# ИНТЕРНЕТ ҚАУІПСІЗДІГІ: АНЫҚТАМАСЫ,

# ҚАЖЕТТІЛІГІ ЖӘНЕ ҚОРҒАНУ ЖОЛДАРЫ

## КІРІСПЕ

**Интернет қауіпсіздігі** – бұл онлайн транзакцияларды, деректерді және әрекеттерді қорғау үшін қолданылатын кез келген киберқауіпсіздік шарасы . Оның негізгі мақсаты – интернет пайдаланушыларды хакерлерден қорғау және деректердің ағып кетуін шектеу немесе толығымен жою . Бұл ұғым киберқауіпсіздік пен компьютерлік қауіпсіздіктің кеңірек идеяларының маңызды құрамдас бөлігі болып табылады, соның ішінде браузер қауіпсіздігі, желідегі әрекет қауіпсіздігі және желі қауіпсіздігі сияқты тақырыптарды қамтиды . Ақпараттық қауіпсіздік, өз кезегінде, мемлекеттік ақпараттық ресурстарды, сондай-ақ ақпарат саласындағы жеке адамдардың құқықтары мен қоғам мүдделерін қорғаудың жалпы жай-күйін білдіреді .

Қазіргі заманда интернет технологияларының барлық салаға терең енуіне байланысты интернет қауіпсіздігінің өзектілігі күннен-күнге артып келеді. Электрондық коммерцияның қарқынды дамуы, онлайн білім берудің кең таралуы, қашықтан жұмыс істеудің танымалдығы және әлеуметтік желілердің ғаламдық ауқымға ие болуы жеке және ұйымдық деректерді сенімді қорғау қажеттілігін тудырады. Осыған байланысты, дәріс материалының мақсаты – тыңдаушыларды интернет қауіпсіздігінің негізгі ұғымдарымен таныстыру, оның қажеттілігін жан-жақты түсіндіру және қазіргі заманғы қауіптерден тиімді қорғану жолдарын көрсету болып табылады.

## ИНТЕРНЕТ ҚАУІПСІЗДІГІНІҢ НЕГІЗГІ ТҮСІНІКТЕРІ

Интернет қауіпсіздігі тікелей ақпараттық қауіпсіздікпен тығыз байланысты. Ақпараттық қауіпсіздік – бұл мемлекеттік ақпараттық ресурстардың, сондай-ақ ақпарат саласындағы жеке тұлғалардың құқықтары мен қоғам мүдделерінің қорғалуын қамтамасыз ететін жағдай . Интернет қауіпсіздігі ақпараттық қауіпсіздіктің маңызды бөлігі ретінде қарастырылады және интернетке қосылған барлық жүйелер мен онда сақталатын деректерді қорғауға бағытталған шаралар кешенін қамтиды.

Интернет қауіпсіздігі бірнеше негізгі құрамдас бөліктерден тұрады. Олардың бірі – желілік қауіпсіздік. Желілік қауіпсіздік компьютерлік желілерді мақсатты жасалған шабуылдардан немесе зиянды бағдарламалардың таралуы сияқты әртүрлі қауіптерден қорғауға бағытталған әрекеттерді қамтиды . Екінші маңызды бөлік – құрылғылар қауіпсіздігі. Бұл интернетке қосылған барлық құрылғыларды, соның ішінде дербес компьютерлерді, смартфондарды, планшеттерді және «заттар интернетінің» (IoT) құрылғыларын рұқсатсыз кіруден, заңсыз пайдаланудан және зиянды әсерлерден қорғауды көздейді 4. Үшінші құрамдас бөлік – онлайн әрекет қауіпсіздігі. Бұл интернеттегі пайдаланушылардың күнделікті әрекеттерін, мысалы, веб-сайттарды шолуын, онлайн транзакцияларды жүргізуін және әртүрлі коммуникация құралдарын пайдалануын қауіпсіз етуге бағытталған шараларды қамтиды.

Интернет қауіптерінің алуан түрі бар, оларды бірнеше негізгі санатқа бөлуге болады. Ең көп таралғандарының бірі – зиянды бағдарламалар (malware), олардың қатарына вирустар, құрттар, трояндық бағдарламалар және шпиондық бағдарламалар кіреді. Бұл бағдарламалар компьютерлерге, серверлерге немесе желілерге зиян келтіру, деректерді ұрлау немесе жою, құрылғылардың жұмысын баяулату немесе тоқтату мақсатында жасалады. Фишинг – бұл құпия ақпаратты, мысалы, пайдаланушы аттары мен құпия сөздерді, банктік деректерді немесе жеке сәйкестендіру нөмірлерін алу мақсатында жалған электрондық хаттар немесе веб-сайттар арқылы жасалатын шабуылдар . Кибершабуылдар – бұл желілерге, жүйелерге немесе құрылғыларға рұқсатсыз кіруді бұғаттау, құнды деректерді ұрлау немесе зақымдау мақсатында жасалатын әрекеттер . Алаяқтық – бұл интернет арқылы ақшаны немесе басқа да құндылықтарды заңсыз иемденуге бағытталған әрекеттердің кең спектрі .

