# ИНТЕРНЕТТЕГІ НЕГІЗГІ ҚАУІПТЕР ЖӘНЕ ИНТЕРНЕТТІ ҚАУІПСІЗ ПАЙДАЛАНУ ЕРЕЖЕЛЕРІ

**1. КІРІСПЕ**

Қазіргі заманда интернет адамзат өмірінің ажырамас бөлігіне айналды. Ол білім алудың, қарым-қатынас жасаудың, ойын-сауық пен басқа да көптеген салалардың негізгі құралы болып табылады. Қазақстанда да интернеттің таралуы жыл сайын артып, қоғамның барлық саласына терең еніп келеді. Дегенмен, интернеттің осындай зор пайдасымен қатар, оның көптеген қауіптері де бар екенін ұмытпауымыз керек. Киберқылмыстың өсуі, жеке ақпараттың ұрлануы, қаржылық алаяқтық және психикалық денсаулыққа зиян келтіру сияқты қауіптер әрбір интернет пайдаланушысы үшін өзекті мәселе болып отыр.

Бүгінгі дәрістің мақсаты – интернеттегі негізгі қауіптерді анықтау және олардан қалай сақтану керектігін түсіндіру. Біз сіздерді онлайн қауіптерден хабардар етеміз және қауіпсіздікті қамтамасыз ету үшін практикалық кеңестер береміз. Лекция барысында біз балаларға, жасөспірімдерге және ересектерге арналған қауіптерді, сондай-ақ Қазақстандағы интернет қауіптерінің нақты мысалдарын қарастырамыз. Сонымен қатар, интернетті қауіпсіз пайдаланудың негізгі ережелерін талқылаймыз.

**2. ИНТЕРНЕТТЕГІ НЕГІЗГІ ҚАУІПТЕР**

Интернетте кез келген жастағы пайдаланушылар үшін көптеген қауіптер бар. Оларды шартты түрде балаларға арналған қауіптер және жасөспірімдер мен ересектерге арналған қауіптер деп бөлуге болады.

**2.1. БАЛАЛАРҒА АРНАЛҒАН ҚАУІПТЕР**

Балалар интернеттің әлеуетін толық түсінбеуіне байланысты онлайн қауіптерге көбірек ұшырайды.

* **Қорлау және буллинг:** Балалар чаттар, электрондық пошта немесе ұялы телефон арқылы қорлау, кемсіту немесе мазалау хабарламаларын алуы мүмкін . Кибербуллинг бүгінгі күні кеңінен таралған мәселе. Жасөспірімдердің 90%-ы кибербуллингті проблема деп санаса, 63%-ы оны елеулі мәселе деп есептейді . Кибербуллинг әлеуметтік желілер мен онлайн ойындарда жиі кездеседі және балалардың психикалық денсаулығына теріс әсер етуі мүмкін. Егер бала қорлаудың құрбаны болса, ол бұл туралы үлкендерге хабарлауы керек және әлеуметтік желі әкімшісіне шағымдануы қажет . Қазақстанда да кибербуллинг мәселесі өзекті болып отыр .
* **Вирустар мен хакерлер:** Балалар кездейсоқ түрде компьютерге зиян келтіретін немесе отбасының құпиялылығы мен қауіпсіздігіне қауіп төндіретін вирустарды жүктеп алуы мүмкін. Хакерлер зиянды бағдарламаларды тарату арқылы жеке ақпаратқа қол жеткізуге тырысады. Сондықтан антивирустық бағдарламалық жасақтаманы пайдалану және қауіпті сілтемелерден аулақ болу өте маңызды.
* **Заңдық және қаржылық қауіптер:** Балалар ата-анасының несие картасының нөмірін беру немесе басқа адамның құқықтарын бұзу сияқты теріс заңдық немесе қаржылық салдары бар әрекеттер жасауы мүмкін . Рұқсатсыз онлайн сатып алулар жасау немесе жеке қаржылық ақпаратты бөлісу қауіпті болуы мүмкін. Балаларды қаржылық алаяқтықтан және заңсыз әрекеттерден қорғау үшін олардың қаржылық және заңдық сауаттылығын арттыру қажет.
* **Тиісті емес материалдарға тап болу:** Балалар жеккөрінішті немесе зорлықшыл сипаттағы немесе қауіпті немесе заңсыз әрекеттерге шақыратын материалдарға тап болуы мүмкін. Бұл материалдарға зорлық-зомбылық көріністері және жеккөрінішті контент жатады. Балалар бұл материалдарды іздеуі немесе кездейсоқ түрде чаттар, электрондық пошта немесе мессенджерлер арқылы көріп қалуы мүмкін. Сондықтан ата-аналар балаларының жасына сай емес контентке қол жеткізуін шектеуі керек.
* **Кибер жыртқыштар:** Бұл балалардың сеніміне кіріп, оларды қауіпті кездесулерге тартуға тырысатын адамдар. Олар анонимділікті пайдаланып, "ойнайық" деген сылтаумен балаларды өздеріне тартады. Ата-аналар балаларымен онлайн әрекеттері туралы ашық сөйлесуі және жыртқыштардың әрекет ету тәсілдері туралы түсіндіруі маңызды.
* **Жеке ақпаратты жариялау:** Балалар әлеуметтік желілерде өздерінің үй мекенжайларын немесе отбасылық демалыс жоспарларын сияқты жеке ақпаратты жариялауы мүмкін . Балаларды онлайн құпиялылық туралы оқыту және қандай ақпаратты жариялауға болмайтынын түсіндіру қажет.

