Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі

Ақпараттық қауіпсіздік комитеті

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

Ұсынымдар

АҚПАРАТТЫҚ КЕҢІСТІКТІ ҚОРҒАУ

Жаһандық цифрландырудың маңызды мәселелерінің бірі **ақпараттық қауіпсіздікті қамтамасыз ету** болып табылады.

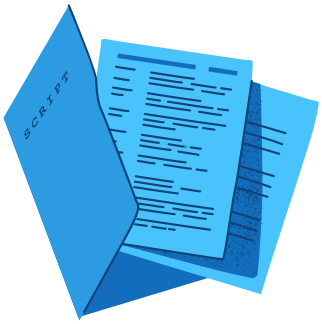
Біріккен Ұлттар Ұйымының Халықаралық электр байланысы одағының (БҰҰ ХЭБО) жаһандық киберқауіпсіздік индексінде (ЖКИ) Қазақстан өз деңгейін жылдам арттырды. ЖКИ индикаторлары бойынша жетістік деңгейін арттыру Қазақстанға БҰҰ ХЭБО сарапшылары жүргізген талдау бойынша белгілі бір нәтижелерге қол жеткізуге және ЖКИ-де **Қазақстан Республикасын 9 позицияға көтеріп**, қазіргі уақытта **31-ші (бұрын 40-шы) орында** орналасуға мүмкіндік берді.

Мемлекет басшысының тапсырмасы бойынша Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы №269 қаулысымен бекітілген **цифрлық трансформация, АКТ саласын және киберқауіпсіздікті дамытудың 2023-2029 жылдарға арналған Тұжырымдамасы** қабылданды.

Бұл тұжырымдамада елдің киберқауіпсіздігін нығайтуға бағытталған қосымша шаралар регламенттелген, атап айтқанда техникалық қорғау, радио бақылауды жетілдіру, дербес деректерді қорғау және халықтың хабардарлығын арттыру жөніндегі іс-шаралар көзделген.

2023 жылғы 11 желтоқсанда Мемлекет басшысы «ҚР кейбір заңнамалық актілеріне ақпараттық қауіпсіздік, ақпараттандыру және цифрлық активтер мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы» Қазақстан Республикасының Заңына қол қойды.

Бұл заң дербес деректерді қорғауды күшейтуге және ақпараттандыру объектілерінің, оның ішінде мемлекеттік органдардың **ақпараттық қауіпсіздігін қамтамасыз ету** кезінде өзара іс-қимылдың жаңа тетіктерін айқындауға **бағытталған**.



КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

КИБЕРҚАУІПСІЗДІК ЭКОЖҮЙЕСІ

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

Киберқауіпсіздік экожүйесінің негізгі элементтері: **адами капитал, киберқауіпсіздік нарығын дамыту, техникалық қорғау** болып табылады.

Адами капиталды дамыту мақсатында елде ақпараттық қауіпсіздік мамандарын даярлайтын **8 жоғары оқу орны және 25 орта арнаулы** оқу орны бар.

2022-2023 оқу жылдары ақпараттық қауіпсіздік мамандығы бойынша **білім гранты 3009-ға дейін** ұлғайтылды (**2021-2022 жылдармен** салыстырғанда **2600-ге дейін грант** бөлінді).

2023-2024 жылдары ақпараттық қауіпсіздік мамандығы бойынша **3723 білім гранты** бөлінді.

85 маман «Болашақ» бағдарламасы бойынша шетелдік жетекші жоғары оқу орындарында **«Ақпараттық (кибер) қауіпсіздік және криптография», «Ақпараттық қауіпсіздік»** мамандықтары бойынша білім алды.

КИБЕРҚАУІПСІЗДІК ЭКОЖҮЙЕСІ

Ақпараттық қауіпсіздік саласындағы сапалы кәсіби қызметтер нарығын дамыту мақсатында 3 бейінді қоғамдық ұйым бар, ақпараттық қауіпсіздік саласындағы 50 компания жұмылдырылған. Маңызды инфрақұрылымы бар 514 стратегиялық нысан анықталды. 41 жеке ақпараттық қауіпсіздік жедел орталықтары құрылды, 3 компьютерлік инциденттерге ден қою қызметі (FIRST) және 9 жеке сынақ зертханасы бар.

Техникалық қорғау мақсатында 2018 жылы ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы құрылып, өз жұмысын бастады. Сонымен қатар, болашақта бейбіт уақытта, соғыс жағдайы мен соғыс уақытында төтенше жағдайлар кезінде оның жұмысын ұйымдастырмау жағдайлары үшін қорғалған резервтік инфрақұрылым бөлігінде мәселе пысықталатын болады.

2022 жылы мемлекеттік ақпараттық қауіпсіздік жедел орталығы (GSOC) құрылды, сонымен қатар салалық ақпараттық қауіпсіздік жедел орталығы (SOC) құрылды.

