бағдарламалар жүктеу кезінде өте абай болыңыз, контентті тек сенімді немесе ресми көздерден ғана жүктеңіз. Жүктеу папкаларын тұрақты түрде тексеріп отырыңыз және белгісіз файлдарды жедел жойып жүріңіз. Ондай файлдар сіздің құрылғыңызға жасырын жүктеу арқылы енген болуы мүмкін.

**11. Хабарларды жариялауда абай болыңыз.**

Есте сақтаңыз: интернетте жарияланған ақпаратты жою мүмкіндігі жоқ. Барлық жарияланған пікірлер мен суреттер Желіде мәңгіге қалып қоюы мүмкін. Себебі, түпнұсқаны жойған кезде сіз олардың басқа пайдаланушылар көшіріп алған көшірмелерін жоя алмайсыз. Пікіріңізді жариялағаннан кейін «өз сөзіңізді кері қайтарып алуға» мүмкіндік болмайды. Сондай-ақ жарияланған әшкерелейтін суреттерді де жою мүмкін емес. Егер сіз жазған нәрселерді достарыңыздың, әріптестеріңіздің немесе әлеуетті жұмыс берушінің көргенін қаламасаңыз, онда ол материалды жарияламаңыз.

Әсіресе, жеке ақпараттарды интернетте жариялауда абай болыңыз, шын өмірде сіз бөтен адамдарға дербес деректеріңізді хабарламайсыз ғой, сол сияқты оларды да интернетте жариялап, миллиондаған пайдаланушыларға қолжетімді ету қажет емес.

Электрондық поштаңызды беру кезінде де сақ болыңыз. Электрондық поштаның тек тіркеу және жазылуға арналған қосымша (екінші, оған қоса үшінші де артық болмайды) есептік жазбасы болған дұрыс. Ол жұмыс поштаңызбен және достарыңыз бен жақындарыңызбен хат жазысуға арналған поштаңызбен ұқсас болмауы тиіс. Бірнеше электрондық поштаның болуы сіздің пошта арқылы хат алмасу әрекеттеріңізді жүйелендіреді: егер жеке басыңызға қатысты хаттар жұмыс поштаңызға келсе, оларды бірден спамға жіберіп отыруға болады.

**12. Онлайн-танысулардан сақ болыңыз.**

Сіз интернеттегі таныстарыңыздың өздерін көрсетіп жатқандай екеніне сенімдісіз бе? Олар кейде нақты адам болмауы да мүмкін. Әлеуметтік желілерде жалған профильдерді пайдалану арқылы зиянкестер ақшаларын ұрлау үшін аңғал пайдаланушыларды табуға тырысады. Интернеттегі әлеуметтік өмірге шынайы әлемдегі әлеуметтік өмірге қараған сияқты сақтықпен қарау керек. Бұл әсіресе, соңғы жылдарда онлайн-танысулар арқылы алаяқтық жасалған жағдайлардың едәуір артуымен байланысты.

**13. Интернетте тапқан ақпаратты мұқият тексеріңіз.**

Өкінішке қарай, интернетте жалған жаңалықтар мен жалған мәліметтер өте көп. Күнделікті алып жүрген ақпараттар ағымында оңай жоғалып кетуге де болады. Егер оқыған ақпараттың сенімділігіне күмәніңіз болса, өзіңіз дербес зерттеу жүргізіп, нақты фактілерді анықтаңыз. Сенімді веб-сайттарда, әдетте, алғашқы дереккөздерге сілтеме жасалады. Ал күмәнді парақшаларда ешқандай сілтемелер көрсетілмейді.

**14. Антивирус қолданыңыз және оны жүйелі түрде жаңартып отырыңыз.**

Интернетте қауіпсіздікті қамтамасыз ету бойынша ұсыныстарды қолданумен қатар, сенімді антивирус пайдалану да өте маңызды. Интернеттегі қауіпсіздікке арналған бағдарламалық жасақтама құрылғы мен деректерді қорғаумен қатар, кеңінен таралған қауіптермен бірге вирустарды, зиянкес бағдарламаларды, сондай-ақ тыңшы-қосымшаларды пайдалану арқылы кешенді шабуылдарды, шифр анықтаушыларды және т.б. бұғаттайды. Операциялық жүйелер мен қосымшалар секілді, антивирустық бағдарламалық жасақтамаларды да жүйелі түрде жаңартып, жаңа киберқауіптерден сенімді қорғанып отыру қажет.