**2.2. ЖАСӨСПІРІМДЕР МЕН ЕРЕСЕКТЕРГЕ АРНАЛҒАН ҚАУІПТЕР**

Жасөспірімдер мен ересектер де интернетте көптеген қауіптерге тап болуы мүмкін.

* **Байланыс қауіптері:** Бала болып көрінетін ересектермен, фото немесе бейне сұрайтын бейтаныс адамдармен және онлайн алаяқтармен байланысу қаупі бар. Романтикалық алаяқтық пен инвестициялық алаяқтық сияқты қауіптерден сақ болу керек.
* **Мінез-құлық қауіптері:** Дұрыс емес, ауыртпалық немесе құрметсіздікпен әрекет ету немесе осындай әрекеттің құрбаны болу қаупі бар . Бұған кибербуллинг, парольдерді дұрыс пайдаланбау, рұқсатсыз сатып алулар және жеке ақпаратты рұқсатсыз жариялау жатады. Онлайн этикетті сақтау және онлайн қарым-қатынаста жауапкершілікті болу маңызды.
* **Келісімшарт қауіптері:** Әділетсіз келісімшарттарға, жазылымдарға немесе шарттар мен ережелерге келісу жеке басын ұрлауға немесе алаяқтыққа әкелуі мүмкін . Онлайн келісімдерге қол қою кезінде мұқият болу және шарттарды түсіну қажет.
* **Фишинг шабуылдары:** Жалған электрондық пошталар, хабарламалар немесе веб-сайттар арқылы құпия ақпаратты алуға тырысу қаупі бар. Фишингтің әртүрлі түрлерін тану және олардан сақтану жолдарын білу маңызды.
* **Зиянды бағдарламалық жасақтама:** Ақпаратты ұрлайтын немесе құрылғыларға зиян келтіретін зиянды бағдарламалық құралдар қаупі бар. Антивирустық бағдарламаны пайдалану және күдікті сілтемелерден аулақ болу керек. Вирустар, құрттар, трояндар және рэнсомвейр сияқты зиянды бағдарламалардың таралу жолдары мен түрлерінен хабардар болу қажет.
* **Жеке басын ұрлау:** Ұрланған жеке ақпаратты пайдаланып, басқа адамның атынан әрекет ету қаупі бар. Жеке ақпаратты қорғау және жеке басын ұрлаудың қаржылық және басқа да салдарын білу маңызды.
* **Деректердің бұзылуы:** Интернеттегі ауқымды дерекқорларды бұзу арқылы жеке деректердің жария болу қаупі бар. Онлайн қызметтерді пайдалану кезінде құпиялылық саясатын қарастыру және деректердің бұзылуының заңдық аспектілерін білу қажет
* **Кибер бопсалау:** Компьютерлік жүйелерге қол жеткізуді бұғаттау немесе деректерді шифрлау арқылы ақша талап ету қаупі бар . Маңызды деректердің резервтік көшірмесін жасау және рэнсомвейр шабуылдарынан қорғану жолдарын білу қажет.
* **Онлайн алаяқтық:** Интернет арқылы ақша немесе жеке ақпаратты заңсыз жолмен алу әрекеттері қаупі бар . Инвестициялық алаяқтық, романтикалық алаяқтық және онлайн сауда алаяқтығы сияқты алаяқтықтың әртүрлі түрлерінен хабардар болу керек .
* **Коммуникациялық тәуекелдер:** киберқудалаудың балалармен байланысы қаупі бар . Балалардың онлайн қарым-қатынасын бақылау және оларға қауіпті жағдайлар туралы түсіндіру маңызды.