2022 жылы дербес деректерге қол жеткізуді бақылау сервисі (ДДБ сервисі) іске қосылды. Бұл сервис азаматтың оның дербес деректеріне қол жеткізуге келісімін қайтарып алуға арналған. Сондай-ақ, Қызмет жеке деректерді рұқсатсыз кіруден немесе таратудан қорғайды.

2023 жылы КДП сервисіне 113 ақпараттық жүйе қосылған.

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

Халықтың хабардарлық деңгейі

Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитетінің тапсырысы бойынша ақпараттық қауіпсіздікке (киберқауіпсіздікке) төнетін қатерлер туралы халықтың хабардар болу деңгейін айқындау және дербес деректерді қорғау мақсатында 2023 жылғы қыркүйек-қараша айларында халықтың ақпараттық қауіпсіздікке (киберқауіпсіздікке) төнетін қатерлер туралы хабардар болуы және дербес деректерді қорғау жөнінде әлеуметтік зерттеу жүргізілді.

Социологиялық зерттеу барысында қамтылды:

3 республикалық маңызы бар қалалар (Астана, Алматы, Шымкент)

17 Республикадағы облыстардың аудандары мен ауылдары

11371 қатысушы респонденттер

Қатысушылар: 18 жастан асқан ҚР азаматтары;

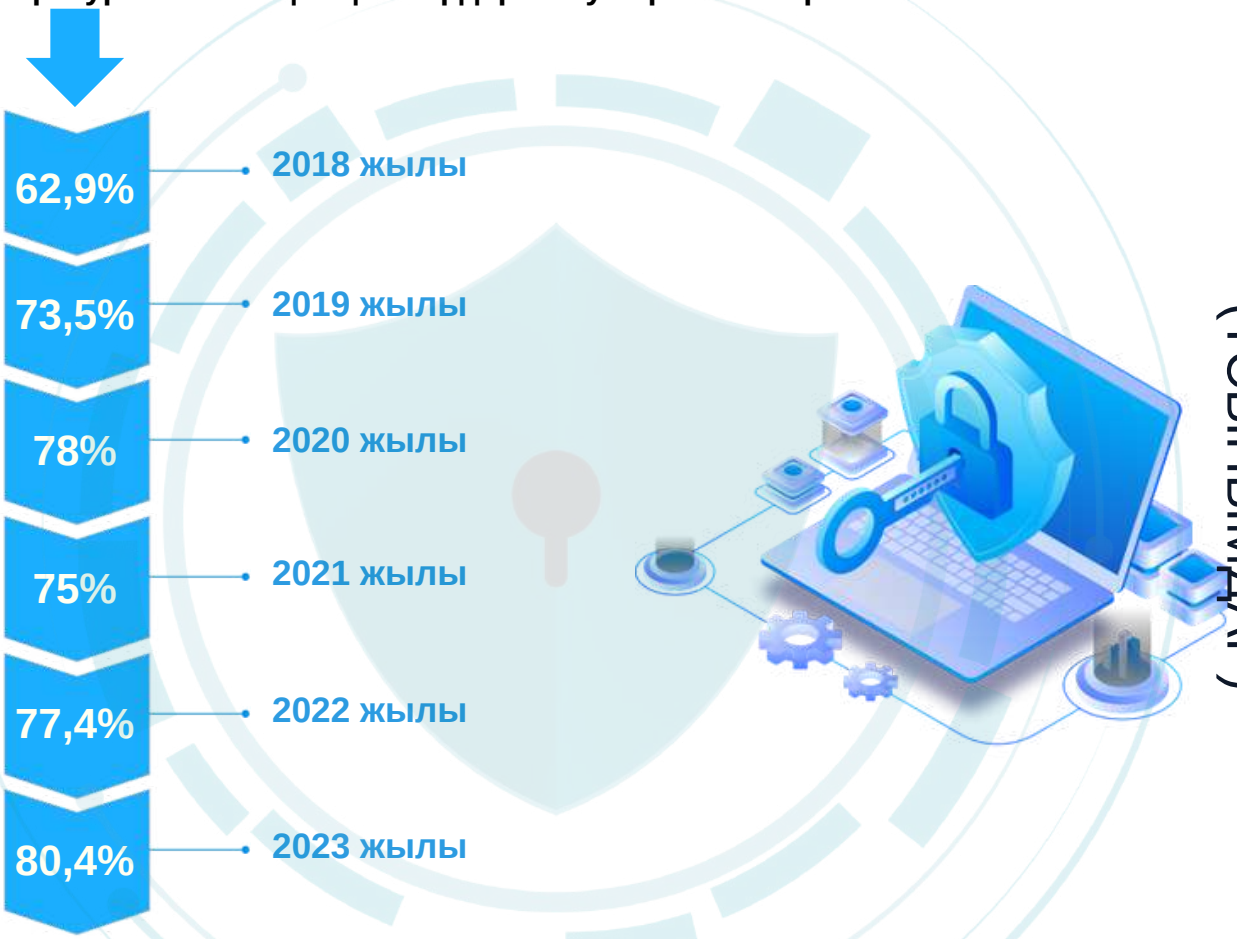
Сауалнама блоктарының сұрақтарының саны:

- әлеуметтік-демографиялық блок - 10;
- негізгі блок - 30;
- қосымша блок - 20;

Халықтың хабардарлық деңгейі

Республика бойынша 3 ай ішінде жүргізілген социологиялық зерттеу сауалнамасына барлығы 11371 респондент қатысты. Сауалнама нәтижелерін талдай отырып, бүгінгі таңда Қазақстан халқының ақпараттық қауіпсіздік бойынша хабардарлық деңгейінің өскенін атап өтуге болады.

