ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ЦИФРЛЫҚ ДАМУ, ИННОВАЦИЯЛАР ЖӘНЕ АЭРОҒАРЫШ ӨНЕРКӘСІБІ МИНИСТРЛІГІНІҢ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІ

КИБЕР-ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

ҰСЫНЫМДАР

КИБЕР-ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

ҰСЫНЫМДАР

Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитетінің тапсырысы бойынша халықтың ақпараттық қауіпсіздікке (киберқауіпсіздікке) төнетін қатерлер туралы хабардар болу деңгейін айқындау мақсатында 2022 жылғы қазаннан бастап қарашаға дейін халық арасында әлеуметтік зерттеу жүргізілді.

Зерттеу барысында мыналар қамтылды:

18 жастағы және одан асқан тұрғындар арасында.

Сауалнама нәтижелерін талдай отырып, бүгінгі таңда ақпараттық қауіпсіздік қатері Қазақстан Республикасындағы өзекті мәселе болып табылатынын атап өтуге болады. Ақпараттық қауіпсіздік (киберқауіпсіздік)қатерлері туралы халықтың хабардар болу көрсеткіштері

АҚПАРАТТЫҚ КЕҢІСТІКТІ ҚОРҒАУДА

Қазақстанда ақпараттық қауіпсіздік саласын дамыту мәселелеріне айтарлықтай көңіл бөлінеді. Мемлекеттік органдар, үкіметтік емес ұйымдар және бизнес бірлесіп жүргізген жұмыстың нәтижесі - бұл біздің еліміз киберқауіпсіздіктің жаһандық индексінде өз позициясын тез жақсартатын соңғы жылдардағы үрдіс. Қазір Қазақстан онда 31-ші орында. Бұл рейтингте ҚХР, Дания, Хорватия, Словакия, Израиль және Швейцария сияқты елдерді басып озды.

Осы жылдар ішінде елімізде киберқауіпсіздік саласын дамытудың негізгі тұжырымдамалық тәсілдері әзірленді. 2022 жылға дейін киберқауіпсіздік тұжырымдамасы ("Қазақстанның киберқалқаны") бекітілді.

Қазақстан Республикасы Мемлекет басшысының тапсырмасы бойынша цифрлық экожүйені дамытудың 2023 - 2027 жылдарға арналған жаңа тұжырымдамасы («Киберқалқан - 2») әзірленді.

Ақпараттық қауіпсіздік («киберқауіпсіздік») саласын дамыту мақсатында бірқатар заңнамалық актілер мен салалық ведомстволық актілер күшіне енді. Бұдан басқа, ақпараттық қауіпсіздік саласында сынақ зертханалары құрылды, ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы іске қосылды, ақпараттық қауіпсіздіктің мемлекеттік жедел орталығы, ақпараттық қауіпсіздіктің салалық жедел орталығы құрылды, компьютерлік инциденттерге ден қоюдың 3 қызметі бар, ақпараттық қауіпсіздіктің 35 жедел орталығы құрылды, 3 бейінді қоғамдық ұйым бар, саладағы 50 отандық компания жұмылдырылды ақпараттық қауіпсіздік, ақпараттық қауіпсіздік және т. б. мамандығы бойынша білім беру гранттарының саны артты.

НЕЛІКТЕН КИБЕРҚАУІПСІЗДІКТІ САҚТАУ МАҢЫЗДЫ?

Социологиялық зерттеу негізінде дайындалған

Ақпараттық қауіпсіздікті қамтамасыз ету және дербес деректерді қорғау ақпараттық қауіпсіздік комитеті атынан уәкілетті орган жұмысының маңызды құрамдас бөлігі болып табылады

«АҚПАРАТТЫҚ ҚАУІПСІЗДІК (КИБЕРҚАУІПСІЗДІК) ҚАТЕРЛЕРІ ТУРАЛЫ ХАЛЫҚТЫҢ ХАБАРДАРЛЫҒЫ»

“Жаһандық киберқауіпсіздік индексінде (GCI) Қазақстан өз позициясын тез жақсартуда. Мысалы, 2019 жылы Қазақстан бірден *42 пунктке — 40 орынға көтерілді. 2021 жылғы 29 маусымда соңғы есепте Қазақстан 31-орынға жайғасты, күтілетін нәтижеден едәуір асып, былтырғы рейтингпен салыстырғанда 9 тармаққа жоғары көтерілді*. Бұл мемлекеттік органдардың, үкіметтік емес ұйымдардың және бизнестің *бірлескен жұмысының нәтижесі*”

КЕЙБІР МАҢЫЗДЫ АҚПАРАТ

Ақпараттық қауіпсіздік біздің өміріміздің ажырамас бөлігі болып табылады. Ақпараттық қауіпсіздік дегеніміз, әдетте, үш маңызды қағиданы сақтау:

Құпиялылық

Қол жетімділік

Тұтастық

Бұл дегеніміз не?

- *Ақпаратқа тек оған құқығы бар адам ғана қол жеткізуі керек.*
- *Ақпарат қажет болған кезде қол жетімді болуы керек.*
- *Ақпарат сенімді болуы керек.*

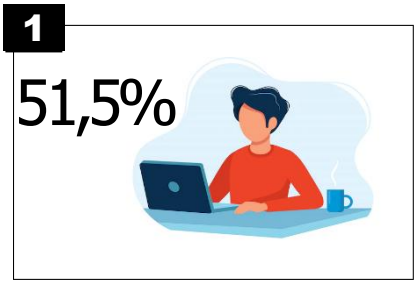
Принциптердің бірін бұзу басқалардың бұзылуына әкелуі мүмкін.

