# WI-FI ЖӘНЕ БАСҚА ЖЕЛІЛЕРДІҢ ҚАУІПСІЗДІГІ

**КІРІСПЕ**

Қазіргі заманда ақпараттық технологиялардың қарқынды дамуы желілердің, әсіресе Wi-Fi және басқа да сымсыз байланыс түрлерінің күнделікті өміріміздегі маңызын еселеп арттырды. Ақпараттық қауіпсіздік ұғымы мемлекеттік ақпараттық ресурстардың, жеке тұлғалардың құқықтары мен қоғам мүдделерінің ақпарат саласында қорғалуын білдіреді . Бұл тұрғыда желілік қауіпсіздік компьютерлік желілерді түрлі қауіп-қатерлерден, соның ішінде мақсатты шабуылдар мен зиянды бағдарламалардан қорғауға бағытталған шаралар кешенін қамтиды .

Wi-Fi желіге қосылудың негізгі технологиясы ретінде бүгінгі таңда кеңінен қолданылады . Интернет біздің күнделікті өміріміздің ажырамас бөлігіне айналды, әлеуметтік медиа, электрондық коммерция және түрлі онлайн қызметтер арқылы біз үздіксіз байланыстамыз . Желілердің маңызы бизнес, білім беру және басқа да көптеген салаларда өте зор . Киберқауіпсіздік бизнестен бастап мобильді технологияларға дейін әртүрлі қолданыс аяларын қамтиды . Осыған байланысты Wi-Fi және басқа желілердің қауіпсіздігін қамтамасыз ету әрбір пайдаланушы мен ұйым үшін өзекті мәселе болып табылады.

Бұл дәрістің мақсаты – желілік қауіпсіздік мәселелері туралы түсінік беру және олардан қорғану жолдарын көрсету. Дәріс барысында Wi-Fi желісінің қауіпсіздігі, сымды, ұялы және Bluetooth желілерінің қауіпсіздігі, сондай-ақ желілік қауіпсіздіктің жалпы үздік тәжірибелері қарастырылады.

**WI-FI ЖЕЛІСІНІҢ ҚАУІПСІЗДІГІ**

Wi-Fi (/waɪˌfaɪ/) – бұл IEEE 802.11 стандартының негізінде құрылған сымсыз желілер үшін Wi-Fi Alliance-нің тіркелген сауда белгісі. Wi-Fi термині "сымсыз адалдық" деген мағынаны білдіреді. Wi-Fi желісінің жұмыс істеу принципі IEEE 802.11 стандартының ресми құжаттарында толығырақ сипатталған. Сымсыз технология болғандықтан, Wi-Fi желілерінің қауіпсіздігі сымды желілерге қарағанда ерекше назар аударуды қажет етеді, себебі деректер ауа арқылы таралады және қолжетімділік аясы кеңірек болады.

Wi-Fi желілері әртүрлі осалдықтар мен қауіптерге ұшырауы мүмкін. Егер сымсыз желі дұрыс қорғалмаса, рұқсатсыз кіру орын алуы мүмкін. Бұл жағдайда желіге қосылған кез келген адам сіздің интернет трафигіңізді бақылап, жеке файлдарыңызды ұрлай алады . Деректерді ұстап қалу қаупі де бар. Әсіресе ашық Wi-Fi желілерінде бұл қауіп жоғары, өйткені хакерлер сіздің құпия ақпаратыңызды, мысалы, құпия сөздер мен несие карталарының мәліметтерін оңай көре алады .

Зиянды бағдарламалық жасақтаманың таралуы да Wi-Fi арқылы мүмкін . Шабуылдаушылар зақымдалған пакеттер немесе қауіпті сілтемелер арқылы сіздің құрылғыңызға зиянды бағдарламаларды орната алады . "Evil Twin" деп аталатын шабуылдар кезінде хакерлер заңды желіге ұқсас жалған Wi-Fi нүктелерін жасайды. Пайдаланушылар білместікпен осы жалған желілерге қосылып, өз деректерін ұрлатуы мүмкін. "Man-in-the-Middle" шабуылдары – ең қауіптілерінің бірі, мұнда шабуылдаушы сіз бен Wi-Fi маршрутизаторының арасына кіріп, деректер ағынын ұстайды . Бұдан басқа, қызмет көрсетуден бас тарту шабуылдары (DDoS) және құпия сөзді бұзу шабуылдары (Brute Force) , сондай-ақ пакеттерді иіскеу (Packet Sniffing) сияқты қауіптер де бар.