Ақпараттық қауіпсіздік (киберқауіпсіздік) және дербес деректерді қорғау қатерлері туралы халықтың хабардар болу көрсеткіштері:



2023 жылы жүргізілген социологиялық зерттеудің нәтижелері бойынша, респонденттердің көпшілігі:

- **90,52 %-ы әлеуметтік желілерді пайдалану кезінде жеке ақпаратты қорғау туралы білім алады;**

- **85,06 %-ы «электрондық цифрлық қолтаңбаны» пайдалану бойынша хабардар;**

- **76,65 %-ы интернетті пайдалану кезінде балаларға төнетін ықтимал қауіптері туралы біледі;**

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

Деректер қауіпсіздігіне қауіп

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

БІЛУ МАҢЫЗДЫ:

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

- **Құпиялылық** — ақпаратқа тек оған құқығы бар адам ғана қол жеткізуі керек.
- **Қол жетімділік** — ақпарат қажет болған кезде қол жетімді болуы керек.
- **Тұтастық** — ақпарат сенімді болуы керек.

Қағидалардың бірін бұзу басқалардың бұзылуына әкелуі мүмкін.

Зиянды бағдарламалар пайдаланушының компьютеріне қалай енеді?

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

Киберқауіпсіздік қауіптерінің түрлері:

- **Фишинг** - бұл онлайн-қолданушылардың мұқият еместігіне негізделген интернеттегі алаяқтықтың кең таралған түрі.
- **Сайтты бұзу** - ішкі деректерге немесе веб-ресурстың басқару тақтасына заңсыз жолмен қол жеткізу.
- **Әлеуметтік инженерия** - белгілі бір әрекеттерді орындау немесе құпия ақпаратты ашу үшін адамдарды психологиялық манипуляциялау.
- **DDos шабуылы** - бұл өтініштерді өңдеуге тыйым салатын сұраныстардың артық санымен ақпараттық жүйенің шамадан тыс жүктелуі.
- **Трояндық ат** - бұл өзінің нақты мақсатын жасыратын зиянды бағдарламалық жасақтама. Сонымен қатар, вирустан айырмашылығы, троян файлдарды дербес көшіруге немесе жұқтыруға қабілетті емес.
- **Төлем бағдарламасы** - компьютерді құлыптайды, содан кейін оның құлпын ашу үшін төлем талап етеді.

Тарату әдістері:

электрондық поштадағы зиянды сайттарға сілтемелер

әлеуметтік желілердегі жазбалар

вирус жұққан файлды жүктеуге сендіреді

вирус жұқтырған сайтқа кіру

компьютерде вирус жұққан USB дискісін пайдалану

олар бұзған веб-сайттардан және басқа компьютерлерден құпия сөздерді жинайды

ҰСЫНЫМДАР:

Кірген сайттар мен ресурстарды мұқият қарап шығыңыз, домендік атауларды тексеріңіз және «иә, мен келісемін» түймесін баспас бұрын немен келісетініңізді мұқият оқып шығыңыз.

Сіз алған хатты ашпас бұрын, оған жауап ретінде бірнеше сөз жазыңыз, өйткені егер жіберуші сенімді болса, хатты жіберген тарап міндетті түрде жауап береді.

Жеке деректерге қол жеткізу үшін күрделі құпия сөздерді және/немесе екі факторлы аутентификацияны орнатыңыз.

Интернетте сатып алу үшін бөлек виртуалды картаны ашып, ішіне сатып алуға есептелген соманы ғана салыңыз.

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

Өткен жылы сіз кибершабуылға ұшырадыңыз ба?

Сауалнамаға сәйкес, өткен жылы Қазақстан халқы кибершабуылдардың төменде көрсетілген түрлеріне ұшыраған:

- **компьютерлік вирустар – 22,8%;**
- **зиянды спам – 16,9%;**
- **есептік жазбаны бұзу – 8.1%;**
- **хакердің шабуылы – 3,6%;**
- **кибер алаяқтық – 6,9%;**

	2023	2022	2021	2020
Компьютерлік вирустардың шабуылы	22,8%	51,7%	16,5%	32,1%
Зиянды спам	16,9%	34,5%	23,0%	13,4%
Әлеуметтік желілердегі аккаунттарды бұзу	8,1%	28,4%	14,5%	3,9%

КИБЕРҚАУІПСІЗДІК БОЙЫНША ҰСЫНЫМДАР:

- **Құпия сөздерді үнемі жаңартып отырыңыз.**
- **Екі факторлы аутентификацияны қолданыңыз.**
- **Балаларға арналған жеке банк карталарын жасаңыз.**
- **Қолданбаларға кіруді шектеңіз және геолокацияны алып тастаңыз.**
- **Әлеуметтік желілерде құпиялылықты орнатыңыз.**
- **Құжаттарды жіберу үшін поштаны пайдаланыңыз.**
- **Бағдарламалық жасақтаманы тек ресми сайттардан жүктеп алыңыз.**
- **Сайттан гөрі ресурстың мобильді нұсқасына артықшылық беріңіз.**

ИНТЕРНЕТТЕ ЖҰМЫС ІСТЕГЕНДЕ ҚАНДАЙ ҚАУІПСІЗДІК ШАРАЛАРЫН ҚОЛДАНАСЫЗ?

