Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігі

Ақпараттық қауіпсіздік комитеті

КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

Ұсынымдар

2025 жылдың наурыз–қыркүйек айларында жүргізілген “Халықтың киберқауіптер туралы хабардарлығы” социологиялық зерттеуінің негізінде дайындалды

Терминдер және анықтамалар

Кибербуллинг деген не?

Цифрлық технологияларды пайдалану арқылы адамның үстінен күш көрсету, қорлау, қорқыту немесе кемсіту.

Жеке деректер бұл:

Электрондық және (немесе) өзге де материалдық тасымалдағышта тіркелген, белгілі бір немесе олардың негізінде айқындалуы мүмкін жеке деректер субъектісіне қатысты мәліметтер.

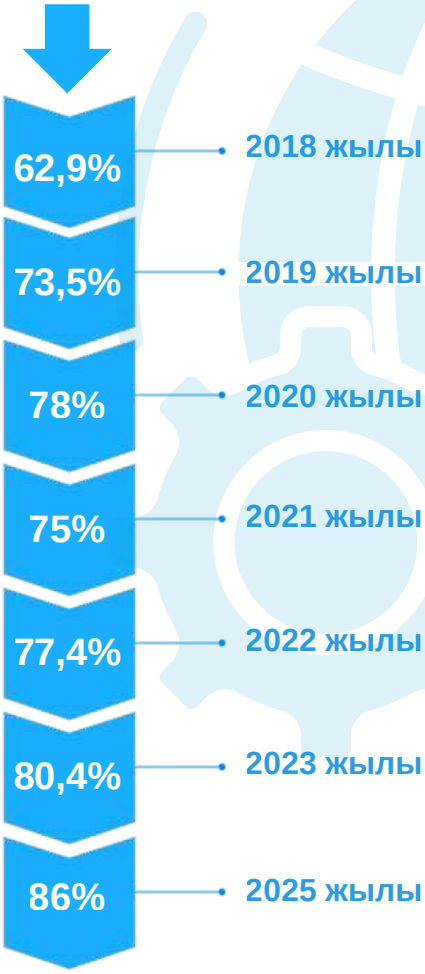
Киберқауіпсіздік түсінігі:

Цифрлық объектілердің құпиялылығын, тұтастығын және қолжетімділігін бұзудан қорғалу жағдайы

Халықтың хабардарлық деңгейі

2023–2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын дамыту және киберқауіпсіздік тұжырымдамасына сәйкес негізгі міндеттердің бірі - халықтың кибергигиена мәселелері бойынша хабардарлық деңгейін арттыру. Осыған байланысты халықтың киберқауіптер мен жеке деректерді қорғау деңгейін айқындау мақсатында Қазақстан халқы арасында социологиялық зерттеу жүргізілді.

Халықтың киберқауіптер мен жеке деректерді қорғау жөніндегі хабардарлық көрсеткіштері:



Социологиялық зерттеу барысында қамтылды:

3 — Республикалық маңызы бар қала (Астана, Алматы, Шымкент)

17 — облыстың аудандары мен ауылдары

6000 — Қатысқан респонденттер

Қатысушылар: 18 жастан бастап және одан жоғары ҚР азаматтары;

Сауалнама блоктарындағы сұрақтар саны:

- **әлеуметтік-демографиялық блок - 5;**
- **негізгі блок - 15;**
- **қосымша блок - 10;**

Қазақстанда киберқауіпсіздік саласын дамыту мәселелеріне ерекше көңіл бөлінуде. Мемлекеттік органдар, ҮЕҰ және бизнеспен бірлескен жұмысының нәтижесі – соңғы жылдардағы үрдіс: біздің еліміз Ғаламдық киберқауіпсіздік индексінде өз позицияларын қарқынды түрде жақсартып келеді. Қазір Қазақстан Tier2 – Advancing тобына кіреді және 29 елден тұратын екінші топта 3-орынды иеленіп, мүмкін болған 100 балдың 94,4 балын жинады.

МАҢЫЗДЫ АҚПАРАТ

Киберқауіпсіздік біздің күнделікті өміріміздің маңызды бөлігіне айналуда. Әдетте киберқауіпсіздік ұғымы үш маңызды қағиданы сақтауды білдіреді:

ҚҰПИЯЛЫЛЫҚ

Бұл нені білдіреді? Ақпаратқа қолжетімділік тек оған құқығы бар адамдарда болуы керек. Ал ондай құқығы жоқ адамдарға ақпаратқа қолжетімділік жабық.

Жағымсыз мысал: *Сіздің картаңыздың нөмірі мен CVV коды жаман адамға қолжетімді болды.*

РЕСПОНДЕНТТЕР ПІКІРІ:

28% **респондент құпия деректерді қорғаудың ең тиімді әрекеттерінің бірі – ақпаратты беру кезінде шифрлау әдістерін қолдану деп санайды.**

29% **респондент құпия деректерді қорғаудың ең тиімді тәсілдерінің бірі – жеке ақпаратқа қоғамдық қолжетімділікті шектеу деп санайды.**

ҚОЛЖЕТІМДІЛІК

Бұл нені білдіреді? Ақпарат қажет болған кез келген сәтте қолжетімді болуы керек. Дереу және жылдам.

Жаман мысал: *Балаңызды балабақшаға орналастыру үшін өтінімді «Әкімдік порталы» арқылы беруіңіз керек. Басқа жолмен қабылдамайды. Бірақ бұл порталдың сайты 5 минут, 15 минут, бір сағат, бір күн, бір апта… ашылмайды.*

ТҰТАСТЫҚ

Бұл нені білдіреді? Ақпарат шынайы болуы керек. Ол өзі өзгеріп кетпеуі тиіс, ал одан да маңыздысы - әдейі бұрмаланбауы қажет.

Жағымсызмысал: *Сіз өз картаңыздан досыңыздың картасына ақша аударып жатырсыз. Зиянды бағдарламалық қамтамасыз ету алушының карта нөмірін өзгертіп, ақшаны алаяқтың картасына жібере алады.*

Сонымен,

КИБЕРҚАУІПСІЗДІК — бұл құпиялылықтың, қолжетімділіктің және бүтіндіктің сақталуы.

Бір қағидаттың бұзылуы, әдетте, басқа қағидаттардың да бұзылуына алып келеді.

	2025	2023	2022	2021	2020
Компьютерлік вирустың шабуылы	18%	22,8%	51,7%	16,5%	32,1%
Зиянды спам	12%	16,9%	34,5%	23,0%	13,4%
Әлеуметтік желілердегі аккаунттарды бұзу	5%	8,1%	28,4%	14,5%	3,9%

ЖАҒЫМСЫЗ ЖАҒДАЙДАН ҚАЛАЙ ҚҰТЫЛУҒА БОЛАДЫ?