Wi-Fi желісінің қауіпсіздігін қамтамасыз ету үшін бірқатар шараларды қолдану қажет. Ең алдымен, күрделі құпия сөздерді пайдалану маңызды. Құпия сөздер әріптердің, сандардың және арнайы белгілердің комбинациясынан тұруы керек. Шифрлауды қосу да қажет. WPA3 - ең қауіпсіз шифрлау түрі болып саналады. VPN (виртуалды жеке желі) пайдалану арқылы интернет қосылымын шифрлауға болады, бұл хакерлердің деректеріңізді ұстап алуын қиындатады. Брандмауэрді пайдалану кіріс және шығыс желілік трафикті бақылауға көмектеседі және күдікті әрекеттерді бұғаттайды. SSID хабар таратуын өшіру желінің атауын жасырады, бірақ бұл толық қауіпсіздікті қамтамасыз етпейді. MAC мекенжайын сүзу арқылы желіге қосылуға рұқсат етілген құрылғыларды шектеуге болады, алайда MAC мекенжайын жасыруға болатындығын ескеру қажет . Қонақ желісін орнату негізгі желіңізді қорғау үшін бөлек желі жасайды . Құрылғылардағы әдепкі құпия сөздерді өзгерту , қашықтан басқаруды өшіру және WPS өшіру де қауіпсіздікті арттыруға көмектеседі. Файлдарды ортақ пайдалануды абайлап пайдалану керек және қажет болмаған жағдайда өшіру қажет 8. Қауіпсіз браузерді таңдау және екі факторлы аутентификацияны қосу қосымша қорғаныс шаралары болып табылады. Бағдарламалық құралды үнемі жаңарту қауіпсіздік осалдықтарын жою үшін өте маңызды. Қоғамдық Wi-Fi желілерінде абай болу керек және құпиялы әрекеттерді орындамау қажет . HTTPS веб-сайттарын пайдалану және күдікті сілтемелер мен электрондық пошталардан сақ болу да маңызды.

**1-кесте: Wi-Fi қауіптері және оларды болдырмау жолдары**

|  |  |  |
| --- | --- | --- |
| **Қауіптің атауы (Threat Name)** | **Қысқаша сипаттамасы (Brief Description)** | **Болдырмау жолдары (Ways to Prevent)** |
| Рұқсатсыз кіру (Unauthorized Access) | Желіге рұқсатсыз қосылу. | Күрделі құпия сөздерді пайдалану, MAC мекенжайын сүзу. |
| Деректерді ұстап қалу (Data Interception) | Желі арқылы берілетін деректерді рұқсатсыз көру. | Шифрлауды қосу (WPA3, WPA2), VPN пайдалану. |
| Зиянды бағдарламалық жасақтаманың таралуы (Malware Distribution) | Желі арқылы зиянды бағдарламаларды тарату. | Брандмауэрді пайдалану, күдікті сілтемелерден аулақ болу, антивирус орнату. |
| "Evil Twin" шабуылдары (Evil Twin Attacks) | Заңды желіге ұқсас жалған Wi-Fi нүктелерін құру. | Қосылатын желілерді тексеру, VPN пайдалану. |
| "Man-in-the-Middle" шабуылдары (Man-in-the-Middle Attacks) | Пайдаланушы мен сервер арасындағы деректерді ұстау. | VPN пайдалану, HTTPS сайттарын қолдану. |
| Қызмет көрсетуден бас тарту (Denial of Service) | Желі ресурстарына қол жеткізуді қиындату. | Брандмауэрді конфигурациялау, трафикті бақылау. |
| Құпия сөзді бұзу (Brute Force Attack) | Құпия сөзді қайталау арқылы табу әрекеті. | Күрделі құпия сөздерді пайдалану, құпия сөзді ауыстыру саясатын енгізу. |
| Пакеттерді иіскеу (Packet Sniffing) | Желі трафигін бақылау және талдау. | Шифрлауды қосу (WPA3, WPA2), VPN пайдалану. |

**БАСҚА ЖЕЛІЛЕРДІҢ ҚАУІПСІЗДІГІ**

Сымды желілер, әдетте, сымсыз желілерге қарағанда қауіпсіз саналады, бірақ олар да қауіпсіздік шараларын қажет етеді. Физикалық қауіпсіздік маңызды, рұқсатсыз физикалық кіруді болдырмау керек . 802.1X аутентификациясын пайдалану , желіні сегменттеу , брандмауэрлер мен кіруді басқару тізімдерін пайдалану , шифрлауды пайдалану , күшті құпия сөздерді пайдалану және бағдарламалық жасақтаманы жаңарту , сондай-ақ кіруді бақылау сымды желілердің қауіпсіздігін қамтамасыз етуге көмектеседі.

Ұялы желілердің қауіпсіздігі көбінесе құрылғыны қорғауға және әлеуметтік инженерия шабуылдарына қарсы тұруға бағытталған . Фишингтік әрекеттерден сақ болу , қауіпті қолданбалардан аулақ болу , құрылғыны құлыптау және құпия сөзбен қорғау , бағдарламалық жасақтаманы жаңарту , қоғамдық Wi-Fi пайдаланғанда VPN қолдану және жеке деректерді абайлап бөлісу ұялы желілерді қауіпсіз пайдалануға мүмкіндік береді.