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ АЛДЫН АЛУ

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

РЕСПОНДЕНТТЕР ОЛАР ТІРКЕЛГЕН САЙТТАР ТУРАЛЫ АҚПАРАТТЫ ТЕКСЕРЕ МЕ?

Әлеуметтік сауалнама нәтижелері:

40,4% — респонденттер сайттар туралы ақпаратты үнемі тексеріп отырады;

42,5% — респонденттер кейде ресурс күмән тудырған кезде сайт ақпаратын тексереді;

16,9% — респонденттер сайттар туралы ақпаратты ешқашан тексермейді;

Егер сіз өзіңіздің банктік шотыңызда интернет-банкингте, онлайн-дүкенде және т. б. күдікті әрекеттерді байқасаңыз, не істеу керек?

5,96% респонденттер әлеуметтік желілерде күдікті белсенділік туралы ақпаратпен бөліседі;

68,91% респонденттер күдікті әрекет туралы дереу банкке хабарлайды;

12,35% респонденттер бәрін сол күйінде қалдырады, мүмкін бұл жүйелік қате;

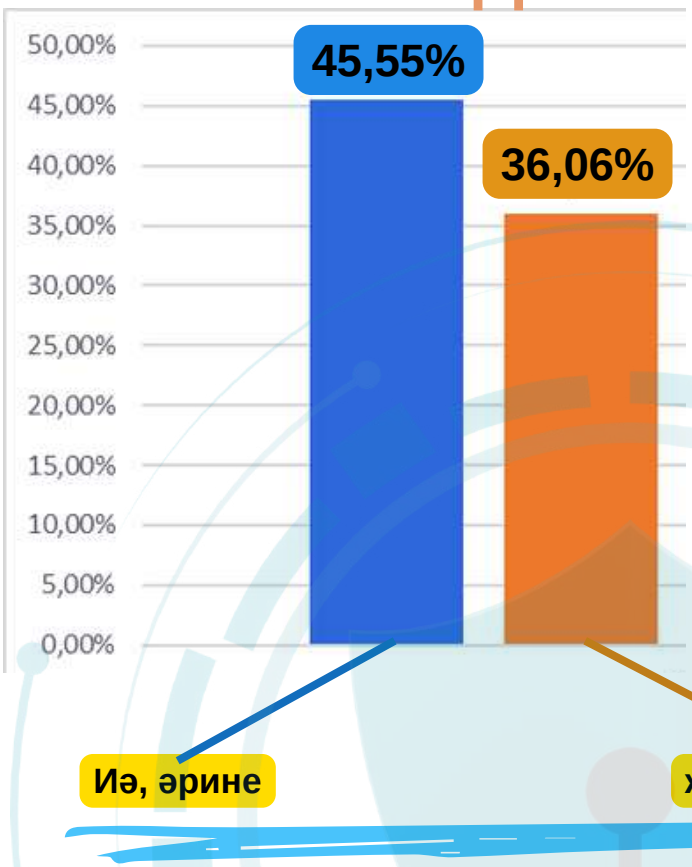
Ұсынымдар
(ақпараттық қауіпсіздік бойынша алдын алу)

- **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 құралды жойыңыз.**
- **Тексерілмеген көздерден лицензиясыз бағдарламалық жасақтаманы немесе бағдарламалық жасақтаманы орнатудан аулақ болыңыз.**
- **Басқа құрылғыларда сіз үшін маңызды деректердің көшірмесін үнемі жасаңыз.**

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ АЛДЫН АЛУ

Сауалнамаға респонденттердің жауабы:

«Сіз ақпараттық қауіпсіздікті қамтамасыз ету мәселелері жөніндегі уәкілетті органның қызметі және оған жүгіну тәсілдері туралы білесіз бе?»



Респонденттердің пікірінше киберқауіпсіздіктің бұзылуына күдік туындаған жағдайда негізгі шара:

Құқық қорғау органдарына жүгіну	10,79%
IT-маманға жүгіну	55,36%
Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы уәкілетті органға жүгіну	15,37%
Ештеңе істеуді қажет деп санамайды	3,70%

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

АҚПАРАТТЫҚ ҚАУІПСІЗДІК БОЙЫНША ҰСЫНЫМДАР

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

ҚҰПИЯ СӨЗ САЯСАТЫ

Парольдерді жұмыс үстелінде электронды түрде сақтауға тыйым салынады.