11% **пайдаланушылар антивирусты және құпиясөзбен қорғауды қолданбайды.**

Жеке КИБЕРҚАУІПСІЗДІККЕ **7** ҚАДАМ арналған

Киберқатерлер, хакерлер, вирустар, трояндар.

Бәрі түсініксіз және шатастырылған ба?

Қорықпаңыз. Өзіңізді және жақындарыңызды қорғаңыз! Біз сізге дұрыс жолды көрсетеміз. Киберқауіпсіздікке апарар жол небәрі 7 қарапайым қадамнан тұрады.

Бізбен бірге болсаңыз, зұлым хакерлер де, олардың вирустары да сізге қауіп төндірмейді.

1 қадам

ЭЦҚ-ны көздің қарашығындай сақтаңыз

- **Бәріміз ЭЦҚ не екенін білеміз. Бұл – Электрондық-цифрлық қолтаңба. Мұнда Сіздің қорғауыңызға ең дәл ғылым – математика көмектеседі. Қазақстанның әрбір азаматы ЭЦП-ны оңай ала алады. ЭЦП – ыңғайлы әрі сенімді.**
- **Бірақ бір үлкен қауіп бар, және оны сіз білуіңіз қажет. Егер ЭЦҚ-ны сізден ұрлап алса, онда құжаттарға сіздің орныңызға басқа біреу қол қоя алады. Кейде бұл өте маңызды құжаттар болуы мүмкін! Иә, иә, ЭЦҚ-ны да қараусыз жатқан кез келген нәрсе сияқты ұрлауға болады.**

Өз ЭЦҚ-ңызды қорғау үшін келесі шараларды қабылдау қажет:

- **ЭЦҚ-ны алғаш алған кезде бірден күрделі пароль орнатыңыз.**
- **ЭЦҚ-ны бөгде адамдарға бермеңіз. Олар құжаттарға сіздің атыңыздан қол қоюы мүмкін, ал жауапкершілік сізге жүктеледі.**
- **ЭЦҚ-ны арнайы чаттарға, мессенджерлерге жібермеңіз.**
- **ЭЦҚ сақталған компьютер немесе ноутбукты вирустардан қорғау бағдарламаларымен қамтамасыз етіңіз.**
- **ЭЦҚ файлда сақтаған кезде құпия сөзді файл атауымен бірге сақтамаңыз**
- **ЭЦҚ-ны басқа адамның атына алуға болмайды. ЭЦҚ-ны бірнеше тәсілмен алуға болады: Халыққа қызмет көрсету орталықтары (ХҚКО) арқылы немесе eGov арқылы.**
- **Смартфондар мен компьютерге тексерілмеген немесе сенімсіз бағдарламаларды орнатудан аулақ болыңыз.**
- **ЭЦҚ-ны жоғалтқан жағдайда немесе ол бөгде адамдардың қолына түскен жағдайда дереу өз кілтіңізді жаңартыңыз.**

1 қадам

МАҢЫЗДЫ!

Әдетте, ЭЦҚ беру кезінде ХҚКО қызметкері үлгілік құпия сөз орнатады. Өз ЭЦҚ-ңыздың құпия сөзін міндетті түрде ауыстырыңыз. Мұны www.pki.gov.kz сайтында жасауға болады.

Немесе ЭЦҚ шығарған кезде өзіңізге тиесілі, үлгілік емес құпия сөзді орнатуды өтініңіз. Бірақ оны есте сақтауға тура келеді.

НЕ ІСТЕМЕУ КЕРЕК!

ЭЦҚ-НЫ ЕШҚАШАН АШЫҚ ТҮРДЕ ЭЛЕКТРОНДЫҚ ПОШТА АРҚЫЛЫ ЖІБЕРМЕҢІЗ.

Поштаны бұзып кіруі мүмкін, сонда ЭЦҚ-ны міндетті түрде ұрлайды. Жіберу керек пе? Өз қауіп-қатеріңізге қарай, бірақ ЭЦҚ-ны кез келген сенімді тәсілмен міндетті түрде шифрлаңыз. Мысалы, «құпия сөзбен архивтеу» әдісі арқылы. «Құпия сөзбен архивтеуді» білмейсіз бе? Маманнан, туыстардан немесе достардан сұраңыз, сізге міндетті түрде көмектеседі.

Өзіңіздің ЭЦҚ-ны ешқашан бейтаныс компьютерлерге көшірмеңіз.

Егер бәрібір бейтаныс компьютерден бірдеңені қол қоюға тура келсе, ЭЦҚ-ңыздың бөгде компьютерде қалып қоймағанына міндетті түрде көз жеткізіңіз.

ЭЦҚ-ны компьютерде сақтамаңыз.

Хакерлер Сізді бұзып кірген немесе вирус компьютеріңізге енген жағдайда, олар ЭЦҚ-ны табуға тиіс емес, себебі ол жерде болмауы керек. Егер ЭЦҚ-ны флешкаға алған болсаңыз, ал жеке куәлікке немесе токенге емес – ЭЦҚ флешкада қалсын. Флешканы сенімді жерде сақтаңыз және ЭЦҚ-дан басқа мақсаттар үшін пайдаланбаңыз.

2 қадам

СІЗДІҢ ҚАЛҚАНЫҢЫЗ — СІЗДІҢ ҚҰПИЯ СӨЗІҢІЗ

Біздің миымыз қызық түрде құрылған. Біз ассоциациялар арқылы ойлаймыз.
Әрбір ой міндетті түрде алдыңғы ойға сүйенеді. Біздің ойлауымыз - өзара байланысты ойлар, естеліктер мен идеялар ағыны.
Біздің екі түрлі жадымыз бар: қысқа мерзімді және ұзақ мерзімді.
Қысқа мерзімді жадта оқиғалар немесе ақпарат бірнеше минут, сағат, кейде күндер бойы сақталады.
Егер ақпарат біз үшін маңызды болып, оны есте сақтау барысында қандай да бір ассоциациялар туындаса, ақпарат ұзақ мерзімді жадқа өтеді.

Миды зерттеушілердің айтуынша, бұл үдеріс бас миы нейрондарының синапстарының қалыптасуына негізделген. Ақпаратты ұзақ мерзімді жадқа енгізудің ең қарапайым тәсілі — жаңа ақпарат пен сіз мәңгі есте сақтап қалған немесе оңай еске түсіре алатын нәрсенің арасында ассоциативтік байланыс жасау.
Біздің миымыздың ең үлкен бөліктерін пайдалану қажет, олар ЕСТУ және КӨРУ үшін жауап береді.

