bilimger.kz
Республикалық білім және ғылым порталы
https://bilimger.kz
ҚР Мәдениет және Ақпарат министрлігі тіркелген — Куәлік нөмірі:
KZ45VPY00102718
2018

БӨЛІМ: ИНФОРМАТИКА

Желідегі қауіпсіздік

ЖАРИЯЛАНДЫ
09.12.2018

СІЛТЕМЕ
https://bilimger.kz/46102/

АННОТАЦИЯ / АҢДАТПА

Пәні:	Информатика	
Мұғалімі: **Күні**	Сапарбаева Үлбір Мәлікқызы 15.10.2018 жыл	
Сынып	8 сынып	
Сабақтың тақырыбы	***Желідегі қауіпсіздік***	
Жалпы мақсаты	Тақырыпты Блум таксономиясы арқылы сыни тұрғыдан игере отырып, оқушылар компьютерлік желілерде ақпараттық қауіпсіздік түрлеріне тоқталып, ақпараттың қорғалу жолдарымен танысады.	
Түйінді идеясы	• Білімді болу деген – жаңалық ашуға қабілетті болу. ***Әбу Насыр Әл Фараби***	
Оқушылар үшін оқу нәтижелері	Компьютерлік желілерде ақпараттық қауіпсіздікті сақтау, ақпаратты қорғау ұғымдарымен танысып, білімдерін бекітеді. Топпен жұмыс істеп идея бөліседі. Бір-бірін тыңдайды, кеңес береді. Шығармашылық тапсырмамен жұмыс жасайды.	
Сабақта қолданылатын материалдар	А4 қағаз, АКТ, стикерлер.	
Оқыту әдістері	Блум таксономиясы алты ойлау деңгейі. Оқушылардың өзара белсенділігін арттырып қызығушылығын ояту.	
Дерек көздері	Слайдтар, қосымша материалдар. www.bilimland.kz сайты.	
Тапсырмалар	Мұғалімнің іс-әрекеті	
3 мин5мин ***7 мин*** ***15 мин*** ***5 мин*** ***7 мин*** ***3 мин***	• Ұйымдастыру. Топқа бөлу. • Тапсырма №1. «Миға шабуыл» әр түрлі сұрақтар арқылы оқушылардың білім деңгейін тексеру. • Тапсырма №2. Жаңа сабақ. Бейне жазба арқылы түсінеді. • Тапсырма №3. Топпен жұмыс тақырыпты ашу. • Тапсырма №4. Салыстырмалы талдау жасау. • Тапсырма №5. Сұрақ Жауап • Үйге тапсырма.Ақпаратты қорғау саласындағы ҚР заңнамасымен танысу.	
Тапсырмалар:		Оқушының іс-әрекеті

Білу	Ашық, жабық сұрақтар	1) Қандай қауіпсіздік ережелерін білеміз?2)ДК-де жұмыс істеу алдында және аяқтау кезінде қандай қауіпсіздік ережелерін сақтау керек? 3)ДК-мен жұмыс кезіндегі қандай қауіпсіздік ережелерін сақтау керек? 4)Аппаттық жағдайларда қандай қауіпсіздік ережелерін білеміз? 5)Аппаттық жағдайда алғашқы көмек көрсету түрлерін білеміз? 6)Көзге арналған жаттығулардың түрлері қандай?
Түсіну	Оқушыларға бейне жазба көрсетіледі	Оқушылар бенежазбадан көргендерін, түсінгендерін бір-бірімен пікірталастырады.
Қолдану	Топпен жұмыс. Қосымша материал үлестіріледі. Постер қорғау	1-ТопА-деңгейі жеке жұмыс В-деңгейі сөздікпен жұмыс С-деңгейі Фишинг және желі құрттары дегеніміз не? 2-топ А-деңгейі жеке жұмыс В-деңгейі сөздікпен жұмыс С-деңгейі деректерді қалай қорғаймыз 3-топ А-деңгейі жеке жұмыс В-деңгейі сөздікпен жұмыс С-деңгейі компьютер қауіпсіздігінің негізгі жолдарына не жатады?
Талдау	Желіде ақпаратты қорғау керекпа? Ақпараттық қауіпсіздік қалай қамтамасыз етіледі?	Салыстырмалы талдау жасау
Жинақтау	Өткен тақырыптан білімдерін жинақтайды.	Тест тапсырмасы www.bilimland.kz сайты.
Бағалау	Тақырыптың өзектілігіне баға беру. Ой жинақтау. Сұраққа жауап беру арқылы.	Компьютерлік желіде ақпараттық қауіпсіздіктің ерекшелігіне маңыздылығына баға береді. Өз ойын айтуға дағдыланады.Сұраққа жауап беру арқылы.
Кері байланыс	Рефлексия	*Мен бүгін .....Маған .....* *Мен үшін.....* *Егер де мен.....* *Алдағы уақытта.....*

Жеке жұмыс:

Жауабы:

Қосымша ақпарат

Компьютер қаіупсіздігінене келгенде, қауіптер, талдаулары, залалдар түрлері қауіпсіздік саясаты сияқты көптеген аспектерге назар аударып содан кейін қорғау әдістеріне оралғаныңыз жөн.

Вирустар, кейлогерлер, фишинг пен **компьютерлік құрттар** шабуылдары жүйеңіздің барлық бөлігінде закымдау үшін болады, бірақ жүйеңіздің қауіпсіздігін қамтамасыз ете алатын жолдар бар.

Компьютер қауіпсіздігінің негізгі жолдарына мыналар кіреді:

- Тексеретін және вирустар туралы ескертіп отыратын вирусқа қарсы

бағдарламалар.