Өндірістік қажеттілік жағдайында пароль мәндерін ашуға жол беріледі.

Құпия сөздер кем дегенде 8 таңбадан тұруы керек және тоқсан сайын жаңартылуы керек.

ПОШТА

Бейтаныс адамдардан 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.

АНТИВИРУСТЫҚ БАҒДАРЛАМАЛЫҚ ЖАСАҚТАМА

Лицензияланған антивирустық бағдарламалық жасақтаманы пайдалану қажет.

Компьютерге қосылған кезде кез-келген тасымалдаушыны вирустарға тексеруді ұмытпаңыз.

Автоматты тексеруді орнату арқылы кіріс электрондық поштадағы барлық файлдарды вирустарға тексеріңіз.

ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ

IP-мекенжайларын және логин мен парольдің тіркесімін үшінші тұлғаларға хабарлауға тыйым салынады.

Бағдарламалық жасақтаманы өз бетінше орнатуға тыйым салынады.

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 парольдерін басқа бағдарламалар мен сайттарда пайдалануға тыйым салынады.

Cookies (шағын көлемді файлдар) пайдаланумен байланысты қауіптерді болдырмау үшін сақталған cookies-ке мезгіл-мезгіл талдау жүргізу ұсынылады.

МЕМЛЕКЕТТІК ҚЫЗМЕТКЕРЛЕРГЕ АРНАЛҒАН КИБЕРҚАУІПСІЗДІК БОЙЫНША ҚОСЫМША ҰСЫНЫМДАР

- Мемлекеттік органның (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, жергілікті атқарушы органдардың (ЖАО) 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 жеткізу, модемдер, радио модемдер, ұялы байланыс операторлары желілерінің модемдері және басқа да сымсыз желілік құрылғылар арқылы МО-ның Бірыңғай көлік ортасына (БКО), МО-ның жергілікті желісіне қосылуға тыйым салынады.

ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУ БОЙЫНША ҰСЫНЫМДАР:

(ҰСЫНЫМДАР)

КЕЛІСІМГЕ ҚОЛ ҚОЮ КЕЗІНДЕ МЫНАЛАРҒА НАЗАР АУДАРЫҢЫЗ:

- **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.**
- **оператор жинайтын дербес деректердің тізбесі;**

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.

СІЗДІҢ ҚҰҚЫҚТАРЫҢЫЗ ЗАҢМЕН ҚОРҒАЛҒАН:

«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.

Сонымен қатар, «Ақпараттандыру туралы» ҚР Заңының 56 - бабына сәйкес дербес деректерді қамтитын электрондық ақпараттық ресурстарды алған ақпараттық жүйелердің меншік иелері мен иелері, 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.

2023 жылғы 11 желтоқсанда «Қазақстан Республикасының кейбір заңнамалық актілеріне ақпараттық қауіпсіздік, ақпараттандыру және цифрлық активтер мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы» заң бойынша қорғаудың жаңа жүйесі пайда болды:

Заң ішінде келесі жаңалықтарды қарастырады:

дербес деректерді қорғау саласындағы уәкілетті органға (Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі) Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасының сақталуын мемлекеттік бақылау функциясын беру;

жеке басын куәландыратын, дербес деректері бар құжаттардың көшірмелерін жинауға, өңдеуге тыйым салуды белгілеу;

азаматтарды дербес деректердің тарап кету фактілері туралы хабардар ету;

банктік қарыздарды алудан ерікті түрде бас тартуды белгілеу;

НЕ ІСТЕУ КЕРЕК?

Жеке деректерді заңсыз жинау және бұзу фактілері анықталған кезде

азаматтар бұзушылықтардың жолын кесу жөнінде шаралар қабылдау үшін Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитетіне жүгіне алады.

Мұны «электрондық үкімет» порталы («Электрондық өтініштер» бөлімі) арқылы жазу арқылы жасауға болады, сонымен қатар төрағаның жеке блогына жазуға болады
(https://dialog.egov.kz/blogs/3932160/welcome)

e-gov

ӨТІНІШТЕР МЫНАЛАРДЫ ҚАМТУЫ ТИІС:

1. Өтініш берушінің аты-жөні, байланыс құралдары;
2. Бұзушылыққа жол берілген жағдайдың сипаттамасы;
3. Бұзушылықты жасау кезеңі мен мерзімдері;
4. Бұзушылықты растайтын сенімді материалдар;
5. 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 ҚОЛТАҢБАНЫ ПАЙДАЛАНУ

Электрондық цифрлық қолтаңба (ЭЦҚ) дегеніміз не?

Қарапайым тілмен айтқанда, электрондық цифрлық қолтаңба (ЭЦҚ) – бұл құжаттарға қол қоюға болатын азаматтың электрондық түрдегі жеке қолтаңбасы.

ЭЦҚ АЛАЯҚТАРДЫҢ НЕМЕСЕ БАСҚА БІРЕУДІҢ ҚОЛЫНА ТҮСКЕН ЖАҒДАЙДА НЕ БОЛУЫ МҮМКІН:

Егер ЭЦҚ парольмен қорғалмаса, ол арқылы құжаттарға немесе қаржылық операцияларға қол қойылуы мүмкін.