ДЕРЕКТЕР ҚАУІПСІЗДІГІНЕ ТӨНЕТІН ҚАУІП

Ақпараттандыру саласындағы ақпараттық қауіпсіздік (киберқауіпсіздік) - электрондық ақпараттық ресурстардың, ақпараттық жүйелер мен ақпараттық - коммуникациялық инфрақұрылымның сыртқы және ішкі қауіптерден қорғалу жағдайы.

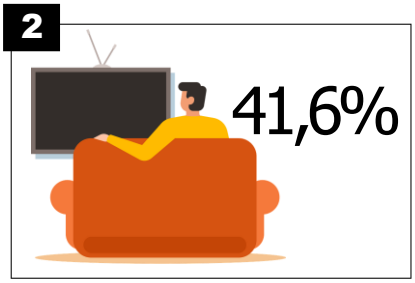
СОЦИОЛОГИЯЛЫҚ САУАЛНАМАНЫҢ НӘТИЖЕЛЕРІ КӨРСЕТЕДІ:

1



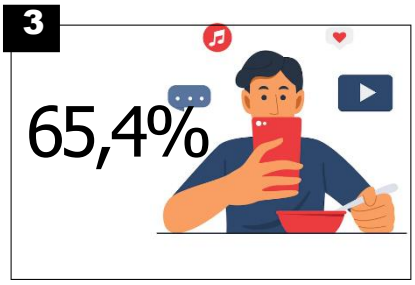
Ақпаратты интернет арқылы алады

2



Теледидар арқылы

3



Мобильді қосымшалар арқылы

Респонденттердің көпшілігі:

ӨТКЕН ЖЫЛЫ СІЗ ҚАНДАЙ КИБЕР-ШАБУЫЛДАРҒА ҰШЫРАДЫҢЫЗ?

Сауалнамаға сәйкес, өткен жылы ел халқы келесі кибершабуылдарға ұшыраған:

	2020	2021	2022
Компьютерлік вирустардың шабуылы	32.1%	16.5%	51.7%
Зиянды спам	13.4%	23.0%	34,5%
Әлеуметтік желі аккаунттарын бұзу	3.9%	14.5%	28.4%

Респонденттердің пікірінше киберқауіпсіздіктің бұзылуына күдік туындаған жағдайда негізгі шара:

-IT-маманға жүгіну — 27,4%

-ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органға жүгіну — 19, 2%

- құқық қорғау органдарына жүгіну — 32,1%

-ешкімге жүгіну — 10,1%

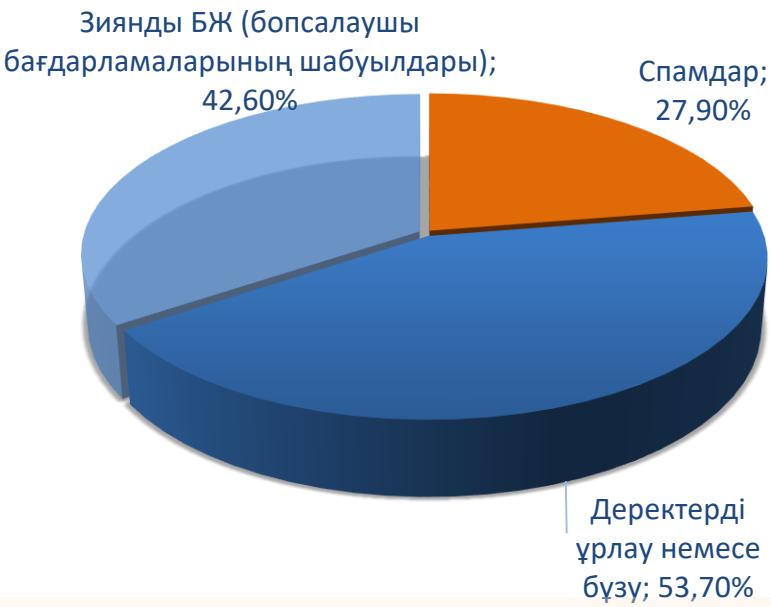
Кез келген стандартты емес немесе ақпараттық қауіпсіздікті бұзуға күдік болған кезде:
- дереу жауапты мамандарға хабарласыңыз;
-сондай-ақ, компьютерлік оқиғаларға жауап беру қызметіне 1400 немесе +7 (7172) 55-99-97, телефон нөмірі бойынша хабарласуға болады:
Эл.пошта:
info@ kz-cert.kz

ИНТЕРНЕТТЕ ЖҰМЫС ІСТЕГЕНДЕ ҚАНДАЙ ҚАУІПСІЗДІК ШАРАЛАРЫН ҚОЛДАНАСЫЗ?