**2.3. ҚАЗАҚСТАНДАҒЫ ИНТЕРНЕТ ҚАУІПТЕРІНІҢ МЫСАЛДАРЫ**

Қазақстанда да интернет алаяқтығы кеңінен таралған. Мысал ретінде келесі жағдайларды келтіруге болады:

|  |  |
| --- | --- |
| **Қауіп түрі** | **Мысалдар** |
| **Банк алаяқтығы** | Өзін банк қызметкері ретінде таныстырып, азаматтарға несие беріп, несие қаражатын иемдену . |
| **Онлайн сауда алаяқтығы** | Әлеуметтік желілерде жалған хабарландырулар орналастыру немесе жалған аккаунттар арқылы тауар сату. |
| **Жеке деректерді пайдалану арқылы алаяқтық** | Банк қызметкері ретінде қоңырау шалып, жеке деректерді сұрау және оларды заңсыз пайдалану. |
| **Алдын ала төлем алаяқтығы** | Автокөлікті сатып алуға ниет білдіріп, алдын ала төлем сұрау және кейін байланысқа шықпау . |
| **Деректердің бұзылуы** | Қазақстандықтардың жеке деректерінің GitHub ресурсында жариялануы. |
| **Кибербуллинг** | Әлеуметтік желілерде қорлау, кемсіту және жалған ақпарат тарату. |

Бұл тек Қазақстанда кездесетін интернет қауіптерінің бірнеше мысалы ғана.

**3. ИНТЕРНЕТТІ ҚАУІПСІЗ ПАЙДАЛАНУ ЕРЕЖЕЛЕРІ**

Интернеттегі қауіптерден сақтану үшін әрбір пайдаланушы қауіпсіздік ережелерін білуі және оларды ұстануы қажет.

**3.1. ҚҰПИЯЛЫЛЫҚТЫ ҚОРҒАУ**

* Жеке ақпаратты бөлісуді шектеңіз. Әсіресе, бейтаныс адамдарға немесе сенімсіз сайттарға жеке деректеріңізді бермеңіз.
* Әлеуметтік медиадағы құпиялылық параметрлерін басқарыңыз. Кім сіздің жазбаларыңызды көре алатынын және қандай ақпарат сіздің профиліңізде көрсетілетінін реттеңіз.
* Қауіпсіз емес Wi-Fi желілерін пайдаланудан аулақ болыңыз. Әсіресе, қаржылық операцияларды жасаған кезде немесе құпия ақпаратты енгізген кезде сақ болыңыз.
* Веб-сайттардың құпиялылық саясатын тексеріңіз. Сайт сіздің деректеріңізді қалай пайдаланатынын және қорғайтынын біліп алыңыз.
* Қажет болған жағдайда анонимді түрде тіркеліңіз. Егер сізге қандай да бір сайтқа тіркелу қажет болса, жеке ақпаратыңызды беруді қажет етпейтін жолдарды іздеңіз.

**3.2. ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ**

* Күшті және бірегей құпия сөздерді пайдаланыңыз. Әрбір онлайн аккаунтыңыз үшін әртүрлі және күрделі құпия сөздер ойлап табыңыз.
* Екі факторлы аутентификацияны (2FA) қосыңыз. Бұл сіздің аккаунттарыңызға қосымша қауіпсіздік деңгейін қосады.
* Бағдарламалық жасақтаманы жүйелі түрде жаңартыңыз. Операциялық жүйені, браузерлерді және басқа да қолданбаларды соңғы нұсқаға дейін жаңартып отырыңыз.
* Антивирустық бағдарламаны орнатыңыз және жаңартыңыз. Бұл сіздің құрылғыңызды зиянды бағдарламалардан қорғауға көмектеседі.
* Күдікті сілтемелер мен электрондық пошталардан сақ болыңыз. Белгісіз жіберушілерден келген хаттарды ашпаңыз және күдікті сілтемелерді баспаңыз.
* Қауіпсіз веб-сайттарда ғана сауда жасаңыз . Сайттың мекенжайында "https://" бар екеніне және құлып белгісінің тұрғанына көз жеткізіңіз.
* VPN қосылымын пайдаланыңыз. Әсіресе, қоғамдық Wi-Fi желілерін пайдаланған кезде бұл сіздің интернет трафигіңізді шифрлайды.
* Деректердің резервтік көшірмесін жасаңыз. Маңызды файлдарыңызды сыртқы қатты дискке немесе бұлттық сақтауға сақтаңыз.
* Файлдарды вирусқа тексеріңіз . Белгісіз көздерден жүктелген файлдарды ашпас бұрын міндетті түрде вирусқа тексеріңіз.