## ИНТЕРНЕТ ҚАУІПСІЗДІГІНІҢ ҚАЖЕТТІЛІГІ

Интернет қауіпсіздігінің қажеттілігі қазіргі заманғы цифрлық әлемдегі әрбір пайдаланушы мен ұйым үшін өте зор. Ең алдымен, ол жеке және қаржылық деректерді қорғау үшін қажет. Жеке деректер, мысалы, аты-жөні, мекенжайы, телефон нөмірі және жеке сәйкестендіру нөмірі өте құнды ақпарат болып табылады, ал олардың заңсыз қолына түсуі ауыр зардаптарға әкелуі мүмкін. Қаржылық деректер, мысалы, банк карталарының нөмірлері мен құпия сөздері тіпті де үлкен қауіп төндіреді, себебі олар алаяқтардың ақшаны ұрлауына немесе жеке басын пайдаланып заңсыз әрекеттер жасауына мүмкіндік береді.

Киберқылмыстың зардаптары жеке тұлғалар мен ұйымдар үшін өте ауыр болуы мүмкін. Жеке тұлғалар ақшасын жоғалтуы, жеке басының ұрлануы немесе психологиялық зардаптарға ұшырауы мүмкін. Ұйымдар болса, қаржылық шығындарға ұшырауы, беделінің түсуі, жұмысының тоқтауы немесе құпия ақпаратының жоғалуы ықтимал.

Қазақстанда да киберқылмыс өршіп тұр. Оған қарсы күрес шаралары жүргізіліп, ұлттық киберқауіпсіздік индексінде елдің орны жақсаруда . Дегенмен, бұл бағытта әлі де көп жұмыс жасау қажет.

## ИНТЕРНЕТ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ

Интернет қауіпсіздігін қамтамасыз ету үшін әртүрлі техникалық және әлеуметтік-ұйымдастырушылық шараларды қолдану қажет.

### ТЕХНИКАЛЫҚ ШАРАЛАР

Ең алдымен, күрделі құпия сөздерді пайдалану маңызды. Құпия сөздер ұзын, әртүрлі символдарды (әріптер, сандар, белгілер) қамтитын және болжауға қиын болуы керек . Әрбір онлайн аккаунт үшін әртүрлі құпия сөздерді орнату ұсынылады. Қосымша қауіпсіздік үшін екі факторлы аутентификацияны қосу керек. Бұл аккаунтқа кіру кезінде екі түрлі растау әдісін, мысалы, пароль және ұялы телефонға келген бір реттік кодты қолдануды білдіреді.

Компьютерлер мен басқа құрылғыларды зиянды бағдарламалардан қорғау үшін антивирустық бағдарламалық жасақтаманы орнату және үнемі жаңартып отыру қажет. Брандмауэрлер желілік трафикті бақылау және күдікті әрекеттерді бұғаттау арқылы қосымша қорғаныс қызметін атқарады. Барлық бағдарламалық жасақтаманы, әсіресе операциялық жүйелерді және қолданбаларды қауіпсіздік осалдықтарын жою үшін үнемі жаңартып отыру өте маңызды.

Интернетте деректерді қауіпсіз беру үшін VPN (Virtual Private Network) және HTTPS (Hypertext Transfer Protocol Secure) протоколдарын қолдану ұсынылады 11. VPN жеке желі арқылы интернетке қауіпсіз қосылуды қамтамасыз етеді, ал HTTPS веб-сайттар мен пайдаланушы арасындағы деректерді шифрлайды 74. Wi-Fi желісінің қауіпсіздігін күшейту үшін шифрлауды (WPA3 немесе WPA2) қосу, SSID хабар таратуын өшіру, MAC-мекенжайларды сүзу және күрделі құпия сөздерді пайдалану қажет 3.

### ӘЛЕУМЕТТІК ЖӘНЕ ҰЙЫМДАСТЫРУШЫЛЫҚ ШАРАЛАР

Киберқауіпсіздіктің маңызды аспектісі – пайдаланушылардың киберсауаттылығын арттыру. Интернет қауіптері туралы хабардар болу және қауіпсіз онлайн мінез-құлық ережелерін үйрену әрбір пайдаланушы үшін өте маңызды. Күдікті әрекеттерден сақ болу, белгісіз сілтемелерді баспау, күдікті хабарламаларға жауап бермеу және жеке деректерді тек сенімді сайттарда енгізу қажет. Жеке деректерді қорғау ережелерін сақтау, мысалы, жеке ақпаратты әлеуметтік желілерде жарияламау, екі факторлы аутентификацияны қолдану және деректерді шифрлау да маңызды рөл атқарады .