Социологиялық сауалнаманың нәтижелері көрсетеді:

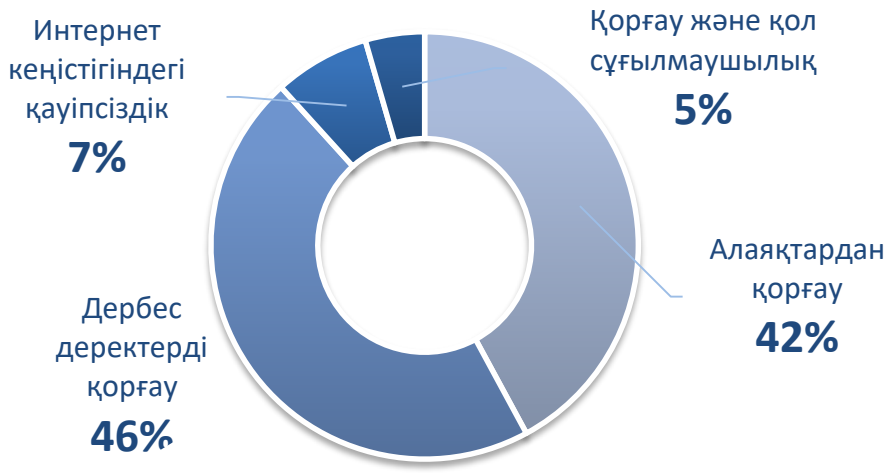
АҚПАРАТТЫҚ ҚАУІПСІЗДІК ПЕН ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУҒА ТӨНЕТІН ҚАУІПТЕРДІҢ БАР ТҮРЛЕРІН БІЛЕСІЗ БЕ?

КИБЕР-ҚАУІПТЕРДІҢ ТҮРЛЕРІ:



Социологиялық сауалнаманың нәтижелері көрсетеді:

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ НЕДЕН ҚАМТАМАСЫЗ ЕТУ КЕРЕК ДЕП ОЙЛАЙСЫЗ:

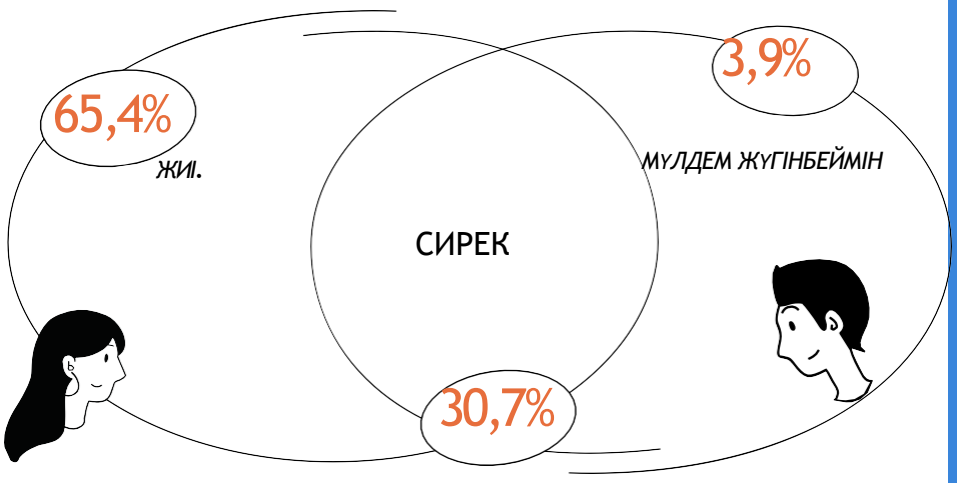


АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ АЛДЫН АЛУ

Ақпараттық қауіпсіздік деректерді, оның ішінде дербес деректерді қорғауды қамтамасыз етудегі негізгі міндеттердің бірі болып табылады және оны арттыру, респонденттердің пікірінше, шаралар қабылдауды талап етеді.

«СІЗ ӘЛЕУМЕТТІК ЖЕЛІЛЕР МЕН МЕССЕНДЖЕРЛЕРДІ ҚАНШАЛЫҚТЫ ЖИІ ҚОЛДАНАСЫЗ?»

Әлеуметтік сауалнама нәтижелері көрсетеді:



РЕСПОНДЕНТТЕР ТІРКЕЛГЕН САЙТТАР ТУРАЛЫ АҚПАРАТТЫ ТЕКСЕРЕ МЕ?

63,1% - Иә, үнемі

Кейде ресурс күмән тудырған кезде - 22,9%

14,0% - Жоқ

ҰСЫНЫМДАР

Ақпараттық қауіпсіздіктің алдын алу (ұсынымдар)

Бағдарламалық жасақтамаға - операциялық жүйелерге, қолданбалы бағдарламаларға, антивирустық бағдарламаларға және басқа бағдарламаларға үнемі жаңартулар орнатыңыз.

Қол жетімді болған кезде бағдарламалық жасақтаманы автоматты түрде жаңарту мүмкіндігін қосыңыз.

Қолданбайтын немесе әзірлеуші жаңартуларын алмаған кезде бағдарламалық жасақтаманы жойыңыз.

Лицензияланбаған бағдарламалық жасақтаманы немесе тексерілмеген көздерден алынған бағдарламалық жасақтаманы орнатудан аулақ болыңыз.

Басқа құрылғыларда сіз үшін маңызды деректердің көшірмесін үнемі жасаңыз.

Зиянды бағдарламалар пайдаланушының компьютеріне қалай енеді ?

Тарату әдістері:

Фишинг

Мақсаты пайдаланушылардың құпия деректеріне (логиндер, парольдер, банк карталарының деректері және т.б.) осы деректерден сырттай ерекшеленбейтін жалған интернет – ресурстар арқылы қол жеткізу болып табылатын интернет - алаяқтықтың бір түрі.