Кәсіпкерлік субъектілері үшін ЭЦҚ алу «Жалған қызметкерлерді» жұмысқа орналастыруға әкелуі мүмкін.

ЭЦҚ иесінің аты бойынша пәтерде бірнеше адамды хабарламай тіркеу.

Өз ЭЦҚ-ыңызды қорғау бойынша мынадай шараларды қабылдау қажет:

ХҚКО-дан ЭЦҚ алғаш алған кезде қарапайым пароль болуы мүмкін, сондықтан оны күрделі парольмен ауыстыру керек.

ЭЦҚ-ны бөгде адамдарға бермеңіз. Жауапкершілік сізге жүктелген кезде олар сіздің атыңыздан құжаттарға қол қоя алады.

Арнайы чаттарда, мессенджерлерде ЭЦҚ жібермеңіз.

ЭЦҚ сақталатын компьютерді немесе ноутбукты вирустардан қорғау бағдарламаларымен қамтамасыз етіңіз.

ЭЦҚ файлдарда сақталған кезде оның файл атауымен паролін сақтамаңыз.

Басқа біреуге ЭЦҚ алмаңыз. ЭЦҚ-ны бірнеше тәсілмен алуға болады: халыққа қызмет көрсету орталықтары (ХҚКО) арқылы немесе eGov арқылы.

Компьютермен смартфон гаджеттеріне тексерілмеген немесе сенімсіз бағдарламаларды орнатудан аулақ болыңыз.

Егер сіз ЭЦҚ жоғалтсаңыз немесе ол басқа адамдардың қолына түссе, кілтіңізді дереу жаңартыңыз.

Интернет желісіндегі балалардың қауіпсіздігін қорғау

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

Бүгінгі таңда интернет-ресурста балаларға қауіп төндіретін көздер көбейіп келеді. Олардың кейбіреулері туралы айтатын болсақ: балаларды өз-өзіне қол жұмсауға немесе балаларға зиян келтіретін қорлаудың теріс әрекеттеріне итермелейтін тыйым салынған қастандықтар, ресурстар және топтар.

Бүгінгі таңда кибербуллинг балалардың қауіпсіздігі үшін өте өзекті мәселе болып табылады. Мұндай жағдайларда ата-аналар назар аударуы керек:

- **Интернетте уақыт өткізгеннен кейін жаман көңіл-күй.**
- **Әсіресе интернет желісінде қажетсіз ақпаратты пайдалану туралы сөз болғанда өте жабық болады**
- **Агрессия немесе ашулану.**
- **Баланың мазасыздығы және/немесе толқуы.**
- **Ақша жиі сұралады.**

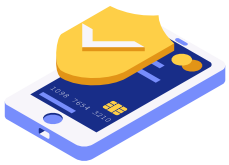
Ата-аналар балаларды киберқауіптен қорғау үшін қандай шаралар қабылдауы керек:

*** Интернетті пайдалану уақытын шектеңіз.**

*** Балалар интернетте және әртүрлі желілерде көретін мазмұнды бақылауға алыңыз.**

*** Интернетте балалармен ықтимал қауіптерді талқылаңыз.**

*** Балаларға теріс мазмұнға ресурс модераторына шағымдануға болатындығын түсіндіріңіз.**



*** Егер балалар интернетте жағымсыз жағдайға тап болса, оларға дауыс көтерместен осы жағдайды жеңуге көмектесіңіз.**

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 арналған 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.
- Интернеттегі достары туралы балалармен сөйлесуді ұмытпаңыз, олар шынайы өмірдегі достар туралы сөйлесетіндей бос емес. Бұл адамдардың таныс екеніне көз жеткізу үшін балалар жедел хабар алмасу қызметтері арқылы байланысатын адамдар туралы сұраңыз.
- Қажет емес мазмұнды блоктау құралдарын стандартты ата-ана бақылауына қосымша ретінде 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?

1. Балаларды электрондық пошта, чаттар, жедел хабар алмасу жүйелері, тіркеу формалары, жеке профильдер және онлайн конкурстарға тіркелу кезінде жеке ақпараттарын бермеуге үйретіңіз.

2. Балаларды сіздің рұқсатынсыз бағдарламаларды жүктемеуге үйретіңіз. Оларға вирустарды немесе басқа қажетсіз бағдарламалық жасақтаманы кездейсоқ жүктеп алуы мүмкін екенін түсіндіріңіз.

3. 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.

4. Оларға спамнан қорғануға көмектесіңіз. Жасөспірімдерге нақты электрондық пошта мекенжайын интернетте бермеуге, қажетсіз хаттарға жауап бермеуге және арнайы пошта сүзгілерін қолдануға үйретіңіз.

5. Балаларға ешбір жағдайда желіні бұзақылық жасау, өсек айту немесе басқа адамдарға қорқыту үшін пайдалануға болмайтынын түсіндіріңіз.