2 қадам

НЕ ІСТЕУ КЕРЕК?

Біздің миымызда көру жады үшін жауап беретін бөліктер өте жақсы дамыған. Сондықтан мұны пайдалану қажет.
Жұмыс компьютердің алдына отырар кезде айналаңызға қараңыз. Үстелдің үстінде, қабырғаларда, шкафтарда немесе тіпті терезенің сыртында — Сіздің жан-жағыңызда үнемі тұратын жүздеген заттар бар.

Жұмыс орныңызда отырып күнде көретін бір затты ойыңызда пароль ретінде «таңдап алыңыз». Сол — сіздің құпия сөзіңіз болады.
Мысалы: Kachestvennyy_organayzer

Күрделі құпия сөзді құрастыратын пайдаланушылар:

2023 жылы — **22%**

2025 жылы — **47%**

МАҢЫЗДЫ!
Құпия сөз ретінде бір затты таңдағанда, екі сөзді ойластырыңыз, мысалы: заттың атауы және оның түсі. Сүйікті әндердің сөздерін, болған қалаларды немесе орындарды да қолдануға болады. Ең бастысы — құпия сөзде кемінде 8 таңба болуы керек.

НЕ ІСТЕМЕУ КЕРЕК?

1) Өзіңіздің құпия сөзіңізді ешқашан басқа адамдарға бермеңіз. Тіпті сұраса да.

2) Құпия сөздеріңізді стикерлерге, қағазға жазбаңыз. Құпия сөздерді электрондық поштаның ішінде сақтамаңыз.

3 қадам

ЭЛЕКТРОНДЫҚ ПОШТА

Өкінішке қарай, алаяқтар бізге келген хаттарды оқитынымызды әлдеқашан түсініп қойған. Демек, айламен жазылған хат арқылы бізді алдауы мүмкін.

Алаяқтық схемасының мысалы: «Шетелдік адвокаттан мұра туралы хат».

Схема мәні:

Электрондық поштаға өзін шетелдік адвокат немесе нотариус ретінде таныстырған адамнан хат келеді. Ол хатта «сіздің тегіңізбен» клиенттің жақында қайтыс болғаны және үлкен мұра қалдырғаны айтылады — әдетте 1 млн-нан 10 млн долларға дейінгі көлемінде.

Алаяқтық қалай дамиды:

1. Адвокат мұрагерлер жоқ екенін және сіз заңды алушы бола алатыныңызды айтады. 2. Содан кейін келесі мәліметтерді сұрайды: жеке куәлік көшірмесі, байланыс деректері, кейде – сенімхат. 3. Кейін рәсімдеу үшін «шағын шығындарды» төлеу қажет екенін айтады: нотариалдық қызметтер, баж салығы, құжаттарды аудару ақысы, банк шотын «жібіту».

Ақша жіберілгеннен кейін алаяқтар байланысқа шықпай қояды.

Жеке компьютерлердің жұқтырылуының ең кең тараған тәсілі — зиянды мазмұны бар электрондық хат жіберу.

НЕ ІСТЕУ КЕРЕК?

Ешқашан өздігінен іске қосылатын файлдарды ашпаңыз.

Мұндай файлдарды атаудың соңғы нүктесінен кейін келетін әріптерден оңай тануға болады. Бұл әріптер файлдың кеңейтімі деп аталады.

Өздігінен іске қосылатын файлдардың кеңейтімдеріне мысалдар:

.exe **.com** **.cmd** **.msi** **.bat**

Мұндай кеңейтімдері бар файлдарды ашуға болмайды.

Тіпті олар архивке салынған болса да. Мысалы, winzip архивіне қапталған болса.

3 қадам

Хакерлер кеңсе қолданбаларының кәдімгі құжат файлдарын да өзгерте алады.
Макростар — кеңсе қолданбаларының стандартты әрекеттерін жазуға және қайта орындауға мүмкіндік беретін командалар жиынтығы.
Сіз макроста қандай командалар жазылғанын білмейсіз. Командалар жиынтығы өте үлкен болуы мүмкін және зиянды кодты білдіруі ықтимал.

МАҢЫЗДЫ!
Электрондық пошта арқылы келген файлдардағы «макростарды» ешқашан қосуға болмайды.

НЕ ІСТЕМЕУ КЕРЕК?

Күдікті хаттарды ашпаңыз.
Егер хат сізге қызық емес болса, демек ол сіздің назарыңызға лайық емес. Қоса берілген файлдарды (тіркемелер) мұқият қарап шығыңыз.

Күдікті хаттарға жауап бермеңіз.

Күдікті хаттардағы сілтемелерге кірмеңіз.
Есіңізде болсын, алаяқтар адам эмоцияларымен ойнайды – ашкөздік, тәкаппарлық, қорқыныш, ашу. Ақылмен ойлаңыз және алаяқтық схемаларына алданып қалмаңыз.

45% **пайдаланушылар әлеуметтік желілер мен мессенджерлерде жіберілген сілтемелерге кірмейді.**

4 қадам

АНТИВИРУСТЫҚ ҚОРҒАНЫС

Атауынан түсінікті болғандай, **Антивирус – «вирустардан» қорғауға арналған құрал.**

Біз барлық зиянды бағдарламалық қамтамасыз етуді «вирустар» деп атаймыз. Бұл толық дұрыс емес, өйткені «вирус» – зиянды бағдарламалық қамтамасыз етудің (қысқаша БҚ) тек бір белгісі ғана.

Бірақ нақты білу керек нәрсе – зиянды БҚ миф емес, ол шынында да зиянды және оның түрлері өте көп. Алаяқтар қолжетімділік, құпиялылық және бүтіндікке қауіп төндіретін барынша айлакер схемаларды ойлап табуға тырысады.

Компьютерлік «вирустар» шынайы жұқпалы ауруларға өте ұқсас, тек олар адамдарды емес, компьютерлік жүйелерді зақымдайды.

Антивирусты компьютерлік «вирустар» үшін вакцина немесе екпе ретінде қабылдау қажет.

ЕКПЕДЕ МАҢЫЗДЫСЫ НЕ?

1. Екпе сапалы дайындалуы керек,

әйтпесе жанама әсерлер пайда болуы мүмкін және ауыр салдарлар орын алуы ықтимал. Вакцинация кезінде біз әрдайым сұраймыз: бұл қандай екпе, оны кім жасады, клиникалық сынақтардан өтті ме?