Әлеуметтік инженерия

бұл адамға психологиялық әсер ету арқылы құпия ақпаратты алу тәсілі. Әлеуметтік инженерияның негізгі мақсаты-парольдерге, банктік деректерге және басқа қорғалған жүйелерге қол жеткізу арқылы пайда табу.

Трояндық ат

хатта Сіздің компьютеріңізді жұқтыратын қауіпті тіркеме болған кезде әлеуметтік инженерияның бір түрі.

Ұсынымдар

Зиянды бағдарламалар көбінесе компьютерге енеді:

- ✓ Электрондық пошта арқылы;
- ✓ ақпарат тасығыштар (флеш жинақтауыштар) арқылы;
- ✓ белгісіз сайттардан файлдарды жүктеу кезінде.

Не істеу керек?

Зиянды бағдарламалар көбінесе басқа файлдармен бірге қосымшада таратылады, сондықтан Сізге белгісіз ресурстардан жіберілген электрондық пошта тіркемелерін ашпаңыз.

- ✓ Амалдық жүйенің кіріктірілген брандмауэрін ешқашан өшірмеңіз..
- ✓ Жүйені ықтимал онлайн қауіптерден қорғау үшін антивирустық БЖ пайдаланыңыз. Сенімді көздерден антивирустық және тыңшылыққа қарсы бағдарламаларды орнатыңыз.
- ✓ Флэш - жинақтауыштарды абайлап қолданыңыз. Компьютерді зиянды бағдарламамен жұқтыру мүмкіндігін азайтыңыз: компьютерге белгісіз флэш-жинақтауыштарды (немесе USB жинақтауышты) қоспаңыз..
- ✓ Сізге таныс емес пайдаланушылардан файлдарды қабылдамаңыз, әсіресе EXE, COM, CMD кеңейтімі бар файлдарға назар аударыңыз.

Интернеттегі ақпараттық қауіпсіздік ережелері (ұсыныстар)

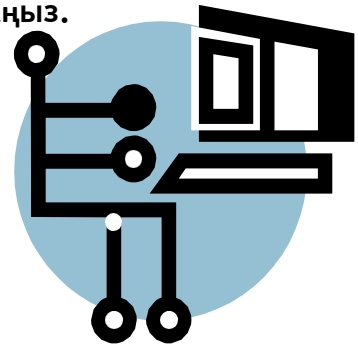
1. Барлық жерде қауіпсіз және әртүрлі құпия сөздерді қолданыңыз. Екі факторлы аутентификацияны және ең үлкен қауіп бар жерде саусақ ізімен салыстыруды таңдаңыз.

.

2. Бейтаныс адамдарға қоңырау шалуға жол бермеңіз. Олар телефонмен қашып қана қоймай, кез келген нәрсені жасай алады.

3. Интернетте сүйікті өзіңіз туралы аз айтыңыз. Эту информацию могут использовать совсем не в хороших и корыстных целях злоумышленники. Бұл ақпаратты зиянкестер жаман және пайдақорлық мақсатта пайдалануы мүмкін.

4. «тегін», «free» «жеңілдік», «тегін және тіркеусіз жүктеу» сөздеріне алдаңбаңыз.



5. Әлеуметтік желілерге немесе поштаға басқа біреудің компьютерінен кіргенде, шығуды ұмытпаңыз.
Бірақ мұны істеуден аулақ болған дұрыс.
Бұл өте қауіпті.

6. Құпия ақпаратты пошта немесе әлеуметтік желі арқылы жібермеңіз.
Төлқұжат пен құжаттардың скандарын дереу жойыңыз

7. Интернетте төлем жасау кезінде әрқашан ережелерді оқыңыз. Ең маңыздысын ең кішкентай әріптермен жазулары мүмкін.

8. Wi-Fi және Bluetooth қолданбаған кезде оны өшіріңіз. Бұл ақпараттық қауіпсіздікті арттырады.

9. Қандай мобильді қосымшалар Сіздің ақпаратыңызға қол жеткізе алатындығын талдаңыз.
Неліктен олар контактілерді білуі, фотосурет алуы, орналасқан жерін анықтауы, камераға немесе микрофонға кіруі керек? Алдымен ойлан

10. Барлық қауіпсіз сайттар қазір «http://» емес «https://» басталады. Төлем жасағанда осыған назар аудар. Сондай-ақ, мұндай сайттар мекенжай жолағында жабық құлыппен белгіленген.

КИБЕРҚАУІПСІЗДІК БОЙЫНША ҰСЫНЫМДАР

1 ҚҰПИЯ СӨЗ САЯСАТЫ

- ✗ Құпия сөздерді жұмыс үстелінде электронды түрде сақтауға тыйым салынады.
- ✓ Өндірістік қажеттілік жағдайында құпия сөз мәндерін ашуға жол беріледі.
- ✓ Құпия сөздер кем дегенде 8 таңбадан тұруы керек және тоқсан сайын жаңартылуы керек.

2 ПОШТА

- ✗ Бейтаныс адамдардан келген электрондық хаттар мен күдікті тіркемелерді ашуға тыйым салынады.
- ✓ Электрондық пошта арқылы кез-келген күдікті сұрау үшін адресаттан сұрау салуды растау үшін балама байланыс арнасын (мысалы, телефон) пайдалану қажет.
- ✓ Жіберуші мен алушының мекен жайының дұрыс жазылуын әрдайым тексеру қажет.