**3.3. ЖАУАПТЫ МІНЕЗ-ҚҰЛЫҚ**

* Онлайн этикетті сақтаңыз . Басқа пайдаланушылармен сыпайы және құрметпен қарым-қатынас жасаңыз.
* Кибербуллингке жол бермеңіз және оның құрбаны болған жағдайда не істеу керектігін біліңіз. Егер сіз кибербуллингке тап болсаңыз, жауап бермеңіз, қорлаушыны бұғаттаңыз және бұл туралы үлкендерге немесе әлеуметтік желі әкімшісіне хабарлаңыз.
* Басқалар туралы жеке ақпаратты жарияламаңыз . Біреудің рұқсатынсыз оның фотосуреттерін, мекенжайын немесе басқа да жеке деректерін жарияламаңыз.
* Жалған ақпаратты таратпаңыз . Көзі жеткізілмеген ақпаратты бөліспеңіз.
* Онлайн уақытты бақылаңыз . Интернетті шектен тыс пайдалану сіздің денсаулығыңызға және басқа да маңызды істеріңізге теріс әсер етуі мүмкін.
* Интернеттегі барлық ақпаратқа сенбеңіз . Ақпараттың шынайылығын әрқашан тексеріңіз.

**3.4. БАЛАЛАР МЕН ЖАСӨСПІРІМДЕРДІ ҚОРҒАУ БОЙЫНША КЕҢЕСТЕР**

* Балалармен интернетті қауіпсіз пайдалану туралы сөйлесіңіз . Оларға онлайн қауіптерді түсіндіріңіз және қауіпті жағдайларда не істеу керектігін үйретіңіз.
* Ата-аналар балаларының онлайн әрекеттеріне қатысып, олармен бірге интернетті зерттеуі керек .
* Балаларға онлайн қауіптерді тануды үйретіңіз . Оларға бейтаныс адамдармен сөйлесудің, жеке ақпаратты бөлісудің және күдікті сілтемелерді басудың қауіпті екенін түсіндіріңіз.
* Технологияларды балаларды қорғау үшін пайдаланыңыз . Ата-аналық бақылау бағдарламаларын орнатыңыз және балалардың жасына сай емес контентке қол жеткізуін шектеңіз .
* Отбасылық медиа жоспарын жасаңыз . Отбасы мүшелерінің интернетті пайдалану уақытын және ережелерін анықтаңыз.
* Балаларды цифрлық сауаттылыққа үйретіңіз . Оларға интернетті жауапкершілікпен және қауіпсіз пайдалануды үйретіңіз.
* Мектептер мен ата-аналар жасөспірімдерге желідегі жауапты мінез-құлық, жөн-жосықсыз репост жасау қаупі және цифрлы азамат сезімін сақтаудың маңызы туралы білім беру үшін бірлесіп жұмыс істеуі керек .

**4. ҚОРЫТЫНДЫ**

Интернет қазіргі заманда біздің өміріміздің маңызды бөлігі болып табылады. Алайда, оның пайдасымен қатар, көптеген қауіптері де бар. Біз бүгін интернеттегі негізгі қауіптерді қарастырдық және қауіпсіз интернет пайдаланудың маңыздылығын атап өттік. Әрбір пайдаланушы өз қауіпсіздігі үшін жауапты екенін есте сақтауы керек. Қауіпсіздік ережелерін ұстану және сақ болу арқылы біз өзімізді және жақындарымызды онлайн қауіптерден қорғай аламыз.

Қосымша ақпарат алу үшін келесі ресурстарға жүгінуге болады:

* ЮНИСЕФ Қазақстан
* Қазақстан Республикасының Ішкі істер министрлігінің сайты
* Интернет қауіпсіздігіне арналған басқа да сайттар мен ұйымдар

Есіңізде болсын, интернетті қауіпсіз пайдалану – бұл сіздің және сіздің жақындарыңыздың әл-ауқатын қамтамасыз етудің маңызды шарты.