2. Екпе тиімді болуы керек,

әйтпесе оны салудың еш мәні жоқ. Мұндай жағдайда вакцинация айтарлықтай зиян келтіруі мүмкін. Біз шын мәнінде жоқ «қорғаныс иллюзиясын» аламыз.

3. Екпені уақытылы салу қажет!

Вакцинация мерзімін өткізіп алуға болмайды және екпені әлсіреген немесе ауырып тұрған ағзаға салуға тіпті болмайды.

4 қадам

Антивирустарға адамның нақты вирустарына қарсы салынатын екпелер сияқты қараңыз.

Интернеттегі ақпараттық қауіпсіздікті қамтамасыз етуде антивирустық БҚ қолдануды ең маңызды деп санайтын респонденттердің саны:

2023 жылы

23%

2025 жылы

23%

Смартфон мен компьютеріңізге кез келген сенімді антивирус орнатыңыз және оның жаңартуларын өшірмеңіз!

5 қадам

ЖАҢАРТУЛАР ЖӘНЕ ТАҒЫ ДА ЖАҢАРТУЛАР

Жүйені жаңарту — бізді бірақ ашуландырады! Бірақ заманауи БҚ мыңдаған кәсіби мамандардың еңбегінің нәтижесі болып табылады.

Қазіргі бағдарламаларда мыңдаған жол код бар. Әрине, бұл кодта түрлі қателер, сәйкессіздіктер, олқылықтар болуы мүмкін. Мұндай қателерді **«осалдықтар»** деп атайды.

Бұл сапасыз салынған, тесіктері бар қабырғаға ұқсайды, тек оны тұсқағазбен жапқан. Егер дәл қай жерде тесік барын білсеңіз, тұсқағазды саусақпен тесуге болады.

Жақсысы — бағдарламалық қамтамасыз ету қабырға емес. Ол компьютерлік кодтар жиынтығы.

Және жақсысы — сіздің смартфон мен компьютер Интернетке қосулы. Бағдарлама өндірушілері өздерінің **«осалдықтарына»** Интернет арқылы **«жамау»** жібереді.

Айтпақшы, **«заплатка»** сөзі ағылшынша patch деп аталады, сондықтан **«заплатка» — патч** деп те айтылады.

Өтінеміз, қабырғалардағы тесіктерді уақытында жабыңыз! Патчтар бағдарламалық қамтамасыз етуіңізге уақытында орнатылсын. Тіпті бірнеше сағатқа кешігу қауіпті.

НЕ ІСТЕУ КЕРЕК?

Бағдарламалық қамтамасыз ету жаңартуларын орнатыңыз. Әрқашан.
Антивирус пен операциялық жүйе автоматты түрде жаңартылуы керек.

Соңғы жаңартулардың орнатылғанын тексеріп отырыңыз.

5 қадам

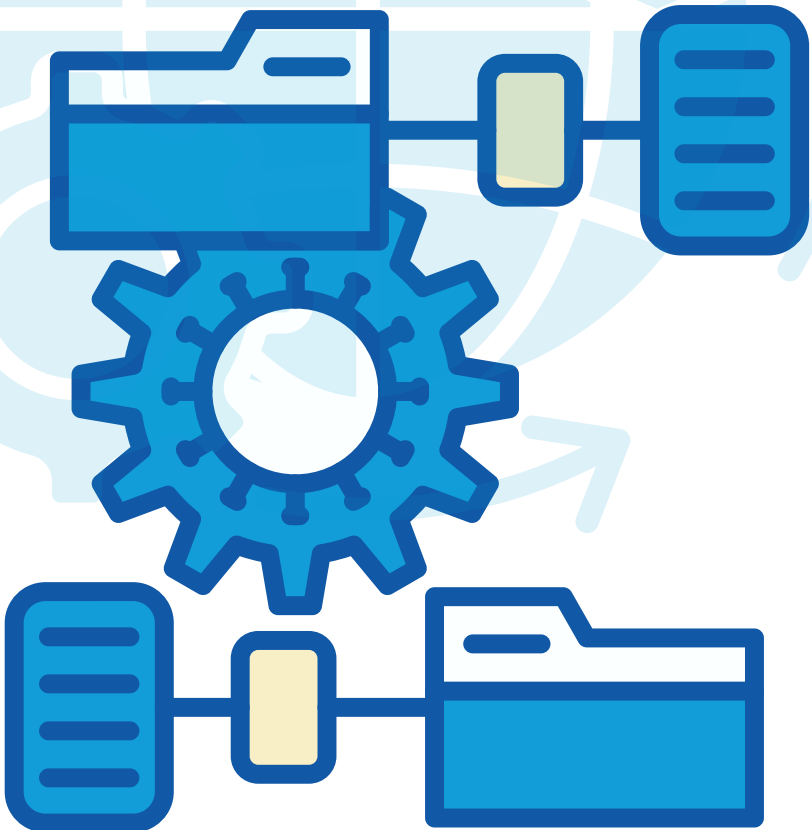
НЕ ІСТЕМЕУ КЕРЕК?

Контрафактілік (пираттық) БҚ қолдану.

Әдетте пираттық БҚ шеберлермен алдын ала бұзылған және жаңарту жүйесінен ажыратылған болады. Өйткені БҚ өндірушінің серверіне жүгінген кезде бірден тауардың контрафактілі екені анықталады. Демек, Сіз жаңартулар алмайсыз және «тесігі бар» БҚ-мен жұмыс істейсіз.

Сізге мұндай қажет пе?

Және, өтініш, жаңартуларды өшірмеңіз.



6 қадам

ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ, ӘЛЕУМЕТТІК ЖЕЛІЛЕР, СКИММИНГ

Әлеуметтік инженерия – адамдардың психология ерекшеліктеріне негізделген, қажетті ақпаратқа қол жеткізу әдісі.
Компьютерлік жүйелердің құпия сөздерін ешқашан ешкімге айтпаңыз. Қағазға жазылған құпия сөздерді көзге көрінетін немесе бөгде адамдар қол жеткізе алатын жерлерде қалдырмаңыз.

Біліп қойыңыз, қаскөйлер біздің эмоцияларымызды манипуляциялауға тырысады. Бейтаныс адамдарға туыстарыңыз бен әріптестеріңіздің мобильді телефон нөмірлерін, IP мекенжайларын, жұмыс орнында немесе үйде болмау уақытын айтпаңыз.

Монитор немесе смартфон экранын иығыңыздың үстінен қарап қоюлары мүмкін. Арқаңызда бөгде адамдар бар кезде компьютер немесе ноутбукпен жұмыс істемеңіз.
Адам көп жерде болсаңыз, арқаңызбен мөлдір емес қабырғаға қаратып отыруға тырысыңыз.