3 АНТИВИРУСТЫҚ БАҒДАРЛАМАЛЫҚ ЖАСАҚТАМА

- ✓ ЛИЦЕНЗИЯЛАНҒАН антивирустық бағдарламалық жасақтаманы пайд қажет.
- ✓ Компьютерге қосылған кезде кез-келген тасымалдаушыны вирустарға тексеріңіз.
- ✓ Автоматты тексеруді орнату арқылы кіріс электрондық поштадағы барлық файлдарды вирустарға тексеріңіз.

4 ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ

- ✗ IP мекенжайларын және логин мен құпия сөздің тіркесімін үшінші тұлғаларға хабарлауға тыйым салынады.
- ✗ Бағдарламалық жасақтаманы өз бетінше орнатуға тыйым салынады.

МЕМЛЕКЕТТІК ҚЫЗМЕТКЕРЛЕРГЕ АРНАЛҒАН КИБЕРҚАУІПСІЗДІК БОЙЫНША ҚОСЫМША ҰСЫНЫМДАР

5 ИНТЕРНЕТ ЖӘНЕ ӘЛЕУМЕТТІК ЖЕЛІЛЕР

- ✗ Белгісіз жіберушіден сілтемелер бойынша өтуге жол берілмейді.
- ✗ Террористік, экстремистік, конституцияға қарсы және өзге де деструктивті бағыттағы материалдарды қамтитын веб-сайттарға кіруге тыйым салынады.
- ✗ Сіз түсінбейтін сайттарға кірген кезде келісімдер қабылдауға тыйым салынады.
- ✗ Жергілікті желіге кіру құпия сөздерін басқа бағдарламалар мен сайттарда пайдалануға тыйым салынады.
- ✓ Cookies (шағын көлемді файлдар) пайдаланумен байланысты қауіптерді болдырмау үшін сақталған cookies-ке мезгіл-мезгіл талдау жүргізу ұсынылады.

- ✗ МО ішкі желілерін Интернетке қосуға тыйым салынады.
- ✓ Интернет желісіне қосылуды тек Интернетке кірудің бірыңғай шлюзі арқылы жүргізу қажет.
- ✗ Интернет желісінің ресурстарымен және электрондық поштамен жұмыс істеу кезінде қызметкерге қызметтік қажеттілік бойынша не өзге де жолмен белгілі болған мемлекеттік, қызметтік және коммерциялық ақпаратты жария етуге тыйым салынады.
- ✓ МО, АҚМ қызметшілері қызметтік хат алмасуды электрондық нысанда жүзеге асыру кезінде қызметтік міндеттерін атқару кезінде тек ведомстволық электрондық поштаны пайдаланады.
- ✗ Компьютерлер мен Интернет-желілерді қараусыз қалдыруға тыйым салынады. Жұмыс орны қалдырылған жағдайда компьютерді құлыптау қажет (- Windows+L пернелер тіркесімі).
- ✗ Сымсыз желілер, сымсыз қол жетімділік, модемдер, радио модемдер, ұялы байланыс операторлары желілерінің модемдері және басқа сымсыз желілік құрылғылар арқылы МО БНАЖ, МО жергілікті желісіне қосылуға тыйым салынады.

ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУ БОЙЫНША ҰСЫНЫМДАР:

Кел ісімге қол қою кезінде мыналарға назар аударыңыз:

- оператор жинайтын дербес деректердің тізбесі;
- дербес деректерді жинау және өңдеу мақсаттары;
- -келісім қолданылатын мерзім немесе кезең;
- -үшінші тұлғаларға беру мүмкіндігі;
- трансшекаралық деректерді беру мүмкіндігі;
- қоғамдық дереккөздерде дербес деректерді тарату мүмкіндігі.

Дербес деректерді кез келген жерге берген кезде міндетті талап не жеке тұлғаның келісімінің болуы не Заңда көзделген негіз болуы

Сіздің келісіміңізсіз жеке деректерді оператор басқа тұлғалар мен ұйымдарға бере алмайды.

Сондай-ақ, жеке деректерді заңсыз таратудан қорғау мақсатында ұйымның жеке деректерінің құпиялылығын сақтау саясатымен танысу, сондай-ақ оларды өңдеу шарттарына мұқият назар аудару ұсынылады.

"Дербес деректер және оларды қорғау туралы" Қазақстан Республикасы Заңының 20-бабының 2-тармағына сәйкес:

дербес деректерді жинау және өңдеу оларды қорғау қамтамасыз етілген жағдайларда ғана жүзеге асырылады.

СІЗДІҢ ҚҰҚЫҚТАРЫҢЫЗ ЗАҢМЕН ҚОРҒАЛҒАН

дербес деректерді қамтитын базаның меншік иесі және (немесе) операторы, сондай-ақ үшінші тұлғалар оларды осы Заңмен қорғау жөнінде шаралар қабылдауға міндетті.

Қазақстан Республикасының Дербес деректер және оларды қорғау туралы заңнамасымен және Қазақстан Республикасының аумағында қолданылатын стандарттармен келісіледі. Бұл міндет дербес деректерді қамтитын электрондық ақпараттық ресурстарды алған сәттен бастап және олар жойылғанға немесе иесіздендірілгенге дейін туындайды.