Bluetooth қауіпсіздігі құрылғылардың көрінуін және жұптастыруын мұқият басқаруды қамтиды, рұқсатсыз кіру мен деректерді ұрлаудың алдын алу үшін . Құрылғыларды жұптастыру кезінде абай болу , Bluetooth-ты пайдаланбаған кезде өшіру 76, күшті PIN кодтарын пайдалану , бағдарламалық жасақтаманы жаңарту , "анықтау" режимін өшіру және құпия ақпаратты Bluetooth арқылы бөлісуден аулақ болу қауіпсіздікті қамтамасыз етеді.

**ЖЕЛІЛІК ҚАУІПСІЗДІКТІҢ ЖАЛПЫ ҮЗДІК ТӘЖІРИБЕЛЕРІ**

Желілік қауіпсіздіктің тиімді стратегиясы техникалық бақылауды ұйымдық саясатпен және пайдаланушылардың хабардарлығымен үйлестіреді. Бағдарламалық жасақтаманы үнемі жаңарту белгілі осалдықтарды жойып, деректерді жоғалту қаупін азайтады. Күдікті әрекеттерден сақ болу және аномальды желі трафигін бақылау қауіпсіздік инциденттерін ерте анықтауға көмектеседі. Қол жеткізуді басқару және құпия сөз саясаты сияқты қауіпсіздік саясатын енгізу адам қателігі мен ішкі қауіптердің ықтималдығын азайтады. Брандмауэрді пайдалану және деректердің сақтық көшірмесін жасау белсенді қорғаныс механизмдерін қамтамасыз етеді және деректерді қалпына келтіруге мүмкіндік береді. Вирусқа қарсы бағдарламалық жасақтаманы пайдалану және екі факторлы аутентификацияны пайдалану қосымша қорғаныс қабаттарын жасайды. Қызметкерлерді киберқауіпсіздік қағидалары бойынша оқыту адам қателігінің тәуекелін азайтады. Желі трафигін шифрлау VPN және HTTPS арқылы деректердің құпиялылығын қамтамасыз етеді. Интрузияны анықтау және алдын алу жүйелерін енгізу белсенді қауіпсіздік шаралары болып табылады.

**2-кесте: Желілік қауіпсіздіктің үздік тәжірибелері**

|  |  |
| --- | --- |
| **Үздік тәжірибе (Best Practice)** | **Қысқаша түсіндірмесі (Brief Explanation)** |
| Бағдарламалық жасақтаманы үнемі жаңарту | Белгілі осалдықтарды жою және қауіпсіздікті арттыру. |
| Күдікті әрекеттерден сақ болу | Аномальды әрекеттерді анықтау және қауіпсіздік инциденттеріне тез әрекет ету. |
| Қауіпсіздік саясатын енгізу | Ұйымдағы барлық пайдаланушылар үшін қауіпсіздік стандарттарын белгілеу. |
| Брандмауэрді пайдалану | Желі трафигін бақылау және рұқсатсыз кіруді бұғаттау. |
| Деректердің сақтық көшірмесін жасау | Ақпаратты жоғалтудан қорғау және қажет болған жағдайда қалпына келтіру. |
| Вирусқа қарсы бағдарламалық жасақтаманы пайдалану | Зиянды бағдарламалар мен вирустардан қорғану. |
| Екі факторлы аутентификацияны пайдалану | Қол жеткізуді растаудың қосымша қабатын қамтамасыз ету. |
| Қызметкерлерді оқыту | Пайдаланушылардың киберқауіпсіздік тәуекелдері туралы хабардарлығын арттыру. |
| Желі трафигін шифрлау | Деректердің құпиялылығын қамтамасыз ету. |
| Интрузияны анықтау және алдын алу жүйелерін енгізу | Желіге жасалған шабуылдарды анықтау және бұғаттау. |

**ҚОРЫТЫНДЫ**

Қазіргі цифрлық әлемде желілік қауіпсіздіктің маңызы күннен-күнге артып келеді. Қауіптердің өсуі жеке және ұйымдық деректерді қорғаудың қажеттілігін тудырады . Деректердің бұзылуының салдары ауыр болуы мүмкін . Кибершабуылдардың зардаптары жеке адамдарға да , ұйымдарға да әсер етеді , тіпті психологиялық зардаптарды да қамтуы мүмкін . Ұйымдар үшін кибершабуылдар қаржылық және беделдік шығындарға әкелуі мүмкін . Желілік қауіпсіздік бұзушылықтарының мысалдары өте көп .

Болашақта желілік қауіпсіздікке төнетін қауіптер де арта түсуде . Киберқауіпсіздік технологияларының дамуы , жасанды интеллектің рөлінің артуы және жаңа шабуыл түрлерінің пайда болуы мобильді қауіпсіздікке көбірек көңіл бөлу қажеттілігін көрсетеді .

Қорыта келе, желілік қауіпсіздікке әрқашан сақ болып, білімді болу маңызды. Қауіпсіздікті басымдыққа қою арқылы біз өзімізді және ұйымдарымызды киберқауіптерден қорғай аламыз.