Скимминг – скиммер арнайы мәліметтерді оқитын құрылғы, яғни осы арқылы банк картасының деректерін немесе парольдерді ұрлау тәсілі.

Қоғамдық орындарда бейнекамералар көп. Құпия сөздерді мүмкіндігінше жасырын енгізуге тырысыңыз, мысалы мобильді телефон экранын алақаныңызбен немесе киіммен жауып. Құпия сөз енгізген кезде ноутбук экранын да барынша жауып, саусақтарыңыздың қозғалысын жасыру қажет.

Банкоматтар мен төлем терминалдары:
Банкоматты пайдаланбас бұрын оны мұқият қарап шығыңыз. Пернетақтаның қалыптан тыс биік болуы немесе картаны енгізу терезесінің ерекше болуы Сізді сақ болуға тиіс.

6 қадам

Күмәндансаңыз – басқа банкоматты пайдаланыңыз. Өзіңізді тура артыңызда бірнеше күмәнді адам тұрғандай ұстаңыз.
ПИН-код немесе пароль енгізген кезде пернетақтаны алақаныңызбен жабыңыз.

НЕ ІСТЕУ КЕРЕК?

Сақ болыңыз, мұқият әрі абай болыңыз.

НЕ ІСТЕМЕУ КЕРЕК?

- **Бейтаныс адамдармен телефон арқылы банк шоттарыңыз немесе карталарыңыз туралы сөйлеспеңіз.**

Әрине, кейде сөйлесу қажет болады, бірақ тек Сіз өзіңіз ресми телефон нөмірі арқылы банкке қоңырау шалған жағдайда ғана.

- **Күдікті хаттарға жауап бермеңіз, бірақ бұны біз Пошта бөлімінде айтқанбыз.**
- **Күдікті банкоматтар мен төлем терминалдарын пайдаланбаңыз**
- **Картаңызды официантқа немесе барменге ұзақ уақытқа бермеңіз. Картамен төлемді тек өзіңіз жасаңыз.**

Егер сіз қоғамдық WiFi арқылы интернетке қосылсаңыз (мысалы, әуежайда немесе кафеде), VPN қызметтерін қолданғаныңыз жөн.

7 қадам

РЕЗЕРВТІК КӨШІРУ

АҚПАРАТ ЖОҒАЛЫП КЕТУІ МҮМКІН. МІНДЕТТІ ТҮРДЕ ЖАМАН ХАКЕРЛЕР ШАБУЫЛ ЖАСАУЫ ШАРТ ЕМЕС. ТЕЛЕФОНДЫ ЖОҒАЛТЫП АЛУЫҢЫЗ НЕМЕСЕ КОМПЬЮТЕРДІҢ ҚАТҚЫЛ ДИСКІ ЖАНЫП КЕТУІ ДЕ ЖЕТКІЛІКТІ.

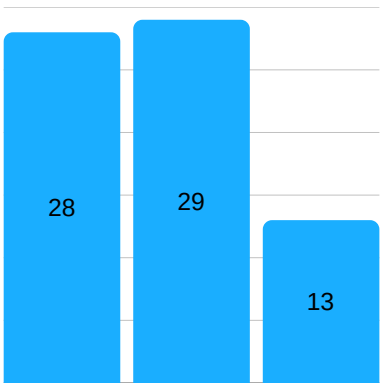
НЕ ІСТЕУ КЕРЕК?

Маңызды ақпаратты үнемі сыртқы тасымалдағышқа көшіру қажет.
Ең қарапайым тәсіл – көптеген резервтік көшіру сервисін пайдалану. Олардың кейбірі тегін, мысалы Google бұлт қоймасы, Apple iCloud, Mail.ru, Yandex.
Сондай-ақ қазақстандық бұлттық қоймалар қызметтерін де пайдалануға болады, мысалы: Oblako.kz және Ps.kz.

МАҢЫЗДЫ!
Егер Сіз ақпаратты сақтау үшін бұлттық сервистерді пайдалансаңыз – демек, Сіз тәжірибелі пайдаланушысыз. Өзіңізді тәжірибелі пайдаланушы сияқты ұстаңыз.Тәжірибелі пайдаланушымын дедіңіз – соған сай әрекет етіңіз.

Құпия деректерді қорғау үшін төмендегі әрекеттердің қайсысын ең тиімді деп санайсыз?

Өткізілген сауалнамаға респонденттердің жауаптары:



- **Деректерді беру кезінде шифрлауды пайдалану – 28%**
- **Жеке ақпаратқа қоғамдық қолжетімділікті шектеу – 29%**
- **Антивирустық бағдарламалық қамтамасыз етуді орнату – 13%**

7 қадам

Құпия сөздер! «Құпия сөздер» бөліміндегі біздің жадынамызды мұқият оқыңыз. Сенімді құпия сөзсіз бұлтта «серуендеу» болмайды.

Екі факторлы аутентификацияны қолданыңыз. Смартфоныңызда саусақ ізімен немесе бет-әлпетін тану арқылы бұғатты ашуды өшірмеңіз.

НЕ ІСТЕМЕУ КЕРЕК?

Өте құпия ақпаратты «бұлтта» сақтауға бәрібір болмайды.
ЭЦҚ-ңызды ашық түрде, сондай-ақ отбасылық немесе жеке құпияларды «бұлтта» сақтамаңыз.

Ең сенімдісі – өзіңізге сыртқы қатқыл диск немесе үлкен жады картасын алыңыз.

Компьютер немесе смартфоннан маңызды ақпаратты осы қатқыл дискке үнемі көшіру жеткілікті. Бұл, әрине, өзін-өзі тәртіпке келтіру мен ұйымдасушылықты талап етеді.

Барлық жеті қадамды орындаңыз – және Сіз жеке ақпараттық қауіпсіздіктің шебері боласыз.

МЕМЛЕКЕТТІК ҚЫЗМЕТКЕРЛЕР ҮШІН КИБЕРҚАУІПСІЗДІК БОЙЫНША ҚОСЫМША ҰСЫНЫМДАР

Мемлекеттік органның (МО) ішкі желілерін Интернетке қосуға тыйым салынады.

Интернет желісіне қосылуды тек Бірыңғай Интернетке қол жеткізу шлюзі арқылы жүзеге асыру қажет.

Интернет ресурстарымен және электрондық поштамен жұмыс істеу барысында қызметтік қажеттілік бойынша немесе өзге жолмен белгілі болған мемлекеттік, қызметтік және коммерциялық ақпаратты жариялауға тыйым салынады.