Сонымен қатар,,

"Ақпараттандыру туралы" ҚР Заңының 56-бабына сәйкес дербес деректерді қамтитын электрондық ақпараттық ресурстарды алған ақпараттық жүйелердің меншік иелері мен иелері,

НЕ ІСТЕУ КЕРЕК?

Жеке деректерді заңсыз жинау және тарату фактілері анықталған кезде азаматтар бұзушылықтардың жолын кесу жөнінде шаралар қабылдау үшін ҚР цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитетіне жүгіне алады.

Мұны kib@mdai.gov.kz электрондық пошта мекенжайына жазу арқылы жасауға болады немесе «Электрондық үкімет» порталы («Электрондық өтініштер» бөлімі) арқылы Төрағаның жеке блогына да (https://dialog.egov.kz/blogs/3932160/welcome) жазуға болады

ӨТІНІШТЕР МЫНАЛАРДЫ ҚАМТУЫ ТИІС:

01 Өтініш берушінің аты-жөні, байланыстары;

02 Бұзушылыққа жол берілген жағдайдың сипаттамасы;

03 Бұзушылықты жасау кезеңі мен мерзімдері;

04 Бұзушылықты растайтын сенімді материалдар;

05 Құқық бұзушылыққа жол берген ұйымның атауы.

Егер Сіз өзіңіздің жеке деректеріңізді сіздің келісіміңізсіз жинауды және өңдеуді жүзеге асыратын біреуді тапсаңыз, Сіз заңсыз жиналған деректерді жоюды талап ете отырып, осы тұлғаға/ ұйымға жүгінуге құқылысыз. Сонымен қатар, Сіз өзіңіздің дербес деректеріңізді жинауға және өңдеуге бұрын берілген келісімді кері қайтарып алуға құқығыңыз бар. Оператор әрекетсіздігі немесе деректерді жоюдан бас тартқан жағдайда, Сіз дербес деректерді қорғау жөніндегі уәкілетті органға - ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ЦИФРЛЫҚ ДАМУ, ИННОВАЦИЯЛАР ЖӘНЕ АЭРОҒАРЫШ ӨНЕРКӘСІБІ МИНИСТРЛІГІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІНЕ шағымдана аласыз.

Өтініштерді кез-келген ыңғайлы және қол жетімді түрде беруге болады..

ЭЛЕКТРОНДЫҚ ЦИФРЛЫҚ ҚОЛТАҢБА ТУРАЛЫ НЕ БІЛУІҢІЗ КЕРЕК ?

Электрондық цифрлық қолтаңба (бұдан әрі-ЭЦҚ) қол қоюшының өз қолымен қойылған қолына тең және бірдей заңдық салдарға әкеп соғады

ЭЦҚ саласындағы бұзушылықтардың алдын алу мақсатында мынадай ұсынымдарды ұстану қажет:

1)ЭЦҚ-ны үшінші тұлғаларға бермеу. Ұйымдарда құжаттарға қол қоюға жауапты қызметкерлерге өкілеттік беру және оларға өздерінің электрондық қолтаңбаларын беру қажет. Ол үшін ұйым басшысының құқықтық актісімен тиісті тұлғаға қол қою құқығын беру және оның атына ЭЦҚ шығару қажет (қызметкерге сенімхат бойынша оның атына шығарылған басшының ЭЦҚ беру заңсыз болып табылады);

2)ұйымнан ЭЦҚ-сы бар қызметкерлерді жұмыстан шығару фактілерін қадағалау және олардың ЭЦҚ-сын кері қайтарып алу;

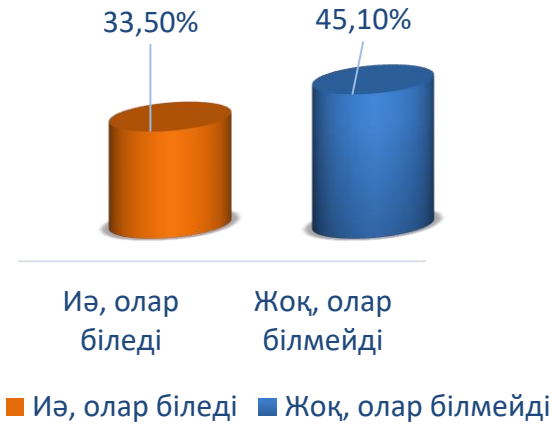
3) жоғалған жағдайда ЭЦҚ-ны қайта алу, алдыңғы ЭЦҚ-ны дереу қайтарып алу, сондай-ақ құпия сөзді стандарттыдан күрделіге ауыстыру.

ЭЦҚ-ны заңсыз беру немесе заңсыз пайдалану фактілері анықталған кезде Қазақстан Республикасының қолданыстағы заңнамасына сәйкес ақпараттық қауіпсіздік комитетін қысқа мерзімде хабардар ету қажет.

*«Электрондық құжат және электрондық цифрлық қолтаңба туралы« 2003 жылғы 7 қаңтардағы Қазақстан Республикасы Заңының 10-бабының 1-тармағы.