**КЕСТЕ 1: ИНТЕРНЕТ ҚАУІПТЕРІНІҢ ТҮРЛЕРІ**

|  |  |  |
| --- | --- | --- |
| **Қауіп түрі** | **Сипаттамасы** | **Ықтимал зардаптары** |
| **Зиянды бағдарламалар (Malware)** | Вирустар, құрттар, трояндар, шпиондық бағдарламалар | Деректерді жою, ұрлау, құрылғыны істен шығару |
| **Фишинг (Phishing)** | Жалған хабарламалар арқылы құпия ақпаратты алу | Қаржылық шығындар, жеке басын ұрлау |
| **Кибершабуылдар (Cyberattacks)** | Желілерге, жүйелерге рұқсатсыз кіру немесе жұмысын бұғаттау | Қаржылық шығындар, беделдің түсуі, жұмыстың тоқтауы |
| **Алаяқтық (Fraud)** | Интернет арқылы ақша немесе басқа құндылықтарды заңсыз иемдену | Қаржылық шығындар, жеке басын ұрлау |

**КЕСТЕ 2: ИНТЕРНЕТ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ**

|  |  |  |
| --- | --- | --- |
| **Шара түрі** | **Әдіс** | **Мақсаты** |
| **Техникалық** | Күрделі құпия сөздер | Рұқсатсыз кірудің алдын алу |
| **Техникалық** | Екі факторлы аутентификация | Аккаунттардың қауіпсіздігін арттыру |
| **Техникалық** | Антивирус және брандмауэр | Зиянды бағдарламалар мен желілік шабуылдардан қорғау |
| **Техникалық** | Бағдарламалық жасақтаманы жаңарту | Қауіпсіздік осалдықтарын жою |
| **Техникалық** | VPN және HTTPS | Деректерді шифрлау және қауіпсіз байланыс |
| **Техникалық** | Wi-Fi қауіпсіздігін күшейту | Сымсыз желілерді рұқсатсыз кіруден қорғау |
| **Әлеуметтік-ұйымдастырушылық** | Киберсауаттылықты арттыру | Қауіптер туралы хабардар ету және қауіпсіз мінез-құлықты үйрету |
| **Әлеуметтік-ұйымдастырушылық** | Күдікті әрекеттерден сақ болу | Алаяқтық пен шабуылдардан аулақ болу |
| **Әлеуметтік-ұйымдастырушылық** | Жеке деректерді қорғау ережелерін сақтау | Жеке ақпараттың құпиялылығын қамтамасыз ету |

## ИНТЕРНЕТ ҚАУІПСІЗДІГІНДЕГІ ЗАМАНАУИ ТРЕНДТЕР

Интернет қауіпсіздігі саласындағы заманауи трендтердің бірі – жасанды интеллектің (ЖИ) рөлінің артуы . ЖИ киберқауіпсіздікте қос рөл атқарады: ол кибершабуылдарды анықтау және алдын алу үшін тиімді құрал бола алады, сонымен қатар киберқылмыскерлердің өз шабуылдарын жетілдіру үшін пайдалануы мүмкін.

2024-2025 жылдарға болжамды киберқауіпсіздік қауіптеріне фишингтің күрделенуі, ransomware шабуылдарының өсуі және «заттар интернетінің» (IoT) құрылғыларына бағытталған қауіптер жатады. Киберқылмыскерлердің әдістері мен құралдары үнемі жетілдіріліп отырады, сондықтан пайдаланушылар мен ұйымдар әрдайым қырағы болып, қорғаныс шараларын үнемі жаңартып отыруы қажет.

## ҚОРЫТЫНДЫ

Интернет қауіпсіздігі қазіргі цифрлық әлемдегі әрбір пайдаланушы мен ұйым үшін өмірлік маңызды мәселе болып табылады. Жеке және қаржылық деректерді қорғау, киберқылмыстың алдын алу және онлайн әрекеттердің қауіпсіздігін қамтамасыз ету – басты міндеттердің бірі. Интернеттегі қауіпсіздікті қамтамасыз ету үшін күрделі құпия сөздерді қолдану, екі факторлы аутентификацияны қосу, антивирустық бағдарламаларды пайдалану, бағдарламалық жасақтаманы жаңарту, VPN мен HTTPS-ті қолдану, Wi-Fi желісінің қауіпсіздігін күшейту және киберсауаттылықты арттыру сияқты шараларды жүйелі түрде орындау қажет. Бұл шаралар қазіргі заманғы киберқауіптерден қорғанудың негізі болып табылады және әрбір интернет пайдаланушысының күнделікті әрекетінің бір бөлігіне айналуы тиіс.