(МО) мен жергілікті атқарушы органдардың (МАО) қызметкерлері қызметтік міндеттерін орындау кезінде электрондық хат алмасу үшін тек ведомстволық электрондық поштаны пайдаланады.

Компьютерлер мен Интернет желілерін қараусыз қосулы күйде қалдыруға тыйым салынады. Жұмыс орнын тастап кеткен жағдайда компьютерді міндетті түрде бұғаттау қажет (пернетақта комбинациясы: Windows+L).

Мемлекеттік органның (МО) Бірыңғай көлік ортасына (БКО), МО-ның жергілікті желісіне сымсыз желілер, сымсыз қолжеткізу, модемдер, радиомодемдер, ұялы байланыс операторларының желі модемдері және басқа да сымсыз желілік құрылғылар арқылы қосылуға тыйым салынады.

ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУ ЖӨНІНДЕГІ ҰСЫНЫСТАР

КЕЛІСІМГЕ ҚОЛ ҚОЙҒАН КЕЗДЕ НАЗАР АУДАРЫҢЫЗ:

- **оператор жинайтын жеке деректер тізімі;**
- **жеке деректерді жинау және өңдеудің мақсаттары;**
- **келісімнің қолданылу мерзімі немесе кезеңі;**
- **үшінші тұлғаларға беру мүмкіндігі;**
- **деректерді трансшекаралық берудің мүмкіндігі;**
- **жеке деректерді қоғамдық көздерде тарату мүмкіндігі.**

Жеке деректерді бір жерге берген кезде, міндетті талап – жеке тұлғаның келісімі болуы немесе Заңда көзделген негіздің болуы.

Сіздің келісіміңізсіз жеке деректер оператор тарапынан басқа тұлғаларға немесе ұйымдарға берілмейді.

Сондай-ақ жеке деректердің заңсыз таратылуынан қорғау мақсатында ұйымның жеке деректердің құпиялылығын сақтау саясатымен мұқият танысу және олардың өңделу шарттарына
ерекше назар аудару қатаң түрде ұсынылады.

НЕ ІСТЕУ КЕРЕК?

Жеке деректердің заңсыз жиналуын немесе таралуын анықтаған жағдайда

азаматтар бұзушылықтардың алдын алу шараларын қабылдау үшін Қазақстан Республикасы жасанды интеллект және цифрлық даму министрлігінің ақпараттық қауіпсіздік комитетіне жүгінуіне болады.

Мұны «Электрондық үкімет» порталымен («Электрондық өтініштер» бөлімі) жазу арқылы жасауға болады, сондай-ақ төрағаның жеке блогына жазуға болады (*https://dialog.egov.kz/blogs/3932160/welcome*)

e-gov

ӨТІНІШТЕ КӨРСЕТІЛУІ ТИІС

1. Өтініш берушінің Т.А.Ә. және байланыс деректері
2. Бұзушылық орын алған жағдайдың сипаттамасы
3. Бұзушылық жасалған мерзімі мен кезеңі
4. Бұзушылықты растайтын дәлелдемелер
5. Бұзушылыққа жол берген ұйымның атауы

Егер сіз қандай да бір тұлға сіздің жеке деректеріңізді сіздің келісіміңізсіз жинап немесе өңдеп жатқанын анықтасаңыз, сіз бұл ұйымға жүгініп, заңсыз жиналған деректерді жоюды талап етуге құқылысыз.
Сонымен қатар, сіз бұрын берілген жеке деректерді жинауға және өңдеуге арналған келісімді қайтарып алуға құқылысыз.
Егер оператор деректерді жоюдан бас тартса немесе әрекетсіз қалса, сіз жеке деректерді қорғау саласындағы уәкілетті органға шағымдана аласыз, яғни - ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ ЦИФРЛЫҚ ДАМУ МИНИСТРЛІГІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІНЕ.
Өтініштерді кез келген ыңғайлы және қолжетімді тәсілмен жіберуге болады.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК КОМИТЕТІНІҢ ӨКІЛЕТТІКТЕРІ

Қазақстан Республикасы Президентінің 2016 жылғы 6 қазандағы №350 Жарлығына сәйкес Ақпараттық қауіпсіздік комитеті құрылды.

1. **ӘЗІРЛЕУ**
   Мемлекеттік органдарды қоспағанда, ақпараттық қауіпсіздікті қамтамасыз ету саласындағы талаптарды әзірлеу.

2. **БАҚЫЛАУ**
   Ақпараттық қауіпсіздік саласында мемлекеттік бақылауды жүзеге асыру, оның ішінде жеке деректерді қорғау, электрондық ақпараттық ресурстар мен ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету.

3. **ПРОФИЛАКТИКА**
   Ақпараттық қауіпсіздік талаптарының сақталуын қамтамасыз ету бойынша профилактикалық іс-шараларды жүргізу.

4. **ҚАЛЫПТАСТЫРУ**
   Ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің тізімін қалыптастыру және мониторинг жүргізу.

5. **БАСҚАРУ**
   Қазақстандық интернет сегменті кеңістігіндегі домендік атауларды басқару және бөлу.

6. **БЕРУ**
   Ақпараттық қауіпсіздік талаптарына сәйкестігін тексеру нәтижелері бойынша қорытынды беру.

7. **ҰЙЫМДАСТЫРУ**
   Ұлттық ақпараттық қауіпсіздік жоспарларын іске асыруды және ақпараттық қауіпсіздік инциденттеріне ден қоюды ұйымдастыру.

8. **ҚАРАСТЫРУ**
   Жеке деректер саласындағы бұзушылықтар бойынша қарастыру және жауапкершілікке тарту.

9. **ІСКЕ АСЫРУ**
   Куәландыру орталықтарын аккредиттеу жөніндегі қызметті жүзеге асыру.

10. **ХАБАРДАР ЕТУ**
    Халықтың ақпараттық қауіпсіздік (киберқауіпсіздік) қатерлері туралы хабардарлығын арттыру.

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

12. **ЫҚПАЛ ЕТУ**
    Кәсіби стандарттарды қалыптастыруға ықпал ету.