- Жүйе мен интернет арасында ақпарат тасымалдауға мүмкіндік беруге баптау жасалған сіздің жүйеңіздің брандмауэрі. (Microsoft Windows-те алдын-ала орнатылған, қауіпсіздік сақтау үшін арналған арнайы бағдарлама).
- Вирустық шабуылдар зардабынан жоғалған файлдарды қалпына келтіруге көмектесетін болғандықтан, резервтік көшірме маңызды файлдар мен құжаттарыңызды қорғаудың тағы бір жолы болып табылады (резервтік көшірме, ақпаратты сақтау үшін қосымша жер алады).

Деректеріңізге арналған негізгі қауіпсіздік операцияларынан басқа, мұнда есіңіздесақтау қажет бірнеше негізгі аспекттер бар. Олар мыналар:
Зиянды бағдарламалардың белгіерін анықтап, қажетті шараларды қолданыңыз
Вирусқа қарсы бағдарламаңыздың вирустық дерекқорын жаңартып отырыңыз
Жүйеңізді аптасына бір рет жаңа ақауларды іздеу үшін тексеріп тұрыңыз
Жеке ақпаратты сұрайтын электрондық пошталардан сақ болыңыз
Деректерді тасымалдау үшін пайдаланатын USB құрылғыларын тексеріңіз

Веб-шолғыш пен операциялық жүйені жаңартып отырыңыз
Жүйеңізде ортақ пайдалану мен файл қауіпсіздігі деңгейін пайдалануды және бумалар мен дерек файлдары үшін рұқсат алуды орнатуды ұмытпаңыз. Жуйеңізді басқа біреумен ортақ пайдалану жағдайында файл деңгейінде рұқсаттарды пайдаланған жөн. Кейбір қолданбалар сізге жеке құжаттар үшін құпия сөз орнатуға мүмкіндік береді EFS шифрлауы жүйе деректерін қорғаудың басқа бір жолы және оны жасау өте оңай, осы қорғаныстыіске қосу үшін ұяшық белгісін таңдасаңыз жетіп жатыр.
Үшінші тарап бағдарламаларының кейбіреулері жүйеңіздің бүкіл дискісін шифрлауға мүмкіндік береді. Бұл шифрлау түрі бүкіл құжаттардың жартысын немесе дискң жетегңн құлыптайды. Егер интернетті жиі пайдаланатын болсаңыз және деректертеріңізді интернет аркылы тасымалдайтын болсаңыз, онда IP қауіпсіздігі опциясын таңдағаньңыз жөн. Дегенмен де бұл тек қабылдау және жіберу жүйелері де мұндай қауіпсіздікке қолдау көрсететін болса көмектеседі. Деректерді сымсыз желілер арқылы жіберуді қорғау маңызды болып табылады, өйткені мұндай деректер хакерлер тарапынан зақымдалуға немесе фишинг әрекетіне ұшырауға жақын, сондықтан шифрлауы бар желтерді пайдалануыңыз қажет.

Сөздік

Акпараттық қауіпсіздік — мемкелеттік ақпараттың ресурстардың, сондай-ақ ақпарат саласында жеке адамның құқыктары мен қоғам мүдделері қорғалуының жай-күйі.

Антивирусттік бағдарлама — вирустармен күресуге арналған арнайы бағдарлама.
Вирус — басқа программалар мен файлдарға өз көшірмесін автоматты түрде кірістіре

отырып, файддарды «Бүлдіретін» компьютерлік шағын бағдарлама (1-2 Кб) немесе макрос. Зақымданған мәліметтерді жедел жадқа жүктеуде онда орналасқан басқа файлдарға өтіп, оларға да зақым келтіре алады.

Желі құрттары — өз бетімен жергілікті немесе ғаламдық компьютер желісімен таралатын зиянды бағдарламалар түрі.

Компьютерлік вирус — компьютердің қалыпты жұмыс істеуіне зиян келтіріп, өз бетімен көбейетін бағдарлама.

Кейлогер, кейлоггер (ағыл. keylogger, окылуы «ки-логгер» — ағыл. key – кілт және logger — тіркеу құрылғысы) — бұл пайдаланушының түрлі іс-әрекетін (мысалы,компьютер пернетақтасындағы батырмаларды басу,тінтуірді пайдаланып т.с.с.) тіркеп отыратын компьютерлік құрылғы немесе бағдарламалық жасақтама.

Хакер (агылш. hack деген сөзінен) — әлемдегі ең ірі әрі күрделі саналатын компьютерлік желілерге кіруге қолжеткізген, өзінің электрондық саладағы білімін жаңа идеялар енгізу арқылы дәлелдейтін және де технологияның даму мәдениетін егжей-тегжейлі білетін адамды айтады. Алайда көпшілік үшін кандай да бір электрондык жүйеге заңсыз шабуыл жасаған адам біздің қоғамда «хакер» деген атка ие болтан.

Фишинг — сенім білдіруге болатын дереккөзі ретінде бүркену арқылы пайдаланушы аттары, құпия сөздер мен кредиттік карталарының мәліметтері сияқты маңызды ақпаратты алу талпынысы.

Encrypting File System (EFS) — Microsoft Windows NT (Windows 2000 бастап жоғары қарай) операциялык жүйелері деп файлдардың деңгейінде шифрлауды жүзеге асыратын, мәліметтерді шифрлау жүйесі

IP қауіпсіздігі (IPsec) – желі аралық IP протоколы арқылы жіберілетін мәліметтердің қауіпсіздігін қамтамасыз ететін протоколдар жиынтығы.