ИНТЕРНЕТ ЖЕЛІСІНДЕГІ БАЛАЛАР МЕН ЖАСӨСПІРІМДЕРДІҢ ақпараттық қауіпсіздігі ережелері

Зерттеуге қатысушылармен диалогты жалғастыру барысында балаларды интернеттегі қажетсіз ақпараттан қорғаудың өзекті мәселесіне байланысты мәселе талқыланды. ***Респонденттердің пікірінше баланы Интернеттегі қажетсіз ақпараттан қорғаудың негізгі шарасы:***



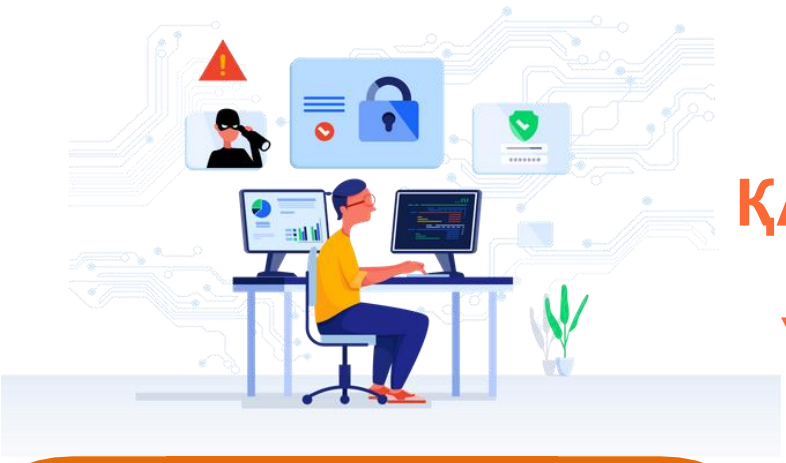
Ата-аналарға ұсынымдар:

- ✓ Жасөспірімдердің қатысуымен Интернетке кірудің үй ережелерінің тізімін жасаңыз және оны сөзсіз орындауды талап етіңіз. Балаңызбен тыйым салынған сайттардың тізімін («қара тізім»), интернеттегі жұмыс уақытын, Интернеттегі байланыс нұсқаулығын (соның ішінде чаттарда) талқылаңыз.
- ✓ Интернет желісіне қосылған Компьютер ортақ бөлмеде болуы керек.
- ✓ Шынайы өмірдегі достар туралы сөйлескендей, Интернеттегі достарымен немен айналысатындары туралы балалармен сөйлесуді ұмытпаңыз. Бұл адамдардың таныс екеніне көз жеткізу үшін балалар жедел хабар алмасу қызметтері арқылы байланысатын адамдар туралы сұраңыз.
- ✓ Стандартты Ата-ана бақылауына қосымша ретінде қажетсіз мазмұнды блоктау құралдарын пайдаланыңыз
- ✓ Сіздің балаларыңыз қандай чаттарды қолданатынын білуіңіз керек. Модераторлық чаттарды пайдалануды ынталандырыңыз және балалардың жеке режимде сөйлеспеуін талап етіңіз.

Балаңыздың Интернетті пайдалануын үнемі бақылаңыз!
Бұл оның жеке кеңістігін бұзу емес, сақтық шарасы және Сіздің ата-анаңыздың жауапкершілігі мен қамқорлығының көрінісі.

БАЛАЛАР МЕН ЖАСӨСПІРІМДЕРДІҢ ИНТЕРНЕТКЕ КІРУІН ҚАЛАЙ ШЕКТЕУГЕ БОЛАДЫ?

- ✓ Балаларды электрондық пошта, чаттар, жедел хабар алмасу жүйелері, тіркеу формалары, жеке профильдер және онлайн конкурстарға тіркелу кезінде жеке ақпараттарын бермеуге үйретіңіз.
- ✓ Балаларды сіздің рұқсатынсыз бағдарламаларды жүктемеуге үйретіңіз. Оларға вирустарды немесе басқа қажетсіз бағдарламалық жасақтаманы кездейсоқ жүктеп алуы мүмкін екенін түсіндіріңіз.
- ✓ Балаңызды интернетке қатысты кез келген қауіп немесе алаңдаушылық туралы хабарлауға үйретіңіз. Балаларға, егер олар сізге өз қауіптері немесе алаңдаушылықтары туралы айтқан болса, олардың қауіпсіз екенін ескертіңіз.
- ✓ Оларға спамнан қорғануға көмектесіңіз. Жасөспірімдерге нақты электрондық пошта мекенжайын интернетте бермеуге, қажетсіз хаттарға жауап бермеуге және арнайы пошта сүзгілерін қолдануға үйретіңіз.
- ✓ Балаларға ешбір жағдайда желіні бұзақылық жасау, өсек айту немесе басқа адамдарға қорқыту үшін пайдалануға болмайтынын түсіндіріңіз.
- ✓ Жасөспірімдермен онлайн құмар ойындарының қиындықтарын және олардың ықтимал қаупін талқылаңыз. Есіңізде болсын, балалар бұл ойындарды заң бойынша ойнай алмайды.



АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ САЛАСЫНДАҒЫ УӘКІЛЕТТІ ОРГАН

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІНІҢ ӨКІЛЕТТІКТЕРІ

Қазақстан Республикасы Президентінің 2016 жылғы 6 қазандағы №350 Жарлығы шеңберінде Ақпараттық қауіпсіздік комитеті құрылды.

01 **Әзірлеу**
Ақпараттық қауіпсіздікті қамтамасыз ету саласында шаралар әзірлеу (мемлекеттік құпияларды қоспағанда).