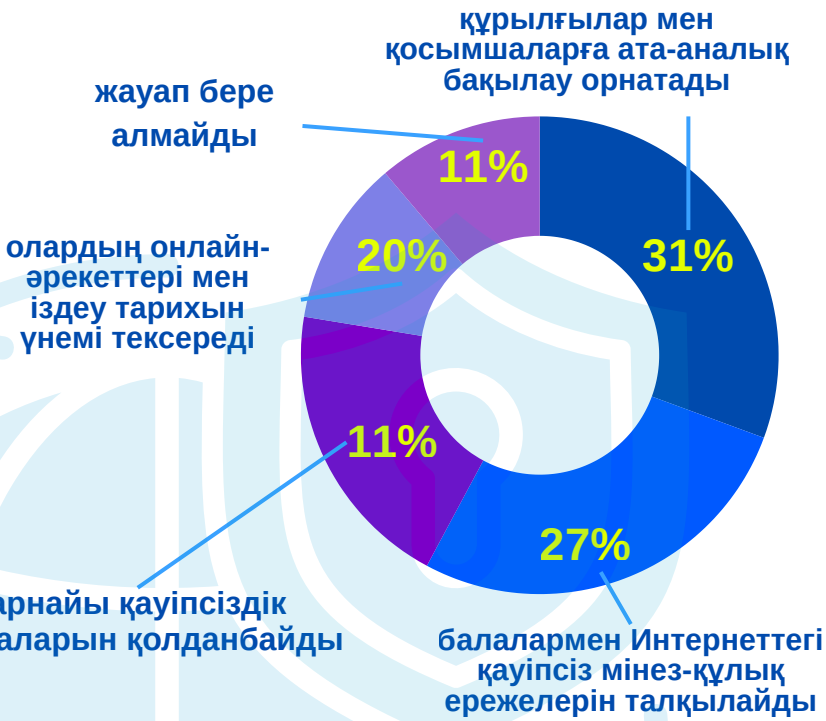
13. **ӨЗАРА ӘРЕКЕТТЕСУ**
    Халықаралық ұйымдармен, ұлттық реттеушілермен және киберқауіпсіздік орталықтарымен өзара әрекеттесу.

14. **РҰҚСАТ БЕРУ**
    Қамтамасыз етілген цифрлық активтерді шығару және айналымға жіберуге рұқсат беру.

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

Балалардың интернет желісіндегі қауіпсіздігін қорғау

Зерттеуге қатысушылармен өткізілген диалогтың жалғасы барысында бүгінгі күні өзекті болып отырған балаларды интернеттегі қажетсіз ақпараттан қорғау мәселесі де талқыланды. Респонденттердің пікірінше, баланы Интернеттегі қажетсіз ақпараттан қорғаудың негізгі шарасы мынадай болып табылады:



Ата - аналар үшін ұсынымдар:

- **Жасөспірімдердің қатысуымен Интернетті пайдалану бойынша үй ережелерінің тізімін жасаңыз және оның бұлжытпай орындалуын талап етіңіз. Балаңызбен бірге тыйым салынған сайттар тізімін («қара тізім»), Интернетте болу уақыты мен Интернеттегі (соның ішінде чаттардағы) қарым-қатынас ережелерін талқылаңыз.**
- **Интернетке қосылған компьютер ортақ бөлмеде орналасуы тиіс.**
- **Балалардың Интернеттегі достары туралы, олардың немен айналысатыны туралы әңгімелесуді ұмытпаңыз – дәл өмірдегі достары туралы сөйлескендей. Балалар жылдам хабар алмасу қызметтері арқылы кімдермен сөйлесетінін сұрап, бұл адамдардың оларға таныс екеніне көз жеткізіңіз.**
- **Стандартты Ата-аналық бақылауға қосымша ретінде қажетсіз контентті бұғаттау құралдарын пайдаланыңыз.**
- **Балаларыңыз қандай чаттарды пайдаланатынын білуіңіз қажет. Модерациялы чаттарды пайдалануды қолдаңыз және балалардың жеке (приват) режимде сөйлеспеуін талап етіңіз.**

Балаңыздың Интернетті пайдалануын үнемі бақылаңыз! Бұл оның жеке кеңістігін бұзу емес, сақтық шарасы және Сіздің ата-аналық жауапкершілігіңіз бен қамқорлығыңыздың көрінісі.

Онлайн алаяқтық кезіндегі негізгі қағидаттар

1 Күдіктену қағидасы

Кез келген **«шұғыл», «дереу», «сіздің шотыңыз бұғатталды»** деген сөздер күмән тудыруы тиіс.

Кибералаяқтар әрқашан **қорқыныш немесе ашкөздікке** қысым жасайды: «ақшаңызды жоғалтасыз», «сіз сыйлық ұттыңыз», «сізге несие мақұлданды».

2 Құпия деректерді ешқашан хабарламаңыз

ПИН-кодтарды, құпия сөздерді, картаның CVV-кодын, SMS немесе PUSH-хабарламалардағы кодтарды **ешкімге айтуға болмайды** — тіпті телефон арқылы «банк қызметкеріне» немесе «полицияға» да. Нағыз банктер мен мемлекеттік органдар мұндайды сұрамайды.

3 Тыныштық жылдамдықтан гөрі маңызды

Егер сізге қоңырау шалып, шотыңызды бұғаттаймыз, айыппұл саламыз немесе қылмыстық іс қозғаймыз деп қорқытса — **дереу тұтқаны қойып**, банкке немесе тиісті мемлекеттік органға өзіңіз қайта қоңырау шалыңыз.

Ешқашан «бір минут ішінде» шешім қабылдамаңыз.

ИНТЕРНЕТ-САТЫП АЛУЛАР ЖӘНЕ ОНЛАЙН-СЕРВИСТЕР

ТӨЛЕМ ЖАСАМАС БҰРЫН САЙТТЫ ТЕКСЕРІҢІЗ

- Сайттың мекенжайы https:// деп басталып және дүкеннің/банктің дұрыс атауын қамтуы керек.
- Төлемді тек ресми сайттарда және сенімді төлем жүйелері арқылы жасаңыз.

ХАБАРЛАНДЫРУЛАР МЕН МАРКЕТПЛЕЙСТЕРГЕ АБАЙ БОЛЫҢЫЗ

- Тым төмен баға, «қазір алдын ала төлеу», платформадағы қауіпсіз мәміледен бас тарту — алаяқтық белгілері.
- Сенімді кепілдіктер жоқ болса, тауар немесе қызметті алғанға дейін «таныс емес адамның картасына» ақша аудармаңыз.

ЖАЛҒАН СЕРВИСТЕР МЕН ҚОСЫМШАЛАР

- Қосымшаларды тек ресми дүкендерден (Google Play, App Store) жүктеңіз.
- SMS немесе хаттағы сілтеме арқылы кірген сайттарға логин мен құпия сөз енгізбеңіз — браузерді ашып, мекенжайды қолмен теріңіз.