6. Жасөспірімдермен онлайн құмар ойындарының қиындықтарын және олардың ықтимал қаупін талқылаңыз. Балалар бұл ойындарды заң бойынша ойнай алмайтынын ескертіңіз.

КӘСІПҚОЙЛАРҒА АРНАЛҒАН БӨЛІМ

Бизнес иелері, тиісті сала қызметкерлері, IT-маманы, ақпараттық қауіпсіздік офицері есте ұстауы керек ұсынымдар:

1 АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫН ӘЗІРЛЕУ

Кәсіпорынның немесе ұйымның басшылығы **ақпараттық қауіпсіздікті қамтамасыз ету тұжырымдамасын** әзірлеп, енгізуі керек. Бұл құжат ішкі регламенттер мен қорғау шаралары жүйесін әзірлеу үшін негіз болып табылады.

2 БІРНЕШЕ ДЕҢГЕЙДЕ ҚОРҒАНЫС ҚҰРУ.

Киберқауіпсіздікке көп деңгейлі көзқарас шифрлаушылардың **шабуыл қаупін** азайтады. Ол бірнеше қорғаныс құралдарын біріктіруді қамтиды. Егер қауіп қорғаныстың бір деңгейін айналып өтсе, келесі деңгейде ол жаңа кедергіге тап болады.

3 ЖЕКЕ ҚҰРЫЛҒЫЛАРДЫ ЖҰМЫС МАҚСАТЫНДА ПАЙДАЛАНУ САЯСАТЫН ҚАЙТА ҚАРАУ.

Қашықтағы қызметкерлер **кейде** жұмыс істеу және кәсіпорын желісіне қосылу үшін өздерінің ноутбуктарын немесе мобильді құрылғыларын **пайдаланады**. Дегенмен, жеке құрылғыларда әрқашан сенімді антивирус немесе басқа қауіпсіздік құралы бола бермейді.

4 ЭЛЕКТРОНДЫҚ ПОШТА СҮЗГІЛЕРІН ПАЙДАЛАНУ.

Әрине, пошта сүзгілері ұйымның фишингтік хатты алмауын қамтамасыз ете алмайды, бірақ олар **қауіпсіздік деңгейін жоғарылатады**. Респонденттердің **46,1%-ы** тек белгілі және сенімді Электрондық хаттарды ашатынын көрсетті.

5 ҚҰПИЯ СӨЗ МЕНЕДЖЕРІН ПАЙДАЛАНУ.

Қызметкерлердің **құпия сөз менеджерін** пайдалануын ұйымдастыру - ол ұзақ және күрделі құпия сөздерді жасайды және сақтайды және оларды қолданбалардағы енгізу өрістеріне тасымалдайды.

КӘСІПҚОЙЛАРҒА АРНАЛҒАН БӨЛІМ

6 ДЕРЕКТЕРДІҢ РЕЗЕРВТІК КӨШІРМЕСІ.

Компьютерде сақталған деректердің ғана емес, мобильді құрылғыларда сақталатын деректердің де резервтік көшірмесін үнемі жасаңыз. Осылайша, құрылғы жоғалған немесе ұрланған жағдайда қажетті ақпаратты тез қалпына келтіре аласыз.

7 ҚЫЗМЕТКЕРЛЕРДІ ОҚЫТУ.

Көп жағдайда қызметкерлер олардың әрекеттері қауіпті болуы мүмкін екенін білмейді. Ұйым қызметкерлерінің киберқауіптер, соның ішінде әлеуметтік инженериямен байланысты қауіптер туралы хабардарлығын арттыру арқылы адам қателігінің қаупін азайтуға болады.

Ақпараттық қауіпсіздікке қауіп төнген жағдайда зерттеу көрсеткендей, респонденттердің 55,4% - ы IT-саласының мамандарына жүгінеді.

8 КИБЕРШАБУЫЛ БОЛҒАН ЖАҒДАЙДА ІС-ҚИМЫЛ ЖОСПАРЫН ҚҰРУ.

Төтенше жағдайға дайын болу керек.Бизнесті, қызметкерлерді және клиенттерді сенімді қорғау үшін шабуыл болған жағдайда егжей-тегжейлі іс-қимыл жоспары болуы маңызды.

9 ҚҰПИЯ СӨЗБЕН ҚОРҒАУДЫ ҚОСЫҢЫЗ.

Орташа шабуылдаушыны мобильді құрылғыдан аулақ ұстау үшін күрделі құпия сөзді немесе PIN кодты пайдалану керек. Респонденттердің 33,6%-ы әр есептік жазба үшін жеке, күрделі құпия сөзді қолданатындығын көрсетті.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІНІҢ ӨКІЛЕТТІКТЕРІ

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

1. **ӘЗІРЛЕУ**
   Ақпараттық қауіпсіздікті қамтамасыз ету саласында шаралар әзірлеу (мемлекеттік құпияларды қоспағанда).

2. **БАҚЫЛАУ**
   Ақпараттандыру, дербес деректерді, электрондық құжатты және электрондық цифрлық қолтаңбаны және қамтамасыз етілген цифрлық активтерді қорғау саласындағы ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мемлекеттік бақылау.