02 **Бақылау**
Ақпараттық - коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптардың сақталуын мемлекеттік бақылау және алдын алу

03 **Құрылу**
Маңызды ақпараттық-коммуникациялық инфрақұрылымның тізбесін қалыптастыру және мониторингі.

04 **Басқару**
Интернеттің қазақстандық сегментінің кеңістігінде домендік атауларды басқару және бөлу.

05 **Беру**
Ақпараттық қауіпсіздік талаптарына сәйкестігін сынау нәтижелері бойынша акт беру.

06 **Үйлестіру**
2022 жылға дейін «Қазақстанның киберқауіпсіздігі» киберқауіпсіздік тұжырымдамасын ведомствоаралық үйлестіру.

07 **Ұйымдастыру**
Ақпараттық қауіпсіздік инциденттеріне ден қоюдың ұлттық жоспарының орындалуын ұйымдастыру.

08 **Қарау**
Дербес деректер саласындағы бұзушылықтар үшін қарау және жауапқа тарту.

09 **Жүзеге асыру**
Куәландырушы орталықтарды аккредиттеуді жүзеге асыру.

10 **Хабардарлық**
Ақпараттық қауіпсіздік (киберқауіпсіздік)қатерлері туралы халықтың хабардарлығын арттыру

11 **Қатысу**
Білім беру бағдарламаларын іске асыруға қатысу.

12 **Жәрдемдесу**
Кәсіби стандарттарды қалыптастыруға жәрдемдесу.

13 **Қолдау**
Ақпараттық қауіпсіздік саласындағы ғылыми зерттеулерді қолдау..

14 **Өзара іс-әрекет**
Халықаралық ұйымдармен, ұлттық реттеушілермен және киберқауіпсіздік орталықтарымен өзара іс-әрекет.

Компьютерлік инцидент кезінде қайда хабарласу керек?

Жауап қайтару қызметі

1400

немесе 8 (7172) 55-99-97
Тегін жедел желі
эл.пошта: info@kz-cert.kz

Қызметтің құзыретіне оларды анықтау және бейтараптандыру мақсатында келесі компьютерлік оқиғаларды өңдеу кіреді:

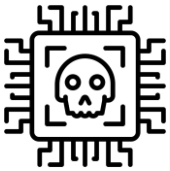
желілік инфрақұрылым түйіндеріне және серверлік ресурстарға олардың жұмыс қабілеттілігін (DoS (Denial of Service) және DDoS) және ақпараттың құпиялылығын бұзу мақсатында шабуылдар;

ақпараттық ресурстарға рұқсатсыз қол жеткізу

зиянды бағдарламалық жасақтамаларды, талап етілмеген хат-хабарларды (спам)тарату;

ұлттық ақпараттық желілер мен хосттарды сканерлеу;

Құпия сөздерді және басқа аутентификациялық ақпаратты таңдау және қолға түсіру;



ақпараттық желілерді қорғау жүйелерін бұзу, оның ішінде зиянды бағдарламаларды енгізу (сниффер, rootkit, keylogger және т.б.).

KZ CERT

KZ-CERT Компьютерлік инциденттерге жауап беру қызметі

Зерттеудің қысқаша талдауы

ақпараттық қауіпсіздік және дербес деректерді қорғау мәселелері бойынша әлеуметтік зерттеу нәтижелері бойынша

Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитетінің тапсырысы бойынша ақпараттық қауіпсіздік (киберқауіпсіздік) және дербес деректерді қорғау мәселелері бойынша әлеуметтік зерттеу жүргізілді. Жүргізілген сауалнама нәтижесі халықтың ақпараттық қауіпсіздікке (киберқауіпсіздікке) және дербес деректерді қорғауға төнетін қатерлер туралы **77,4%.** деңгейінде хабардар болуының жалпы көрсеткішін айқындады.

Жалпы, социологиялық зерттеудің нәтижелері ақпараттық қауіпсіздіктің (киберқауіпсіздік)келесі жай-күйін көрсетеді:

- халықтың компьютерге және басқа да сандық құрылғыларға меншік деңгейі (73,8%)құрады;

- халықтың 51,5% - ы үшін ақпарат алудың негізгі көзі интернет болып табылады. Бұл ретте, Интернетке тікелей шығу үшін мобильді құрылғыларды, смартфондар мен планшеттерді пайдалану (70,2%)құрады;

- Халықтың 45,1% - ы балаларды интернеттегі қажетсіз ақпараттан қорғаудың негізгі әдістерін білмейді және т. б.

Осыған байланысты, жүргізілген әлеуметтік сауалнаманы ескере отырып, зерттеу тобы азаматтардың ақпараттық қауіпсіздігін одан әрі қамтамасыз ету және олардың ақпараттық кеңістіктегі дербес деректерін қорғау үшін тиісті ұсынымдар мен ұсыныстар әзірледі.

"Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті" РММ тапсырысы бойынша

Қазақстан Республикасы 010000, Астана қ., Мәңгілік ел даңғ. 55/14, блок С 2.4

тел.: +7 (7172) 64-93-96, +7 (7172) 64-93-99

e-mail: **kib@mdai.gov.kz**

https://www.gov.kz/memleket/entities/infsecurity?lang=ru

ҰСЫНЫМДАР

Астана қ. 2022