КӘСІБИ МАМАНДАРҒА АРНАЛҒАН БӨЛІМ

Егер сіз бизнес иесі, жауапты қызметкер, IT-маманы немесе ақпараттық қауіпсіздік офицері болсаңыз – осы ұсынымдарды сақтаңыз:

КИБЕР ҚАУІП-ҚАТЕРЛЕР ТӘУЕКЕЛДЕРІН АЗАЙТУ ҮШІН 10 ҚАДАМ

1 **Ақпараттық қауіпсіздік саясатын әзірлеу.** Бұл – бірінші деңгейдегі құжат, ақпараттық қауіпсіздік саласындағы сіздің конституцияңыз. Бірақ конституциядан бөлек заңдар да қажет. Мұндай заңдар «Екінші деңгейдегі құжаттар» деп аталады және саясат талаптарын нақтылай түседі. Толығырақ Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 (ЕТ) қаулысында, 33-тармақта көрсетілген.

МАҢЫЗДЫ!
«Мобильді құрылғылар мен ақпарат тасымалдағыштарын пайдалану ережелері» құжатын міндетті түрде бекітіңіз.

2 **Пайдаланушыларды ағарту және хабардар ету.**
Персоналды даярлау бағдарламасын әзірлеу. Барлық қызметкерлерге ақпараттық қауіпсіздік нормаларын үйрету жүйелерін енгізу.
Пайдаланушылардың кибер-тәуекелдер туралы хабардарлығын қолдау.

3 **Инциденттерді басқару.**
Келесі шаралар қажет (ал кейбір ұйымдар үшін міндетті):
ақпараттық қауіпсіздік оқиғаларын тіркеу, ақпараттық қауіпсіздік инциденттерін басқару, ақпараттық қауіпсіздік инциденттері туралы жауаптыларды хабардар ету, ақпараттық қауіпсіздік инциденттерін Мемлекеттік техникалық қызметтің Компьютерлік инциденттерге әрекет ету қызметінде тіркеу.
Сіз не болғанын және не болып жатқанын нақты білуіңіз керек.
Толығырақ Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысында, 2-параграфта көрсетілген.

КӘСІБИ МАМАНДАРҒА АРНАЛҒАН БӨЛІМ

4

Тәуекелдерді басқарыңыз.
Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесін әзірлеу ұсынылады. Сіздің ұйымыңызға қандай қауіп-қатерлер төнетінін білуіңіз қажет.

5

Пайдаланушылардың артықшылықтарын басқару.
Тіркелгі деректерін басқару процестерін енгізіп, артықшылыққа ие тіркелгілердің санын шектеу қажет. Пайдаланушылардың артықшылықтарын шектеп, олардың әрекеттерін бақылау керек. Қол жеткізуді, пайдаланушы әрекетін және аудит журналдарын бақылау жүзеге асырылады.

6

Алынбалы тасымалдағыштарды басқару элементтері.
Алынбалы тасымалдағыштарға қол жеткізуді басқару саясатын әзірлеу қажет. Тасымалдағыш түрлері мен пайдаланылуын шектеу. Корпоративтік жүйеге импорттамас бұрын барлық тасымалдағыштарды зиянды бағдарламаларға тексеру.

7

Мониторинг.
Мониторинг стратегиясын және оған қосымша саясатты әзірлеу қажет. Барлық АКТ жүйелері мен желілеріне тұрақты мониторинг жүргізу. Шабуылға нұсқауы мүмкін әдеттен тыс әрекеттерді анықтау үшін журналдарды талдау.

8

Қауіпсіз конфигурация.
Қауіпсіздік патчтарын қолданыңыз және барлық АКТ жүйелерінің қауіпсіз конфигурациясы сақталғанына көз жеткізіңіз. Барлық АКТ құрылғылары үшін түгендеу жүйесін және базалық жинақты анықтау механизмін жасау.

9

Зиянды бағдарламалардан қорғау.
Сіздің қызмет бағытыңызға сәйкес келетін және өзекті зиянды бағдарламалардан қорғау саясатын әзірлеп, орнату қажет.
Ұйым ішінде зиянды бағдарламаларға сканерлеу жүргізу.

10

Желілік қауіпсіздік.
Желіні сыртқы және ішкі шабуылдардан қорғау. Желі периметрін басқару. Рұқсатсыз қолжетімділік пен зиянды мазмұнды сүзгіден өткізу. Қауіпсіздік бақылау элементтерін мониторингтеу және тестілеу.

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 Республикасының Жасанды интеллект және цифрлық даму министрлігінің «Ақпараттық қауіпсіздік комитеті» республикалық мемлекеттік мекемесінің тапсырысы бойынша киберқауіпсіздік және жеке деректерді қорғау мәселелері жөнінде социологиялық зерттеу жүргізілді.

Сауалнама нәтижесі халықтың киберқауіпсіздік пен жеке деректерді қорғау саласындағы бар қауіптер туралы хабардарлық деңгейін **86%** деңгейінде көрсетті.

Жалпы алғанда, киберқауіпсіздік және жеке деректерді қорғау мәселелері жөніндегі социологиялық зерттеу нәтижелері аталған мәселелердің азаматтардың күнделікті өміріндегі **маңыздылығының артып келе жатқанын көрсетеді**:

- фишинг әрекеттерін тану қабілеті деңгейі – **84,8%**;
- **80,5%** онлайн-сервистерде тіркелу кезінде қауіпсіз стратегияны таңдайды (әр түрлі күрделі құпиясөздер);
- **85,9%** респондент интернет-дүкендерде тауар сатып алу кезінде қауіпсіздік шараларын қолданады;
- кемінде **86%** ата-ана балалары интернетте қарайтын контентті айына бір рет немесе одан да жиі тексеріп отырады.

Зерттеу нәтижелері халықтың киберқауіпсіздік және жеке деректерді қорғау саласындағы хабардарлығын қалыптастыруда **оң динамика** бар екенін көрсетеді. Алайда, бұл саладағы сын-қатерлер азаматтардың мүдделерін цифрлық дәуірде сенімді қорғау үшін шаралар мен тетіктерді үздіксіз жетілдіруді талап етеді.

Осыған байланысты, жүргізілген социологиялық сауалнама нәтижелерін ескере отырып, зерттеу тобы азаматтардың киберқауіпсіздігін және олардың жеке деректерін цифрлық кеңістікте қорғауды одан әрі қамтамасыз ету бойынша **тиісті ұсыныстар мен ұсынымдар әзірледі**.

ҰСЫНЫМДАР

Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігінің «Ақпараттық қауіпсіздік комитеті» РММ тапсырысы бойынша

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

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

Астана қ., 2025 ж.