3. **АЛДЫН АЛУ**
   Ақпараттық – коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптардың сақталуының алдын алу.

4. **ҚАЛЫПТАСТЫРУ**
   Маңызды ақпараттық-коммуникациялық инфрақұрылымның тізбесін қалыптастыру және мониторингі.

5. **БАСҚАРУ**
   Интернеттің қазақстандық сегментінің кеңістігінде домендік атауларды басқару және бөлу.

6. **БЕРУ**
   Ақпараттық қауіпсіздік талаптарына сәйкестігін сынау нәтижелері бойынша акт беру.

7. **ҰЙЫМДАСТЫРУ**
   Ақпараттық қауіпсіздік инциденттеріне ден қоюдың ұлттық жоспарының орындалуын ұйымдастыру.

8. **ҚАРАСТЫРУ**
   Дербес деректер саласындағы бұзушылықтар үшін қарау және жауапқа тарту.

9. **ЖҮЗЕГЕ АСЫРУ**
   Куәландырушы орталықтарды аккредиттеуді жүзеге асыру.

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

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

12. **ЖӘРДЕМДЕСУ**
    Кәсіби стандарттарды қалыптастыруға жәрдемдесу.

13. **ӨЗАРА ӘРЕКЕТТЕСУ**
    Халықаралық ұйымдармен, ұлттық реттеушілермен және киберқауіпсіздік орталықтарымен өзара іс-қимыл.

14. **РҰҚСАТ**
    Қамтамасыз етілген цифрлық активтерді шығаруға және айналысқа рұқсат беру

15. **ҚОЛДАУ**
    Ақпараттық қауіпсіздік саласындағы ғылыми зерттеулерді қолдау.

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ (ҰСЫНЫМДАР)

КОМПЬЮТЕРЛІК ОҚИҒАЛАР КЕЗІНДЕ ҚАЙДА ЖҮГІНУГЕ БОЛАДЫ?

Компьютерлік оқиға кезінде сіз хабарласуыңыз керек!

Әрекет ету қызметі
1400
(8 (7172) 55-99-97

info@kz-cert.kz

Ұлттық компьютерлік инциденттерге жауап беру қызметі - бұл компьютерлік инциденттер туралы ақпаратты жинау мен талдауды, пайдаланушыларға компьютерлік қауіпсіздік қатерлерінің алдын алуда консультациялық және техникалық қолдау көрсетуді қамтамасыз ететін Ұлттық ақпараттық жүйелер мен Интернет желісінің сегментін пайдаланушылар үшін бірыңғай орталық.

ҚЫЗМЕТТІҢ ҚҰЗЫРЕТІНЕ ОЛАРДЫ АНЫҚТАУ ЖӘНЕ БЕЙТАРАПТАНДЫРУ МАҚСАТЫНДА КЕЛЕСІ КОМПЬЮТЕРЛІК ОҚИҒАЛАРДЫ ӨҢДЕУ КІРЕДІ:

желілік инфрақұрылым түйіндері мен сервер ресурстарына шабуылдар;

ақпараттық ресурстарға рұқсатсыз қол жеткізу;

ұлттық ақпараттық желілер мен хосттарды сканерлеу;

парольдерді және басқа аутентификациялық ақпаратты таңдау және түсіру;

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

ақпараттық желілерді қорғау жүйелерін бұзу;

Ақпараттық қауіпсіздік (киберқауіпсіздік) және дербес деректерді қорғау мәселелері бойынша социологиялық зерттеу нәтижелерін ҚЫСҚАША ТАЛДАУ

«Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті» республикалық мемлекеттік мекемесінің 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 80,4% деңгейінде хабардар болуының жалпы көрсеткішін айқындады.

Тұтастай алғанда, ақпараттық қауіпсіздік (киберқауіпсіздік) және дербес деректерді қорғау мәселелері бойынша социологиялық зерттеудің алынған нәтижелері азаматтардың күнделікті өміріндегі ақпараттық қауіпсіздік мәселелерінің өсіп келе жатқан маңыздылығын көрсетеді:

- **фишинг әрекеттерін тану қабілетінің деңгейі – 74,64%-ды құрады;**
- **халықтың 90,52%-ы әлеуметтік желілерді пайдалану кезінде жеке ақпаратты қорғау туралы біледі.**

Зерттеу нәтижелері ақпараттық қауіпсіздік (киберқауіпсіздік) және дербес деректерді қорғау саласындағы халықтың хабардарлығын қалыптастырудағы оң динамизмді көрсетеді. Алайда, бұл саланың сын-қатерлері цифрлық дәуірде азаматтардың мүдделерін тұрақты қорғауды қамтамасыз ету үшін шаралар мен тетіктерді үнемі жетілдіруді талап етеді.

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

ҰСЫНЫМДАР

"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: **moap@mdai.gov.kz**
https://www.gov.kz/memleket/entities/infsecurity?lang=ru

Астана қаласы, 2023 ж.